IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-3, CONTROLLING A COMPUTER BOTNET THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:15 cv 240 LMB/IDD

FILED UNDER SEAL PURSUANT TO LOCAL CIVIL RULE 5

DECLARATION OF KARTHIK SELVARAJ IN SUPPORT OF PLAINTIFFS' APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Karthik Selvaraj, declare as follows:

1. I am a Senior Anti-Virus Researcher/Strategist in the Malware Protection Center of Microsoft Corporation. I make this declaration in support of Plaintiffs' Application for An Emergency Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. INTRODUCTION

A. My Experience In The Investigation Of Cybercrime

2. In my role at Microsoft, I am responsible for identifying & building technology to protect against computer security threats and exploits by conducting laboratory-based research. I also provide strategic direction for the security research team with the goal of eradicating

computer security threats and helping to build next generation platform security in the Windows operating system. Prior to joining Microsoft, from 2007 to 2012, I was employed in various engineering capacities at Symantec Corporation, most recently as a Principal Software Engineer. At Symantec, I was responsible for identifying and responding to new security threats, exploits, and malware. I researched and analyzed the latest techniques used by cyber-attackers and reverse engineered complex malware circulating on the Internet. Additionally, I conducted laboratory-based research to build new systems and to develop new tools and defenses to effectively respond to threats. A true and correct copy of my current C.V. is attached hereto as **Exhibit 1**.

B. Overview Of My Investigation Into Ramnit And My Top Conclusions

3. My declaration concerns a botnet referred to as "Ramnit." A botnet is a network of computers connected to the Internet that are infected with malicious software ("malware"). The malware gives the individuals propagating the botnet—the Defendants in this matter—control of the infected computers, and they typically exploit that control for illegal activity. A botnet may consist of a few hundred, tens of thousands, or even millions of infected computers. Once an individual or organization has created a large-scale botnet, they can use its massive infrastructure to engage in malicious activity, such as stealing financial credentials, stealing personal identifying information, stealing confidential data, remotely controlling other computers, or anonymously conducting other illegal activity or technical attacks. Because Ramnit enables Defendants to remotely control infected computers, it is possible for Defendants to engage in a wide range of harmful conduct such as turning on cameras connected to victim computers to eavesdrop on victims, removing files from victim computers, using the victim computers to send electronic communications to others, and stealing contact information for third parties located on infected computers.

4. The Ramnit botnet targets financial institutions and their customers. The operators of the Ramnit botnet use it to monitor the victims' online financial activities; steal the

victims' online account credentials, particularly those used in online banking; and then use that stolen information to steal money from the victim. It is also possible for Defendants to use Ramnit's various modules to spy on victims by, for example, turning on cameras attached to infected computers. Ramnit modules also facilitate identity theft and associated crimes. In this Declaration, I explain how the Ramnit botnet propagates and the manner through which Defendants control it.

5. I joined with other investigators at Microsoft, Symantec, and FS-ISAC to investigate Ramnit. The other investigators with whom I worked are co-declarants in this matter, and I may refer the Court to their declarations for further information on particular aspects of Ramnit. I have reviewed the declarations of these individuals and agree with their conclusions. These investigators are the following:

a. Tim Liu is an Anti-Virus Researcher in the Malware Protection Center of Microsoft. Mr. Liu's declaration describes the internal functioning of Ramnit and how it harms both the user of the infected computer and the infected computer itself.

b. Jason Lyons is a Senior Manager of Investigations in the Digital Crimes Unit of Microsoft's Legal and Corporate Affairs Group. Mr. Lyons' declaration addresses Ramnit's self-defense mechanisms and the proposed plan for disabling Ramnit.

c. Vikram Thakur is a Senior Manager with the Security Response Group at Symantec Corporation. Mr. Thakur's declaration describes the history of the propagation of Ramnit as well as technical details of the manner in which Ramnit commits fraud against the computer user and the computer itself.

d. Eric Guerrino is an Executive Vice President of FS-ISAC, Inc., the Financial Services Information Sharing & Analysis Center. Mr. Guerrino's declaration describes the impact of Ramnit and similar financial-fraud botnet on the banking industry.

6. In the course of our investigation, we purposely infected several investigator-controlled computers with Ramnit malware. This placed the computers under the control of the cybercriminals operating the botnet, but allowed us to monitor all of the illicit communications going to and coming from the infected computers, and to analyze the activities of the infected computers. Among other things, we observed the infected computers connect to and receive instructions from the Ramnit botnet's command and control servers, and through this method, we were able to identify by domain name and I.P. address all of the command and control computers used to control Ramnit botnet. Additionally, we carefully analyzed the changes Ramnit makes to Microsoft's operating system and application software during the infection process, and we reverse-engineered the Ramnit malware to determine how it operates. Further, I have reviewed literature published by other well-regarded computer security investigators concerning Ramnit, and their findings have confirmed my own conclusions regarding the Ramnit botnet. Through these and related investigative steps, I have developed detailed information about the size, scope, and illegal activities of the Ramnit botnet.

7. Based on my investigation, I have reached the following conclusions: Ramnit is a targeted botnet that specializes in stealing money from victims engaged in online banking activities; Ramnit's design is modular and is consistent with a trend towards more flexible, targeted malware. It first came to the attention of security researchers around 2010, spread prolifically and infected hundreds of thousands of computers, and was then customized to commit financial fraud. While its operators have thus far primarily targeted banks located in Europe, it also targets financial institutions in the United States. The customers of the banks targeted by Ramnit are spread across the globe, and include many individuals living in the United States.

8. The identity and location of the Defendants who created and operate the Ramnit botnet is currently unknown. However, there is some evidence to suggest that the perpetrators are located in the Eastern Europe.

9. Defendants control the Ramnit botnet through a command and control infrastructure of Internet domains, name servers, and IP addresses that are all maintained on an interconnected network. In sum, my investigation has uncovered what is, in effect, a single Ramnit criminal enterprise, comprised of Defendants who develop and support the Ramnit botnet using infrastructure designed for the purpose of carrying out the botnet functionality.

10. Ramnit inflicts severe damage on individuals whose computers it infects. Once a computer is infected with Ramnit, Defendants can constantly monitor the online banking activities of its unknowing victims. Defendants' primary goal, as made evident by the Ramnit botnet's functionality, is to steal financial account login IDs, passwords, and other personal identifying information, so as to steal the victims' money. In addition, Defendants are able to use the Virtual Network Computing ("VNC") module of the Ramnit malware to monitor and control every aspect of the victim's computer (for example, Defendants could use the VNC module to activate cameras attached to victim computers, download files, and otherwise remotely control infected computers to eavesdrop on victims).

11. Ramnit also severely damages the computers it infects, making low-level changes to the operating system and neutralizing the security features of the computers. It disables the Windows firewall, blocks the computer from getting anti-virus software updates,[1] and it kills any security related process running on the computer that it detects. Ramnit thus not only cripples any security mechanisms that might result in removal of Ramnit from the computer, it also

[1] Anti-virus ("AV") applications must be continually updated with information about malware circulating on the Internet. Most AV applications receive updates by connecting to the website of the AV application's vendor. Ramnit keeps the victim's computer from doing so. As the user's AV application falls further and further out of date, it becomes less and less effective at detecting and blocking newer malware on the Internet thereby exposing victims to further harm.

leaves the victim's computer completely exposed to and defenseless against many other types of malware widely prevalent on the Internet today.

12. Ramnit also inflicts substantial damage on Microsoft and the many financial institutions whose customers Ramnit victimizes and whose products and trademarks Defendants frequently abuse as part of the botnet's fraudulent operations.

C. Outline Of My Declaration

13. In the remainder of this Declaration, I will explain:

a. the organization and structure of the Ramnit botnet;

b. the manner in which Defendants have deployed and operated the Ramnit botnet around the world; and

c. the harm that Ramnit does to the infected computer and the Microsoft software on that computer.

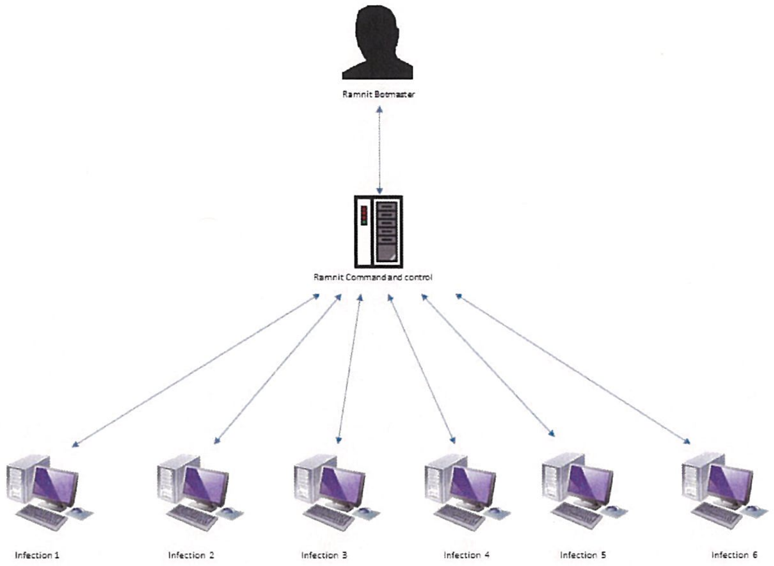
II. RAMNIT—STRUCTURE AND FUNCTION OF AN ILLEGAL BOTNET

A. Overview of Ramnit's Infrastructure

14. Botnets can generally take on one of several structures that allow a single criminal or criminal organization to command and control the vast array of compromised computers in the botnet (known as "bots").

15. Ramnit uses a typical hierarchical, two-tier command and control infrastructure. The first tier is the "Infection Tier." This consists of user computers infected with Ramnit. The second tier is the "Command and Control Tier" that consists of computers Defendants use to control and to maintain the Ramnit botnet. Defendants control the computers and target the users of the computers in the Infection Tier through the servers in the command and control tier. In effect, Defendants hide behind the computers in the command and control tier, which they can locate anywhere in the world and access remotely. The tiered architecture of the Ramnit botnet is represented below in **Figure 1**:

Fig. 1

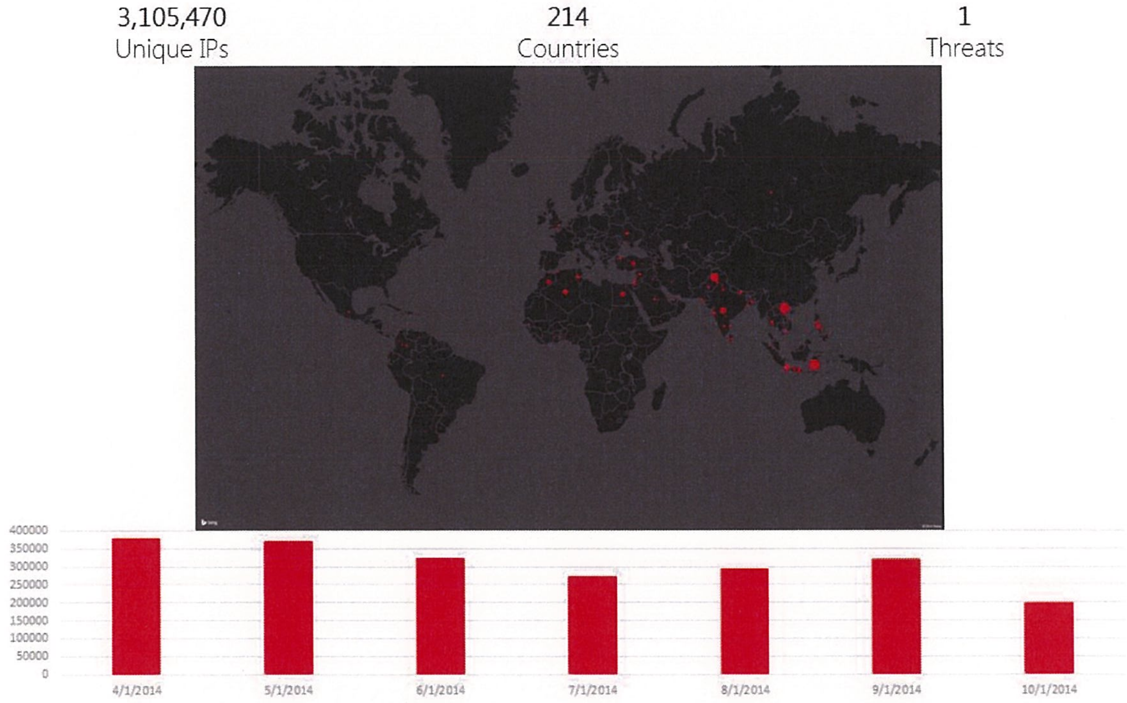


1. The Ramnit Infection Tier

16. The lowest tier, the "Infection Tier" consists of tens of thousands of infected user computers of the type typically found in businesses, living rooms, schools, libraries, and Internet cafes around the world.

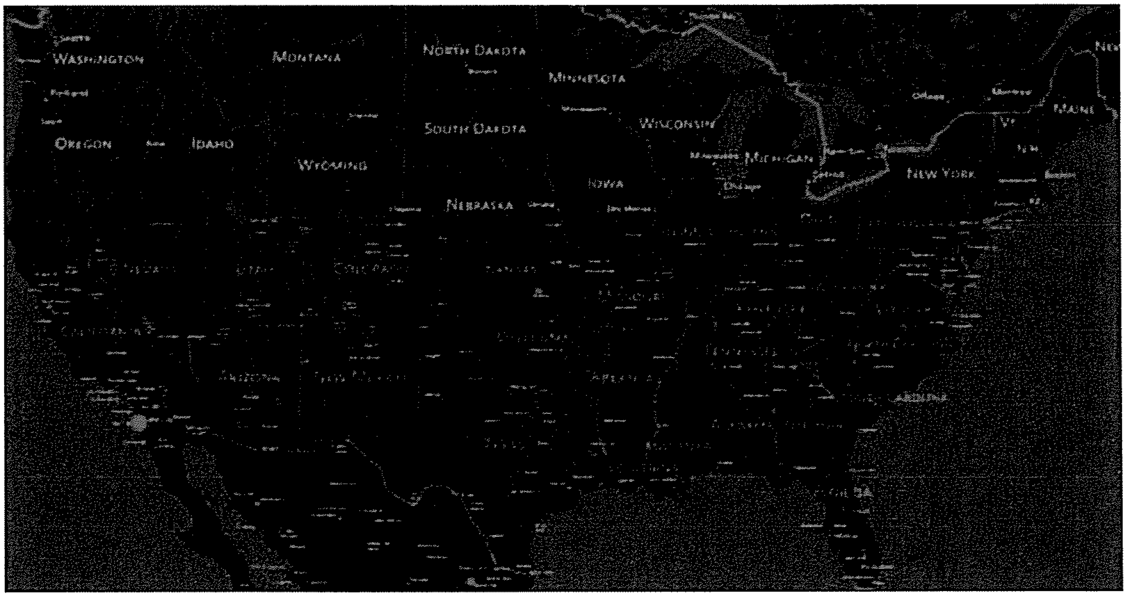
17. In general, Defendants are engaged constantly in infecting additional user computers. In an attempt to counter Defendants' activities, a number of software providers and software security firms are constantly engaged in trying to disinfect those computers. Microsoft has conducted an independent investigation to determine the number of computers infected by Ramnit. Between June and October 2014, Microsoft logged an average of approximate 350,000 Ramnit related encounters each month. A graph of this data is shown in **Figure 2**, below. Over the full course of our monitoring of the Ramnit botnet, Microsoft has traced Ramnit-related encounters to over 3 million unique machines located in 214 countries. This data gives an approximate view of the far-reaching size of the Ramnit botnet.

Fig. 2



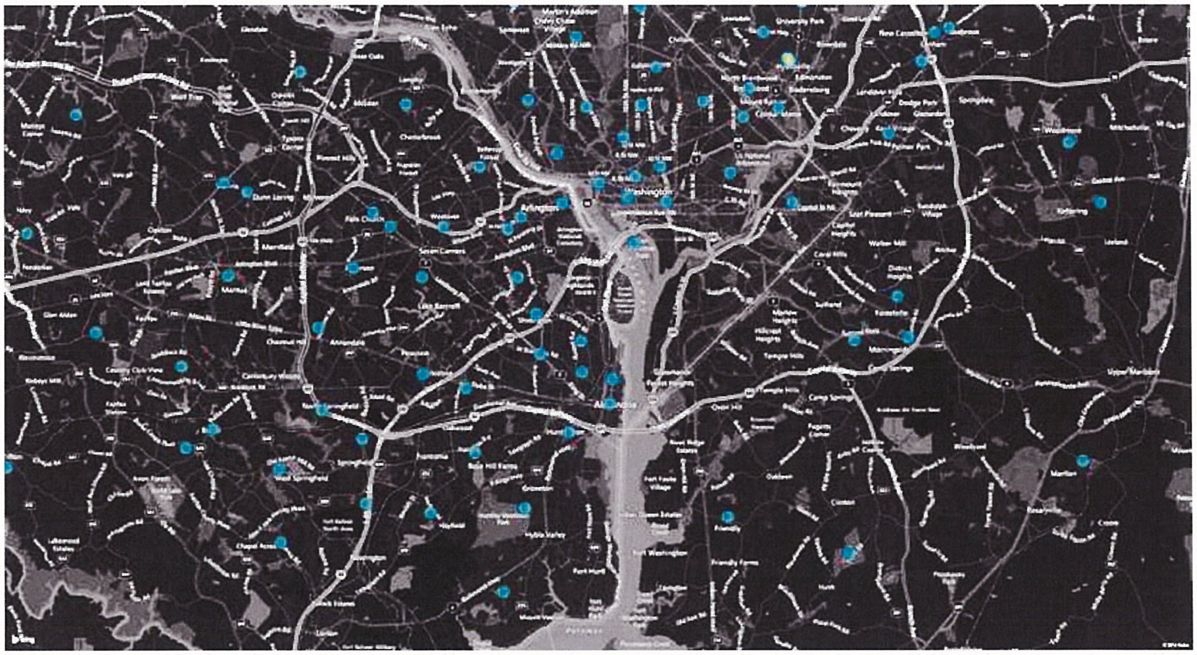
18. Because Defendants have targeted user computers in various states in the United States and in many countries around the world, the Ramnit botnet has global reach. For example, **Figure 3**, below, shows the Ramnit-infected computers that Microsoft has traced to various locations in the United States.

Fig. 3



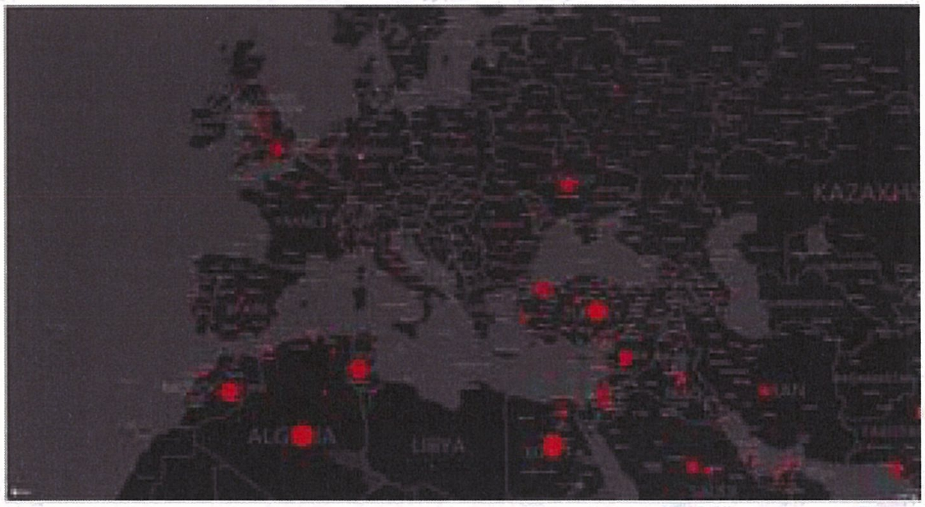
19. **Figure 4**, below, shows the locations of some of the Ramnit-infected computers in the Infection Tier believed to be located in and around the Eastern District of Virginia, based on an analysis of IP addresses through which those computers are connected to the Internet, as uncovered during my investigation.

Fig. 4



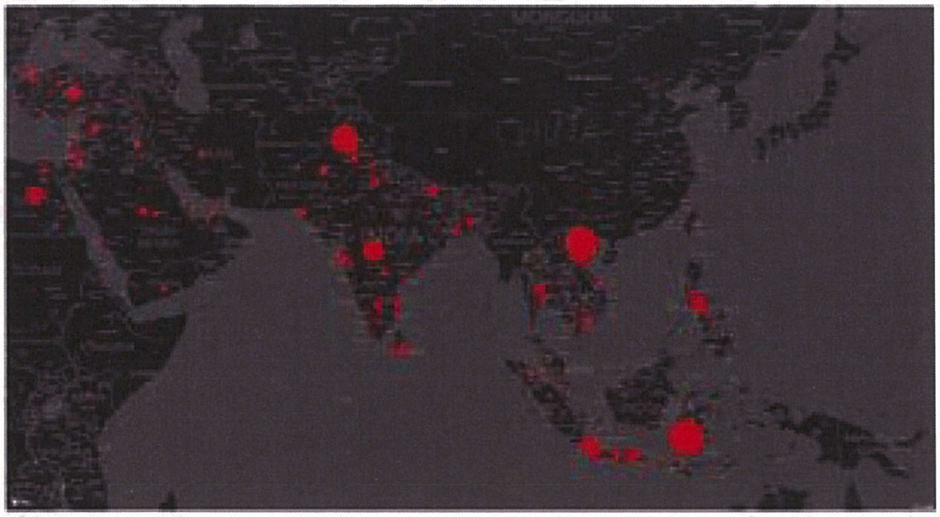
20. Ramnit infections are even more widespread in Europe and other parts of the world. **Figure 5** shows the 25 countries in Europe, Africa, and the Middle East with the highest number of infected computers in the Infection Tier.

Fig. 5



21. **Figure 6**, below, shows the 25 countries in Asia with the highest number of infected computers in the Infection Tier.

Fig. 6



22. Defendants target the owners of computers in the Infection Tier. The daily work of the Ramnit botnet is to access and steal their account credentials and other personal information and ultimately steal money from these individuals' bank accounts.

2. <u>The Ramnit Command And Control Tier</u>

23. The second level of the architecture, the "Command and Control Tier," consists of specialized computers known as servers. Defendants purchase or lease these servers and use them to send commands to control the Ramnit-infected computers in the Infection Tier, to send them additional malware modules that extend the types of fraud the bot can commit, and to receive data stolen from the owners or other users of those infected computers. Defendants set up accounts with web-hosting providers—*i.e.*, companies, usually legitimate, that provide facilities where computers can be connected through high-capacity connections to the Internet and locate their servers in those facilities. By contacting a command and control server, a Ramnit bot can receive updated commands and modules from and communicate with the Defendants.

24. Each Ramnit command and control server is identified by a "domain name." A domain name, commonly thought of as a website name, is an alphanumeric string separated by one or more periods, such as "allbigmoney.net" or "hufqifjq.com." To create an active domain,

Defendants must register the domain name with any one of the many domain name registrars in the world. During the registration process, Defendants must associate the domain name with one or more specific I.P. addresses. The I.P. address can be thought of the physical location on the Internet of the computer that corresponds to that domain name. An "IP address" is a unique string of numbers separated by periods. For example, from July 31, 2014 to present, the domain name hufqifjq.com was associated with the IP address 166.78.62.91.

25. On the Internet, specialized computer servers known as domain name servers maintain tables mapping domain names with IP addresses. For example, if a user's computer attempts to connect to the website "hufqifjq.com," it will first check with a domain name server for the IP address of the computer supporting that website, receive the reply that the computer associated with hufqifjq.com is located at the IP address 166.78.62.91, and then connect to the computer at that address.

26. Defendants control the domains and the IP addresses used to distribute and propagate Ramnit, to receive communications from the Ramnit-infected computers, and to control those same computers. True and correct lists of the Ramnit command and control domains, attached hereto as Appendix A to the Complaint, is attached hereto as **Exhibit 2**. A true and correct list of the Ramnit botnet's command and control IP addresses is listed in **Figure 7 herein.** These command and control servers send the most fundamental instructions, updates, and commands to Ramnit-infected computers. Defendants carry out overall control of the Ramnit botnet through the servers. The relief sought in this case is directed at disabling the Ramnit Command and Control Tier by taking control of these domains and redirecting traffic heading for the IP addresses through which Defendants control the Ramnit botnet.

III. PROPAGATION AND OPERATION OF THE RAMNIT BOTNET

A. Initial Infection

27. I have studied the mechanism Defendants use to infect computers and have concluded that the operators of Ramnit have deployed several of the most common means to

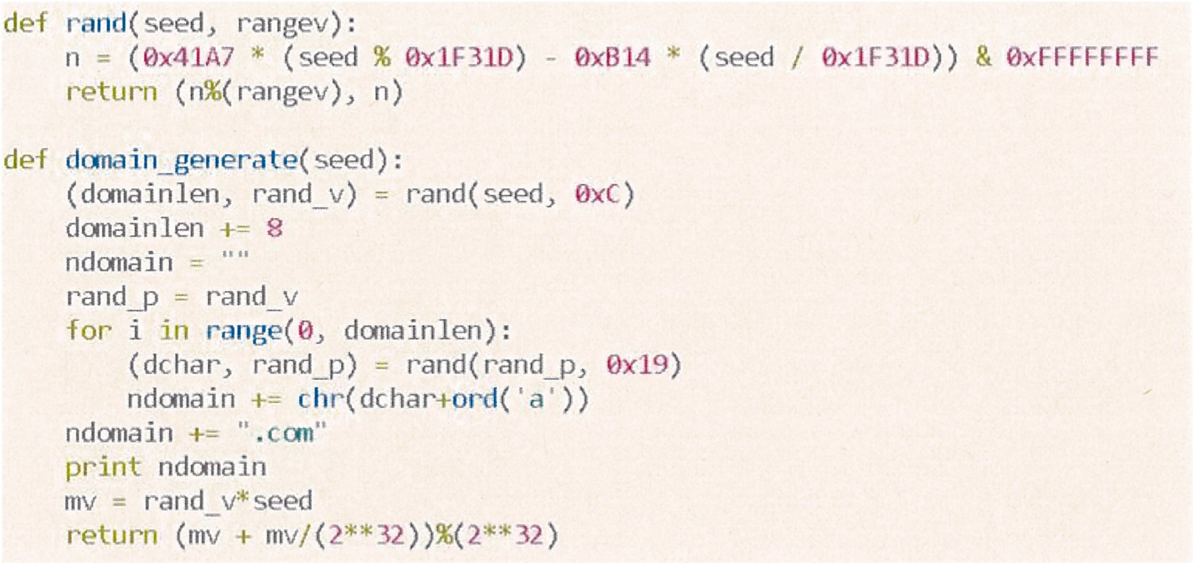
spread Ramnit infections including what are known as "drive-by-downloads," infected portable media such as USB "thumb-drives," or by infecting other clean executable files associated with legitimate software programs.

28. In a drive-by-download infection, a cybercriminal places specialized software known as an "exploit pack" on a website. An exploit pack is software that is designed to infect user computers that connect to the website. These websites are consequently known as "exploit websites." Sometimes exploit websites are created by the botnet operator specifically for the purpose of spreading the infection, but other times they may be normal, legitimate websites that have been hacked by the botnet operator. When a user's computer connects to an exploit website, the exploit pack silently probes the user's computer, looking for unpatched vulnerabilities in the operating system or in third-party applications that would provide an opportunity to infect the computer. If the exploit pack identifies a vulnerability, it downloads and installs the Ramnit malware.[2] From that point forward, Defendants are in control of the user's computer and use it to defraud the user.

B. <u>Connection With The Ramnit Command And Control Tier</u>

29. After Ramnit infects a victim computer, it uses a "domain generation algorithm" ("DGA") to generate a list of possible command and control domains. The Ramnit DGA uses a custom algorithm (based on logic written by Defendants) to create a set of randomized domains. These domain names are nonsensical strings of characters such as "acuhjbadvnmhthwnlxv.com," "bmjvrxrqpkiwdrdv.com," and "exmfhgyv.com." The DGA is depicted in the screencapture bleow:

[2] For further information on how Ramnit uses exploit packs and deceptive techniques, *see New Ramnit variant seeks to evade two-factor authentication*, April 30, 2013, SC Magazine; the April 2, 2103 McAfee article entitled "*What is a 'Drive-by' Download*; the March 26, 2014 Sophos infographic entitled *How Malware Works. Anatomy Of A Drive-by Download Web Attack*; and a January 12, 2012 Contagio blog post entitled *Blackhole Ramnit-Samples and Analysis*. True and correct copies of these articles and documents are attached hereto as **Exhibits 3-6**, respectively.



```
def rand(seed, rangev):
    n = (0x41A7 * (seed % 0x1F31D) - 0xB14 * (seed / 0x1F31D)) & 0xFFFFFFFF
    return (n%(rangev), n)

def domain_generate(seed):
    (domainlen, rand_v) = rand(seed, 0xC)
    domainlen += 8
    ndomain = ""
    rand_p = rand_v
    for i in range(0, domainlen):
        (dchar, rand_p) = rand(rand_p, 0x19)
        ndomain += chr(dchar+ord('a'))
    ndomain += ".com"
    print ndomain
    mv = rand_v*seed
    return (mv + mv/(2**32))%(2**32)
```

Defendants can predict and control the domains generated by the DGA. Current variants of Ramnit generate 300 domain names. Each infected computer uses the same algorithm and starting numeric input, known as the "seed," to generate the exact same list of domain names as every other computer infected with the same variant of Ramnit. As noted above, **Exhibit 2** contains a complete list of Ramnit domain names generated by the currently deployed versions of Ramnit.

30. A newly-infected computer, after it generates the list of 300 potential command and control domains, will next begin to attempt to contact each one in turn over the Internet, and will continue cycling through its list until one of the domains responds authoritatively with a Ramnit-encrypted response. Defendants, of course, have generated the exact same list of domain names as have the infected computers. To communicate with the Ramnit bots, the Defendants need only register at least one of the domains in the list of 300 domains, associating the domain name with a numeric IP address and a command and control computer located at the IP address. Remotely, over the Internet, Defendants can then place further instructions or malware on that command and control computer for the bots to download, and can receive information uploaded

by the bots. **Figure** 7, below, shows the computers currently used (with the associated IP Address) by Defendants in the command and control of the Ramnit botnet.

Fig. 7

<table>
<tr><th colspan="4">Ramnit Command and Control Servers</th></tr>
<tr><th>Domain Names</th><th>IP Addresses</th><th>Physical location</th><th>Purpose</th></tr>
<tr><td>Jhghrlufoh.com
vRnDmDrDrJoFf.com
Nvlyffua.com</td><td>217.23.13.42
95.141.36.218</td><td>Netherlands</td><td>Historical C&C</td></tr>
<tr><td>khllpmpmare.com</td><td>217.23.11.117</td><td>Netherlands</td><td>Current C&C</td></tr>
<tr><td>Ppyblaohb.com</td><td>5.152.205.194</td><td>United Kingdom</td><td>Current C&C</td></tr>
<tr><td>Knpqxlxcwtlvgrdyhd.com</td><td>95.141.36.218 (Current)
93.190.138.126 (Prior)</td><td>Italy</td><td>Backup C&C</td></tr>
<tr><td>Santabellasedra.com</td><td>148.251.35.151 (prior)</td><td>Germany</td><td>Web inject server (prior)</td></tr>
<tr><td>campbrusderapp.com</td><td>5.9.224.198</td><td>Germany</td><td>Web inject server</td></tr>
</table>

IV. RAMNIT DAMAGES ITS VICTIMS IN MULTIPLE WAYS

A. Damage To Computers And Microsoft Software

31. The Ramnit infection itself harms Microsoft and Microsoft's customers by damaging the customers' computers and the software installed on their computers. The Ramnit malware is designed to infect and run on computers equipped with the Windows operating system. The Windows operating system is licensed by Microsoft to its users. Attached hereto as **Exhibit** 7 is a true and correct copy of the Windows 7 end-user license agreement. Attached hereto as **Exhibit 8** is a true and correct copy of the Windows Vista end-user license agreement. Attached hereto as **Exhibit 9** is a true and correct copy of the Windows 8 end-user license agreement.

32. A Ramnit infection begins with the download to the user's computer of the executable files that Ramnit uses to install itself on the computer. The installation of malicious

software in and of itself damages the user's computer and the Windows operating system on the user's computer. During the infection of a user's computer, Ramnit make changes at the deepest and most sensitive levels of the computer's operating system, including the kernel, registry, and system files. One purpose of the changes is to disable Windows security features. The changes include the following:

a. Ramnit injects code into a background process run by Windows called svchost.exe. The Ramnit code kills any anti-virus process that Ramnit detects.

b. Ramnit stops certain security related Windows services, including "ControlService," and "ChangeServiceConfigA."

c. Ramnit makes changes to the Windows registry, which is a repository of information that the operating system depends upon for normal operation. In so doing, Defendants deceptively and improperly leverage registry keys paths bearing "Microsoft," and "Windows" trademarks within the Windows operating system. These changes are the following:

   i. Ramnit resets the "EnableLUA" value to "0" under key HKLM\Software\Microsoft\Windows\CurrentVersion\policies\system.

   ii. Ramnit resets the value of the following keys to "1" under key HKLM\SOFTWARE\Microsoft\Security Center: AntiVirusOverride, AntiVirusDisableNotify, FirewallDisableNotify, FirewallOverride, UpdatesDisableNotify, UacDisableNotify, AntiVirusOverride, AntiVirusDisableNotify, FirewallDisableNotify, FirewallOverride, UpdatesDisableNotify, UacDisableNotify.

   iii. Ramnit resets the "Start" value to "4" under the HKLM\SYSTEM\CurrentControlSet\Services\wscsvc key.

iv. Ramnit resets the “EnableFirewall” value to “0” under the key HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile. This change disables the user’s firewall.

v. Ramnit resets the “Start” value to “4” under the HKLM\SYSTEM\ControlSet001\Services\wscsvc key.

vi. Ramnit resets the "Start" value to “4" under the HKLM\SYSTEM\ControlSet001\Services\wuauserv key.

vii. Ramnit resets the “Start” value to “4” under the HKLM\SYSTEM\CurrentControlSet\Services\WinDefend key.

viii. Ramnit deletes the SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Windows Defender key.

33. Microsoft’s customers whose computers are infected with Ramnit are damaged by these changes to Windows, which alter the normal and approved settings and functions of the user’s operating system, place hooks into the operating system so Ramnit can hide its presence and activities, destabilize it, and forcibly conscript the computer into the botnet.

34. In effect, once infected, altered and controlled by Ramnit, the Windows operating system and Internet Explorer browser cease to operate normally and become tools for Defendants to conduct their theft. Yet they still bear the Microsoft Windows and Internet Explorer trademarks. This is obviously meant to and does mislead Microsoft’s customers, and it causes extreme damage to Microsoft’s brands and trademarks.

35. Customers are usually unaware of the fact that their computers are infected and have become part of the Ramnit botnet. Even if aware of the infection, they often lack the technical resources or skills to resolve the problem, allowing their computers to be misused indefinitely, as manual steps to remove the malicious software may be difficult for ordinary users.

36. In one instance, **Exhibit 10**, even though Microsoft Security Essentials has detected that the user is infected with Ramnit, the user is still urged to change all of his or her online passwords as a security precaution.

37. In a second instance, **Exhibit 11**, a user discusses the problems caused by Ramnit and the need to reformat his entire computer to remove the infection. Similarly, in another instance, **Exhibit 12,** a user discusses the inability of their anti-virus software to eliminate Ramnit and the potential loss of data from the user's hardware.

38. In another case, **Exhibit 13**, the user finds that his Windows Security Center will not launch, and that he can't download or upload anything as a result of a Ramnit infection.

39. In **Exhibit 14**, an unfortunate user finds he cannot turn his firewall on, but that his anti-virus scans report that there is no malware on his computer. After a complex series of communications and procedures over 4 days, the user determines that his computer is infected with Ramnit.

40. And as a final example, in **Exhibit 15**, an article discusses the complex process for removing Ramnit and its infection of over 4,300 files on a user computer.

41. In my experience, these customers were relatively sophisticated in that they were able to detect a problem in the first place, and in that they also know how to report their problems and follow relatively complex instructions to fix their computers. Most victims of Ramnit will never learn that they are infected, or, if they do determine that, will have a very difficult time in removing the infection and in restoring the security features of their computers.

42. Even with professional assistance, cleaning an infected user computer can be exceedingly difficult, time-consuming, and frustrating. Microsoft, other security companies, members of the public generally must invest considerable time and resources investigating and remediating the Defendants' intrusion into these computers.

B. Ramnit Damages Microsoft's Reputation, Brands, And Goodwill

43. Ramnit irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows® operating system, and Internet Explorer®, and a variety of other software and services. Trademark registrations for marks infringed by Defendants are attached to Plaintiffs' Complaint as **Appendix B**. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditures of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Windows and Internet Explorer.

44. The activities of Ramnit injure Microsoft and its reputation, brand, and good will because users subject to the negative effects of these malicious applications incorrectly believe that Microsoft, Windows, Microsoft Security Essentials, Windows Security Center service, or Internet Explorer, are the sources of their computer problems. As explained above, because of Ramnit, users of infected computers will experience degraded computer performance. There is a great risk that users may attribute this problem to Microsoft and associate these problems with Microsoft's Windows products, thereby diluting and tarnishing the value of these trademarks and brands.

45. To carry out the intrusion into user computers, Defendants cause the Ramnit command and control servers to make repeated copies of Microsoft's trademarks onto user computers, in the form of file names, domain names, target names and/or registry paths containing the trademarks "Windows," and "Live." These uses of Microsoft's trademarks are designed to cause the intrusion into the user's computer and to confuse the user into believing that the software installed is a legitimate part of the Windows operating system, when it is not.

46. Based on my experience assessing computer threats and the impact on business, I conclude that customers may, and often do, incorrectly attribute to Microsoft the negative impact of Ramnit and other malware downloaded to their computers as a result of having their browsers hijacked and redirected to malware download sites. Further, based on my experience, I conclude that there is a serious risk that customers may move from Microsoft's products and services because of such activities. Further, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks.

47. Microsoft devotes significant computing and human resources to combating Ramnit and other malware infections and helping customers determine whether or not their computers are infected, and if so, cleaning them. Not only does Microsoft expend resources in helping users combat Ramnit, these efforts require in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft's customers. Microsoft, as a provider of the Windows operating system and Internet Explorer web browser, must also incorporate security features in an attempt to stop account credential theft by the Ramnit botnet from occurring to customers using Microsoft's software.

C. <u>The Ramnit Botnet Causes Severe Injury To Third Parties And The Public</u>

48. As set forth more fully in the declaration of Eric Guerrino, the Ramnit botnet causes injury to numerous financial institutions, the trade groups that represent their cybersecurity-related interests, including FS-ISAC, and the individual account holder victims whose information and funds are stolen.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 19th day of February, 2015, in Washington, D.C.

02/19/2015

Karthik Selvaraj

Karthik Selvaraj
Senior Anti-Virus Researcher/Strategist,
Microsoft Corporation,
USA

Employment history

- Currently Employed with Microsoft Corporation, Redmond, USA (Oct 2012 to Present)
- Worked with Symantec Corporation, Culver City, USA (Oct 2009 to Sep 2012)
- Worked with Symantec Corporation, Pune, India (Feb 2007 to Oct 2009).
- Worked with Wipro Technologies, Pune, India (July 2004 to Feb 2007).

During which he act(ed) as,
- Senior Anti-virus Researcher / Strategist in Microsoft Malware protection Center, Microsoft USA.
- Principal Security Research Engineer in Security Response team, Symantec USA.
- Senior Security Research Engineer in Security Response team, Symantec USA.
- Senior Security Research Engineer in Security Response team, Symantec India.
- Senior Software Engineer & Project Engineer in Core OS team of WindRiver ODC.
- Senior Software Engineer for VxWorks in Panasonic ODC.

Current Role:

As Senior Anti-virus Researcher in Microsoft Malware protection center, Mr. Selvaraj is responsible for identifying & building protection technology to computer security threats and exploits in the field by conducting laboratory-based research by applying deep understanding of operating systems, network communications, cryptography and reverse engineering skills.

He also plays an important role as a Strategist for Microsoft malware protection center, Redmond Operations. Principal responsibility is to provide strategic direction for the security research team with the goal of eradicating computer security threats and help build next generation platform security in the Operating system.

Past Security Research Experience:

From February 2007 until December 2008, Mr. Selvaraj was employed as a Software Engineer at Symantec Corporation. In this role, he functioned as a member of the technical staff in the Symantec Security Response Team. Mr. Selvaraj reverse engineered software applications to identify malware code predominantly found on the Win32 platform. He used C++ for algorithmic generic detection of malware; performed x86, ARM, and MIPS assembly/disassembly programming to reverse engineer programs in those platforms; and wrote IDA scripts and plugins to analyze malware on virtualization platforms such as VMware and virtual pc. He also used Python scripting to automate aspects of malware analysis and reverse engineering. Mr. Selvaraj performed active debugging of threats using WinDbg and OllyDbg.

From January 2009 to July 2012, Mr. Selvaraj was employed as a Senior Software Engineer at Symantec Corporation. As a senior member of the Symantec Security Response Team, Mr. Selvaraj analyzed complex malware and developed defenses to protect against threats. He used C++ for algorithmic generic detection of malware, and also used C++ to write static unpackers, file-format parsers, scanners, internal analyst tools, and customer fixtools. He wrote custom emulators and parser tools using x86, ARM, and MIPS assembly/disassembly to assist reverse engineering and to analyze the malware; applied his understanding of virtualization platforms to identify VM detection and anti-VM tricks employed by malware; and wrote IDA scripts and plugins to analyze malware. He also conducted Python scripting to automate aspects of malware analysis and reverse engineering and performed active debugging of threats using WinDbg and OllyDbg. In addition, Mr. Selvaraj helped junior members of the Symantec Security Response Team with malware analysis and provided technical assistance with evaluating work created by others.

From July 2012 to September 2012, Mr. Selvaraj was employed as a Principal Software Engineer. In this role, he was responsible for identifying and responding to new security threats and exploits. He also conducted laboratory-based research to build new systems and to develop new tools to effectively respond to threats. Mr. Selvaraj created anti-virus signatures, definitions, and rule sets to update Symantec security products. He also distributed defenses and performed research into the latest techniques used by attackers. Mr. Selvaraj used C++ for algorithmic generic detection of malware, and also used C++ to write static unpackers, file-format parsers, scanners, internal analyst tools, and customer fixtools. He wrote custom emulators and parser tools using x86, ARM, and MIPS assembly/disassembly to assist reverse engineering and to analyze the malware; applied his understanding of virtualization platforms to identify VM detection and anti-VM tricks employed by malware; and wrote IDA scripts and plugins to analyze malware. He also conducted Python scripting to automate aspects of malware analysis and reverse engineering and performed active debugging of threats using WinDbg and OllyDbg. In addition, Mr. Selvaraj mentored and provided technical direction to new analysts regarding security threat issues.

During this entire period, Mr. Selvaraj gained computer malware reverse engineering experience. He also gained experience with C++; x86, ARM, and MIPS assembly level programming; IDA scripting and plugin development; scripting; virtualization platforms; Win32; and WinDbg and OllyDbg.

Achievements & Awards:

- Wrote a paper on "The Rise of *PDF* Malware" (Yr 2010)
- Was instrumental in setting up Anti-virus team in India, includes training India team and setting operations for proactive threat coverage & threat intelligence.
- Was a Trainer for CERT India in Reverse engineering & Malware Analysis at Symantec, Pune.
- Presented paper "Malware & Rogue, and attractive business model" at Cutting Edge 2008, Salt Lake City, Utah.
- Received 'Standing Ovation' Award for outstanding work in Advanced Malware Heuristics, Symantec. (Yr 2008)
- Received "A++" Award for outstanding work & technical contribution to team, Symantec. (Yr 2008)
- Received "A++" Award for outstanding work in setting up Spyware operations in Symantec security response, India. (Yr 2007)

APPENDIX A

REGISTRY FOR .COM DOMAINS

Verisign Naming Services
21345 Ridgetop Circle
4th Floor
Dulles, Virginia 20166
United States

Verisign Global Registry Services
12061 Bluemont Way
Reston Virginia 20190
United States

CURRENTLY REGISTERED .COM DOMAINS

anxsmqyfy.com
campbrusderapp.com
jhghrlufoh.com
khllpmpmare.com
knpqxlxcwtlvgrdyhd.com
nvlyffua.com
ppyblaohb.com
riaaiysk.com
santabellasedra.com
tqjhvylf.com
vrndmdrdrjoff.com

DEFENDANTS JOHN DOES 1 – 3 CONTACT INFORMATION

caewoodydr@uymail.com
campmorgenapp@arcticmail.com
carmiller@mail.com
redswoodster@engineer.com
gromsmoothe@arcticmail.com

UNREGISTERED .COM BACKUP DOMAINS GENERATED BY BOTNET

acuhjbadvnmhthwnlxv.com
advvpbrtyw.com
aflgqgddfi.com
apbhwiohxqbvoxlumdh.com
apkdwbwdpickk.com
aprocqhqmmkl.com
asdldoqoolcgm.com
aufdloglxlqoxxlepp.com
avxvatwmxwbyiepwmwo.com
ayketyjlsaeu.com
bltolwbwychlyt.com
bmaucdrfpmnh.com
bmjjksysowdwmoy.com
bmjvrxrqpkiwdrdv.com
bpiwebgqddyvgcnjgh.com
briujbxmkjeusvslrln.com
bseboouatanfddgbrdv.com
bvqdvfihwnaja.com

cbxyvrxewvlnxhkadfg.com
ccylbclg.com
cgwootylkoyxe.com
cjagpjgd.com
ckgvnbwdywbxvlnk.com
clkcdjjmyylwib.com
cqvylephudwsuqjhge.com
croxxnrtvrqt.com
cuhbjlgw.com
cyanlvwkuatvmw.com
dbygksqtu.com
dfalxqubjhl.com
dfvxuvljbykia.com
dhfejwhoj.com
dledwgrxiiqspx.com
dnqjposxrclhqplwli.com
duhjqituiokycypi.com
dwbdecmppklvbevtjq.com
dwksmbrq.com
dxktegertgbgeeoi.com
dxxteubknwecsdutlp.com
ealxbraobohxb.com
ebrfoyrs.com
ecsgmpariu.com
edvxemrsvvycwt.com
egopuefrdsefc.com
eipvatwwexl.com
ejfrcfwdbsaahtdt.com
emlxeyirx.com
emxwjwdcb.com
ersbvvdxamjotwpm.com
etjdsnjpvb.com
euvyalbkwahxxjn.com
evrlsscrxvmd.com
exmfhgyv.com
eyvvpstmcwwvsyjtif.com
facmttijcdq.com
fgcdhqgcdomle.com
fijdmkqvralmgorinlc.com
fkcfkcygpldjcr.com
fmdjnmskmjhjq.com
fmjboahxkasxdl.com
fmqegimr.com
fsxgwfwychumrgrmhwo.com
fuogcmhewqer.com
fvkcrcflhy.com
fxngienbgebck.com
fycecyuksgjfxy.com
gaqqerty.com
gbcpynphvropsyu.com
gdekatkjjihi.com
gmsxrgagrfgivh.com
gqnoupteuivrwte.com
grbfrnxxej.com
gtiswnukb.com
guifymdmxj.com
gunqwxgyrl.com
gwmjxjueqme.com
gwnppapgwhntidegx.com
hajqfvvqjkkaejwi.com
hjahmduyebf.com
hjvlshecwshpfxwfl.com
hllcololi.com
hllnakmxmgoyh.com
hlrsxjdakvl.com
hoeqosqeicddv.com
hqskceeltysbbnc.com
hvklxvhkmfsdgd.com
hvyfjjqdlwhnlrpaa.com
hwruujnk.com
ibvtknxochoyjidm.com
icqxkusbfdwhy.com
ifbomanec.com
ijfwbyvcirepgd.com
ikkjjgbqgts.com
ilpvrpxwfauqaxyq.com
imvfakaudq.com
iqhafgpvsrj.com
ixwnsfmyg.com
iylelocfjsj.com
jherkljjcsloepd.com
jhfykbugtthmdkgga.com
jhrqfnrlpyvo.com
jjdvasey.com
jkgvbneenmrbklortr.com
jkyyolccxfy.com
jmesrbwtcjev.com
jmmurxyktxvegsxid.com
jnjjlojgnvxesr.com
jvmckcospyqedcsjny.com
jycxmcdof.com
jymqfxgwfhyns.com

kavkwpjdndsk.com
kcilhmepervm.com
kdjsnsre.com
kdkdpwql.com
kjpsjoxqsutgewlrah.com
kuwkdqstblavept.com
kvcovjrpsb.com
kvfkfxakmqoof.com
kynknfyngikfno.com
kyskhoopsmkbmenau.com
labxpyvjtwuiijwghie.com
lcqavndroo.com
lehmgspxp.com
liedjckipkehqxwtdl.com
llgnygbqhv.com
llurxdkpkbvjx.com
lorwmtrf.com
lpivbutq.com
lpvdauemfexnvoyh.com
lsvnoumbqcsjl.com
ltrpfybf.com
luvrqdhavhxcbtc.com
lvqdhrqhfxlsglkf.com
lvrjjmbdtfapwev.com
lwnggpwijlvyagmu.com
lybfxrtkcdkbbqr.com
lyftposyknpigp.com
lyvxrtpkchmddb.com
lyxbotuappfreadkfk.com
mbpnjenhxgcimx.com
mchpmdywgs.com
mfnaqngqorgbxbnsc.com
mhuvivlyndmsx.com
mioqhqvmduqicvoey.com
mkdnthyiqlq.com
mktxegrucbkv.com
mlgdwljfmnkt.com
mqojcxmnnxy.com
muabyljiutasgqjedl.com
mxgainbmtvariv.com
myhyfpuoh.com
myqenkelfk.com
nbkqygsfvri.com
nfbodxdevgpjba.com
nfqhufvxyssyda.com
nglqogrh.com
nhcdrnwpsasnaar.com
nqgsmrbkwvnifdyost.com
nqnyteqxqgqohvco.com
ntikqcjtehpvih.com
nvgmdyabspq.com
nwuqfobauuwsyuppii.com
nxhdmugxeiht.com
nxlakdliamyuejsss.com
nxxuwtws.com
ocvqccdhenkjs.com
odcenmfimwibhrfvxxy.com
oexdjxjdoiplmxfybbm.com
ogfavxwxus.com
ogmwrgryk.com
okfatclblpl.com
ootuuujaep.com
optiidevdabtlewjd.com
otdvlbjeucwyqkfbn.com
ovhlfqcpfxoyjgjb.com
ovtindng.com
ovypjimjcnvwwooiamj.com
owerubvhcinavarinm.com
oyuqibrjowbfmvj.com
oyxmxbsppuucbtiwm.com
pacffcnx.com
pbdlsfkjrxclqjo.com
pgnpuktvbnmrybjsv.com
pgtujjyovgffyfrn.com
pnfnkahiocdseewyen.com
ppvrnfkbarbnlm.com
ptvaolhg.com
pxjjwmhlmptbsvhuq.com
qdboaveuhwabhwik.com
qglhlsyskvufb.com
qhnhlgmfepeuelxtpkv.com
qiisbgyqkrokokwrbq.com
qnyyirhtuautt.com
qpfrvbstn.com
qtyvbditfgmkxqjrik.com
qvberjspofqsxdnr.com
qwmqyrcvkseynvrgdnv.com
qxqkdvwayhengjqm.com
qyuylvjwh.com
repliinjqssbrnf.com
rgrtvwsmalhmx.com
rijfxtotkuysyfh.com

rjbejalpcsghdm.com
rmdmqetbpbpgpufhql.com
rmjkunxkbcrsltbc.com
rrewytfucjjylju.com
rwcdljyemxplouufjvd.com
sblbtuqtiavvtrkrn.com
sbpvpkuwoxevjiy.com
scfxvdlmfbgf.com
sdjvmbngpgwnpdj.com
shnlojyteeocltymxe.com
slvmktdpxdd.com
smisifkrfkyccnlk.com
snpryjitnos.com
srjkrxvxmkuql.com
srvmkdeaerccaffs.com
ssclrhiimfeodm.com
sthspflawbhacxp.com
tbajypaiecloxihf.com
tjslktadkjklb.com
tnqtdfodepctna.com
todyennhm.com
twwrktawwgpito.com
typmyloijdcxtdxd.com
ucfenxbryboqwbmlxke.com
udiivoyrbugyfruq.com
uehhvrdnuc.com
ugkrxtjrlfbxmakmt.com
uoidxmhugvidc.com
upnsdndflqokigybdr.com
uuofllccd.com
uvkejdrigublblsst.com
vcssgidqhxkar.com
vdbtvdpujtfhwa.com
vefqierywsov.com
veymnlvyoknk.com
vffamysgsfsodw.com
vfrpojablskkqrx.com
vilapacdnnodhsehneh.com
vlglwuyqoxjn.com
vpwxxqwcnvdrxpc.com
vrvfonqdkfjo.com
vwlcnujosuovul.com
wacwpxqx.com
wehtwbqu.com
wgvmlfyygec.com
wjpsxawqxomokepfbw.com

wknfjeopkdj.com
wldlrwlygck.com
wnftxxhnwiugtvwyo.com
wvmmvpbkjrds.com
wxkeojjdshd.com
wxxnufbeacmrtdam.com
xbjersli.com
xcpvexsyqjsf.com
xdtfqohfbskcgxameg.com
xdyowsheht.com
xirrjlpllrcosfqsf.com
xktepjxakoyq.com
xlqaburwns.com
xmlonthptunynnxf.com
xnttexmtc.com
xoqxabqb.com
xrtgqevawtlmulghjj.com
xsmympdmnacrqxkdb.com
xtbwxayxxvqpspo.com
xuajockq.com
ybgpdikdudmdfr.com
ycafyovxdnlsa.com
ycmusvulvknohnbwhvp.com
yctgocejemh.com
yctkhjksne.com
ycvmwjae.com
ydgsadpgvne.com
yembvgbgmdipfwjmd.com
yovkoaxsana.com
yoxbjnpkmkjirj.com
yxiibnav.com
yxkhvhehtjfoqrnedi.com
yytbonkxjwy.com

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

- SC US
- SC UK

Former CBS reporter claims gov't hacked computer

United notifies members of access gained to accounts

Reboot takes a look at the past, present and future of security.

Danielle Walker, Senior Reporter
Follow @daniellewlkr

April 30, 2013

New Ramnit variant seeks to evade two-factor authentication

Share this article:

- facebook
- twitter
- linkedin
- google

Once a persistent worm, Ramnit has evolved into a banking trojan capable of injecting victims' web browsers to conduct and conceal fraudulent wire transfers.

The variant uses HTML injection to display subtle changes in banking sites with the hopes of luring users into revealing their one-time passwords (OTP), an addit authentication that is valid for only one login session, according to new findings from security firm Trusteer.

The Ramnit worm was discovered in 2010, but in 2011 researchers spotted a new strain that had incorporated source code from the notorious Zeus banking trojan. rchers now classify Ramnit as financial malware.

The fresh variant, which has been targeting banks in the U.K. over the last couple of weeks, waits until users login to their bank accounts before launching the OTP scam, according to Etay Maor, fraud prevention solutions manager at Trusteer.

×

Next Article in News

News briefs: Malware cripples South

Victims see a message that they need to configure their OTP service with their bank, while Ramnit initiates a wire transfer to fraudsters without the victim noticing. The user receives the one-time password via SMS, and once they enter it into the web page, Ramnit uses the password to complete the wire transfer to a "money mule" account.

In a Tuesday interview, Maor told SCMagazine.com that Ramnit's browser injection feature is a significant development.

“It's changing the HTML that the user sees,” Maor said. “Why try to hack a bank website that's super secure, when you can attack the victim's computer, which is pretty easy?”

So far, fewer than 10 banks have been targeted in the U.K., Maor said. The malware is still being analyzed, but Maor added that attackers are likely delivering Ramnit to victims via drive-by download, in which they are unknowingly infected simply by visiting a website.

In one incident, Ramnit attackers went as far as to inject their own text into a banking site's "FAQ" section, in case users sought to learn more information about how OTP works.

“The malware uses the same idea of injection [for the] FAQ section," Maor said. "I've never seen so much attention to detail. Usually [fraudsters] are just worried about getting all the information from the user, not covering all the other things."

0
Share this article:

- facebook
- twitter
- linkedin
- google

You must be a registered member of SC Magazine to post a comment.
Click here to login | Click here to register

×

Next Article in News

News briefs: Malware cripples South

How Do I Defend Against Threats in the Latest McAfee Labs Report?

McAfee Labs provides important information about threats in a variety of ways, from our McAfee Global Threat Intelligence service that feeds into many of our products, to published Threat Reports, our...

Read More | All Posts in Business

Cybersecurity and The State of the Union
Executive Perspectives

Don't Believe These 6 Mobile Security Myths
Consumer

How Do I Defend Against Threats in the Latest McAfee Labs Report?
Business

At Intel Security, Protecting Customers Takes Precedence
McAfee Labs

Consumer, Family Safety, Identity Protection, Mobile Security

What is a "Drive-By" Download?

By Robert Siciliano on Apr 02, 2013

Like 8 Share 14 g+1 3 Tweet 2

Gone are the days when you had to click to "accept" a download or install a software update in order to become infected. Now, just opening a compromised web page could allow dangerous code to install on your device.

You just need to visit or "drive by" a web page, without stopping to click or accept any software, and the malicious code can download in the background to your device. A drive-by download refers to the unintentional download of a virus or malicious software (malware) onto your computer or mobile device.

A drive-by download will usually take advantage of (or "exploit") a browser, app, or operating system that is out of date and has a security flaw. This initial code that is downloaded is often very small (so you probably wouldn't notice it), since its job is often simply to contact another computer where it can pull down the rest of the code on to your smartphone, tablet, or computer. Often, a web page will contain several different types of malicious code, in hopes that one of them will match a weakness on your computer.

These downloads may be placed on otherwise innocent and normal-looking websites. You might receive a link in an email, text message, or social media post that tells you to look at something interesting on a site. When you open the page, while you are enjoying the article or cartoon, the download is installing on your computer.

Security researchers detect drive-by downloads by keeping track of web addresses that they know have a history of malicious or suspicious behavior, and by using crawlers to wander the Web and visit different pages. If a web page initiates a download on a test computer, the site is given a risky reputation. Links in spam messages and other communications can also be used as source lists for these tests.

The best advice I can share about avoiding drive-by downloads is to avoid visiting websites that could be considered dangerous or malicious. This includes adult content, and file-sharing websites. Some other tips to stay protected include:

- Keep your Internet browser, and operating system up to date
- Use a safe search tool that warns you when you navigate to a malicious site
- Use comprehensive security software on all your devices, like McAfee All Access, and keep it up to date

Robert Siciliano is an Online Security Expert to McAfee. He is the author of 99 Things You Wish You Knew Before Your Mobile was Hacked! (Disclosures)

Tags: cybercrime, identity theft, malware

Like 8 Share 14 g+1 3 Tweet 2

No Comments

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment

Privacy & Te

Post Comment

Top 10 Trending Tags

online safety
cybercrime
malware
mobile security
endpoint protection
identity theft
computer security
protecting kids online
network security
email and web security

Intel Security on Twitter

IntelSecurity Attending #VMwarePEX next week? We've got a plethora of demos and giveaways going on at our booth, 421. Be sure to stop by!
18 mins ago·Reply·Retweet·Favorite

IntelSecurity Last week, cybersecurity took the stage at the #SOTU. Find out what @youngdchris and others had to say about it: http://t.co/gX0Q7TxD4e

1 hour ago·Reply·Retweet·Favorite

Follow @IntelSecurity

Also Find Us On

Meet the Bloggers

McAfee Labs

Consumer

Business

Executive Perspectives

About Subscribe Contact & Media Requests Privacy Policy Legal

SOPHOS

PRODUCTS LABS PARTNERS COMPANY SUPPORT

Enduser Network Server SophosLabs Partners

How malware works: Anatomy of a drive-by download web attack (Infographic)

26-03-2014 / John Zorabedian

NETWORK **SECURITY TIPS** ***Tags:*** *malware* , *UTM* , *Web*

We'd like to show you in visual format how a web attack works. As you can see in the infographic below, a web attack happens in five stages, and this whole process takes less than a second.

The web is the number one source of malware (a term that combines "malicious" and "software"), and the majority of these malware threats come from what is called a **drive-by download**.

5 Stages of a Web Attack

The term drive-by download describes how malware can infect your computer simply by visiting a website that is running malicious code (Stage 1: **entry point**).

Most of the time, these are legitimate websites that have been compromised to redirect you to another site controlled by the hackers (Stage 2: **distribution**).

Today's cybercriminals use sophisticated malware packaged in an "exploit kit" that can find a vulnerability in your software among thousands of possibilities.

When your browser is redirected to the site hosting an exploit kit, it probes your operating system, web browser and other software (such as your PDF reader or video player) to find a security vulnerability that it can attack (Stage 3: **exploit**).

Remember — if you are not applying security updates to your operating system and software, you are unprotected against these exploits.

Once the exploit kit has identified a vulnerability, that is where Stage 4: **infection** begins. In the infection phase of an attack, the exploit kit downloads what is known as a "payload," which is the malware that installs itself on your computer.

Finally, in Stage 5: **execution**, the malware does what it was designed to do, which is mainly to make money for its masters.

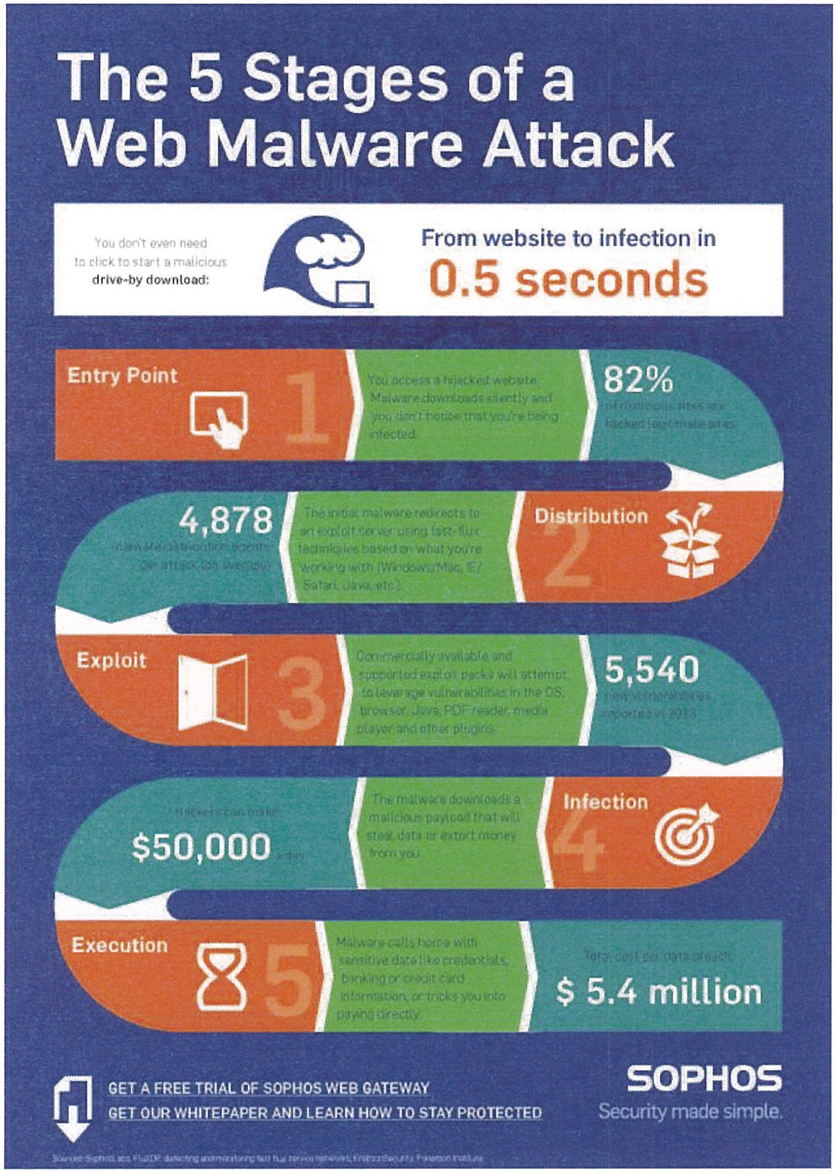
Follow

Follow "Sophos

The malware known as Zbot can access your email or bank accounts. Another type of payload called ransomware can hold your files hostage until you pay to have them released.

○ Follow

Follow "Sophos



The 5 Stages of a Web Malware Attack

You don't even need to click to start a malicious **drive-by download:**

From website to infection in **0.5 seconds**

Entry Point 1

You access a hijacked website. Malware downloads silently and you don't notice that you're being infected.

82% of malicious sites are hacked legitimate sites

Distribution 2

The initial malware redirects to an exploit server using fast-flux techniques based on what you're working with (Windows/Mac, IE/Safari, Java, etc.)

4,878 malware distribution agents per attack (on average)

Exploit 3

Commercially available and supported exploit packs will attempt to leverage vulnerabilities in the OS, browser, Java, PDF reader, media player and other plugins.

5,540 new vulnerabilities reported in 2013

Infection 4

The malware downloads a malicious payload that will steal data or extort money from you.

Hackers can make **$50,000** a day

Execution 5

Malware calls home with sensitive data like credentials, banking or credit card information, or tricks you into paying directly.

Total cost per data breach: **$ 5.4 million**

GET A FREE TRIAL OF SOPHOS WEB GATEWAY

GET OUR WHITEPAPER AND LEARN HOW TO STAY PROTECTED

SOPHOS
Security made simple.

Sources: SophosLabs, FluxDP: detecting and monitoring fast flux service networks, KrebsonSecurity, Ponemon Institute

Secure the Web

Follow

Follow "Sophos

This kind of attack happens all the time. But you don't have to be a victim. Download our checklist of technology, tools and tactics for effective web protection to find out how you can protect your organization from malware attacks at every step of the way. You should also check out our free whitepaper explaining how malware works and offering tips to help you stop it: Five Stages of a Web Malware Attack. (Registration required).

At Sophos, our real-time reputation filtering protects you from newly infected websites as soon as they come online. We do this using our ever-growing, cloud-hosted database of malicious sites, compiled by our global intelligence centers called SophosLabs.

Learn more about how we can secure the web for you.

Share this:

Twitter 40 LinkedIn 49 Facebook 25 Google Email Print More

★ Like

2 bloggers like this.

← How to manage native encryption on Macs and Windows PCs (Video)

Will NSA spying hurt the U.S. tech industry? (Video and Podcast) →

Comments for this thread are now closed.

0 Comments Sophos Blog Login

Sort by Best Share Favorite ★

Subscribe Add Disqus to your site Privacy

Subscribe to our blog

Enter your email address and you'll get a notification when we post something new. Be the first to know what's happening with Sophos!

Follow

Follow "Sophos

Sign me up!

Recent Network Posts

Written By Editor on January 8, 2015 at 9:19 am

5 things you should know about the EU Data Protection Regulation (even if you're not from the EU) »

Written By John Zorabedian on December 18, 2014 at 8:02 am

SophosLabs research spotlights rising threat of Vawtrak financial malware »

Written By Eric Bégoc on December 17, 2014 at 8:43 am

UTM Up2Date 9.305 Released »

Written By Editor on December 12, 2014 at 12:15 pm

The top 6 retail threats and how to stop them »

Written By Editor on December 11, 2014 at 10:54 am

Our top 10 predictions for security threats in 2015 and beyond »

Upcoming EU Data Protection Regulation
See if you are at risk
60 SECOND COMPLIANCE CHECK
SOPHOS
Take test >

Follow

Follow "Sophos

Follow

Follow “Sophos

Follow

Follow "Sophos

Helpful Links

- RSS Feed
- About Us
- Our Products
- SophosLabs
- Get Support
- Free Tools
- Whitepapers

Top Posts & Pages

- 5 things you should know about the EU Data Protection Regulation (even if you're not from the EU)
- Sophos UTM Advantage (9.3) is now available - find out what's new!
- Keep your website secure from exploit kits and hacker attacks (Video)
- UTM Up2Date 9.305 Released
- Next-Generation Enduser Protection – Thinking outside the (sand)box
- Safe Christmas — A security song for the holidays
- How to upgrade your network security with our free firewall
- SophosLabs research spotlights rising threat of Vawtrak financial malware
- Our top 10 predictions for security threats in 2015 and beyond
- UTM Up2Date 9.304 Released

Archives

Select Month

Follow

Follow “Sophos

POPULAR
Free Tools
Whitepapers
Buy Online

COMMUNITY
Social Networks
Naked Security News
Sophos Blog
Podcasts
RSS

WORK WITH US
Become a Partner
Partner Portal (login)
Resellers
Tech Partners
OEM

ABOUT SOPHOS
Jobs/Careers
Feedback
Contact Us
Press

SUPPORT
Knowledgebase
Downloads & Updates
Documentation
Training

Legal Privacy Cookie Information

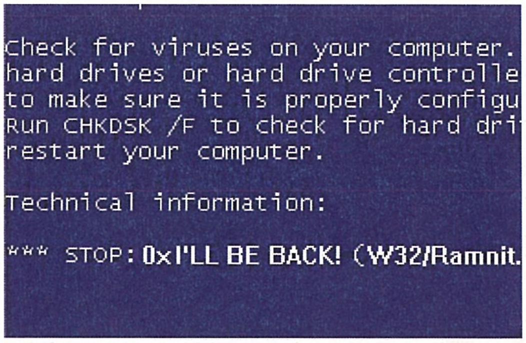
Follow

Follow “Sophos

Home

Thursday, January 12, 2012

Blackhole Ramnit - samples and analysis



```
Check for viruses on your computer.
hard drives or hard drive controlle
to make sure it is properly configu
Run CHKDSK /F to check for hard dri
restart your computer.

Technical information:

*** STOP: 0xI'LL BE BACK! (W32/Ramnit.
```

Ramnit - a Zeus-like trojan/worm/file infector with rootkit capabilities has been in the wild for a long time but recently made news because Seculert reported about a financial variant of this malware aimed at stealing Facebook credentials.

While I did not see any Facebook related activity in my samples, I am posting them anyway for your research as their functionality is the same.

The samples I have are being spread not via Facebook but via Blackhole exploit kit, which is a very effective method. Blackhole exploit kit was associated with the spread of ZeuS, Spyeye, and it is not surprising that Ramnit is being spread in the same manner by the same groups. The group of command and control servers that I researched is associated with pharma spam and "Canadian" online pharmacies.

General File Information

File: 607B2219FBCFBFE8E6AC9D7F3FB8D50E
MD5: 607B2219FBCFBFE8E6AC9D7F3FB8D50E

File: c33e7ed929760020820e8808289c240e
MD5: C33E7ED929760020820E8808289C240E

File: 76991eefea6cb01e1d7435ae973858e6 - not analysed
MD5: 76991EEFEA6CB01E1D7435AE973858E6

File: 2ff2c8ada4fc6291846f0d66ae57ca37 -not analysed
MD5: 2FF2C8ADA4FC6291846F0D66AE57CA37

Download

Download all the binaries and dropped files as a password protected archive (email me if you need the password)

Distribution

The files analysed were / are being distributed via Blackhole exploit pack. It starts with the usual large letter message "Please wait page is loading" -then Java exploit launches and compromise takes place if the machine is vulnerable. . Here you can see the Blackhole domains spreading Ramnit in the Malwaredomainlist . **Amberfreda.com** domain belongs to a legitimate company and is registered in Arizona, while a subdomain **best.amberfreda.com** is registered by some Ukranian guy. Not sure how they managed that.

amberfreda.com
173.201.97.1
p3nlhg49c090.shr.prod.phx3.secureserver.net
Domains By Proxy, LLC
DomainsByProxy.com
15111 N. Hayden Rd., Ste 160, PMB 353
Scottsdale, Arizona 85260
United States

best.amberfreda.com
178.162.145.184
178-162-145-184.local
Host unreachable
178.162.145.128 - 178.162.145.255
VPS services

Ukraine
Vladimir Gubarenko
p/o box 8967
61106, Kharkov
Ukraine
phone: +7 4956637354
fax: +7 4956637354
admin@imhoster.net

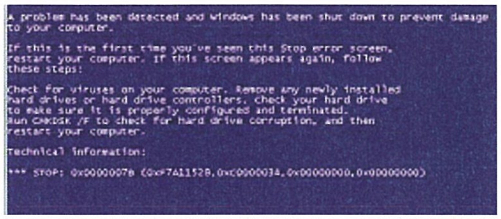
Please wait page is loading...

http://www.malwaredomainlist.com/mdl.php?search=amberfreda.com&colsearch=All&quantity=50

Brief Analysis

607B2219FBCFBFE8E6AC9D7F3FB8D50E

Hendrik Adrian from Japan posted his analysis of the same sample (0day.JP - Ramnit) where he described the files created by the malware and the spam sending capabilities of the bot .



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check for viruses on your computer. Remove any newly installed
hard drives or hard drive controllers. Check your hard drive
to make sure it is properly configured and terminated.
Run CHKDSK /F to check for hard drive corruption, and then
restart your computer.

Technical information:

*** STOP: 0x0000007B (0xF7A11528,0xC0000034,0x00000000,0x00000000)
```

The bot deletes registry settings for the safe boot, which causes BSOD and prevents one from removing the malicious files in the safe mode.

```
----------------------------------
Keys deleted:248
----------------------------------
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\AppMgmt
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\Base
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\Boot Bus Extender
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\Boot file system
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\CryptSvc
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\DcomLaunch
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\dmadmin
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\dmboot.sys
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\dmio.sys
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\dmload.sys
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\dmserver
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\EventLog
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\File system
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\Filter
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\HelpSvc
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\Netlogon
```

2. Adds a Windows service

Micorsoft Windows Service - note the spelling

```
Keys added:18
----------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MICORSOFT_WINDOWS_SERVICE
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MICORSOFT_WINDOWS_SERVICE\0000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MICORSOFT_WINDOWS_SERVICE\0000
\Control
HKLM\SYSTEM\ControlSet001\Services\Micorsoft Windows Service
HKLM\SYSTEM\ControlSet001\Services\Micorsoft Windows Service\Security
HKLM\SYSTEM\ControlSet001\Services\Micorsoft Windows Service\Enum
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MICORSOFT_WINDOWS_SERVICE
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MICORSOFT_WINDOWS_SERVICE\0000
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MICORSOFT_WINDOWS_SERVICE\0000
\Control
HKLM\SYSTEM\CurrentControlSet\Services\Micorsoft Windows Service
HKLM\SYSTEM\CurrentControlSet\Services\Micorsoft Windows Service\Security
HKLM\SYSTEM\CurrentControlSet\Services\Micorsoft Windows Service\Enum
HKU\S-1-5-21-789336058-1580436667-1060284298-1003
\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\dll1
HKU\S-1-5-21-789336058-1580436667-1060284298-1003
\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\exe1
```

3. Adds the following files (names vary)

- \Application Data\nvamibiv\vcryserj.exe - copy of the original
  http://www.virustotal.com/file-scan/report.html?id=f52bfac9637aea189ec918d05113c36f5bcf580f3c0de8a934fe3438107d3f0c-1326310185

File: vcryserj.exe
Size: 135680
MD5: 607B2219FBCFBFE8E6AC9D7F3FB8D50E

- \Application Data\wduqtdai.log - number of logs varies, contain encrypted data
- \Application Data\xtyepaef.log number of logs varies, contain encrypted data
- **\Temp\nhptugtstukgwpyi.exe - copy of the original**

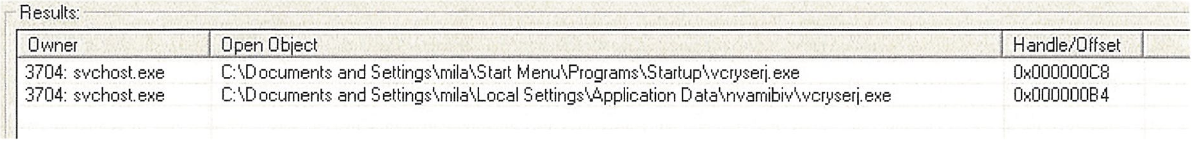
File: nhptugtstukgwpyi.exe
Size: 135680
MD5: 607B2219FBCFBFE8E6AC9D7F3FB8D50E

- **\Start Menu\Programs\Startup\vcryserj.exe - copy of the original**

File: vcryserj.exe
Size: 1356
MD5: 607B2219FBCFBFE8E6AC9D7F3FB8D50E

- **\Local Settings\Temp\dnsgvbny.sys the rootkit**
  http://www.virustotal.com/file-scan/report.html?id=c1293f8dd8a243391d087742fc22c99b8263f70c6937f784c15e9e20252b38ae-1326346542

File: dnsgvbny.sys
Size: 15360
MD5: A6D351093F75D16C574DB31CDF736153


Results:

Owner	Open Object	Handle/Offset
3704: svchost.exe	C:\Documents and Settings\mila\Start Menu\Programs\Startup\vcryserj.exe	0x000000C8
3704: svchost.exe	C:\Documents and Settings\mila\Local Settings\Application Data\nvamibiv\vcryserj.exe	0x000000B4

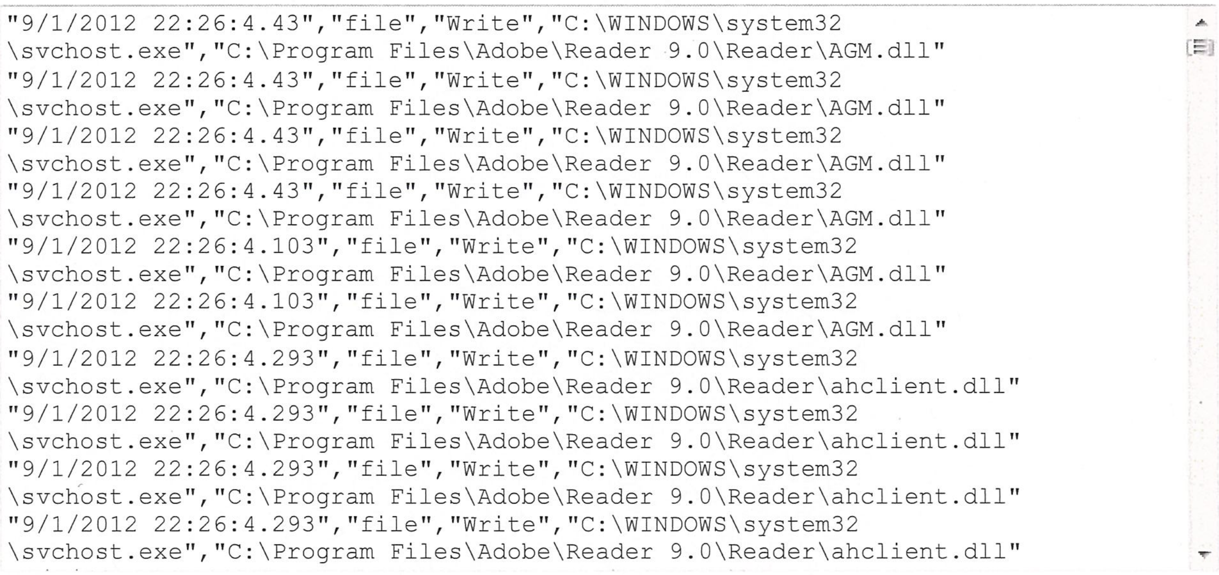
Ramnit injects itself into two svchost.exe processes and you can see them if you sort all processes by PID, the last two will those created by Ramnit.

It generates spam that it sends out on port 25, Hendrik already described this behavior in his post.

C33E7ED929760020820E8808289C240E
The second file has file infector features I did not observe in **607B2219FBCFBFE8E6AC9D7F3FB8D50E.**
As you see in the log below, malicious svchost.exe modifies or tries to modify every binary and HTML file by appending malicious code to each file or a vbs script to HTML files - like

described in this post by ESET Win32/Ramnit.A. and here in the post by Avira - Closer look at W32/Ramnit.C

This does not break the infected binaries, all files continue to work as designed, except they infect or reinfect the computer they are running on. Webmasters may upload infected html files and visitors of their sites may get infected as well. For an average user, it is impossible to clean a system compromised with Ramnit file injector and use it confidence. The only way is say good bye to all the HTM(L), DLL and EXE files and build a new system without trying to copy any hrml files, bookmark or applications.



```
"9/1/2012 22:26:4.43","file","Write","C:\WINDOWS\system32
\svchost.exe","C:\Program Files\Adobe\Reader 9.0\Reader\AGM.dll"
"9/1/2012 22:26:4.43","file","Write","C:\WINDOWS\system32
\svchost.exe","C:\Program Files\Adobe\Reader 9.0\Reader\AGM.dll"
"9/1/2012 22:26:4.43","file","Write","C:\WINDOWS\system32
\svchost.exe","C:\Program Files\Adobe\Reader 9.0\Reader\AGM.dll"
"9/1/2012 22:26:4.43","file","Write","C:\WINDOWS\system32
\svchost.exe","C:\Program Files\Adobe\Reader 9.0\Reader\AGM.dll"
"9/1/2012 22:26:4.103","file","Write","C:\WINDOWS\system32
\svchost.exe","C:\Program Files\Adobe\Reader 9.0\Reader\AGM.dll"
"9/1/2012 22:26:4.103","file","Write","C:\WINDOWS\system32
\svchost.exe","C:\Program Files\Adobe\Reader 9.0\Reader\AGM.dll"
"9/1/2012 22:26:4.293","file","Write","C:\WINDOWS\system32
\svchost.exe","C:\Program Files\Adobe\Reader 9.0\Reader\ahclient.dll"
"9/1/2012 22:26:4.293","file","Write","C:\WINDOWS\system32
\svchost.exe","C:\Program Files\Adobe\Reader 9.0\Reader\ahclient.dll"
"9/1/2012 22:26:4.293","file","Write","C:\WINDOWS\system32
\svchost.exe","C:\Program Files\Adobe\Reader 9.0\Reader\ahclient.dll"
"9/1/2012 22:26:4.293","file","Write","C:\WINDOWS\system32
\svchost.exe","C:\Program Files\Adobe\Reader 9.0\Reader\ahclient.dll"
```

Thsi is what happens with VirustotalUpload2.exe (and most other Programs including Adobe, MS Office and Windows files)

http://www.virustotal.com/file-scan/report.html?id=a40aacca731c142148733786cae64d45df2e740e3fb744ffc513d251ec121cf7-1326169765
VirusTotalUpload2.exe
Submission date:
2012-01-10 04:29:25 (UTC)
Result:37 /43 (86.0%)
Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2012.01.09.00	2012.01.09	Win32/Ramnit.O
AntiVir	7.11.20.218	2012.01.10	W32/Ramnit.E
Avast	6.0.1289.0	2012.01.09	Win32:Ramnit-H
AVG	10.0.0.1190	2012.01.10	Win32/Zbot.G

BitDefender	7.2	2012.01.10	Win32.Ramnit.N
ByteHero	1.0.0.1	2011.12.31	Trojan.Win32.Heur.Gen
CAT-QuickHeal	12.00	2012.01.09	W32.Ramnit.C
ClamAV	0.97.3.0	2012.01.10	Trojan.Patched-168
Commtouch	5.3.2.6	2012.01.10	W32/Ramnit.E
Comodo	11229	2012.01.10	TrojWare.Win32.Patched.SM
DrWeb	5.0.2.03300	2012.01.09	Win32.Rmnet.8
Emsisoft	5.1.0.11	2012.01.10	Virus.Win32.Zbot!IK
eTrust-Vet	37.0.9672	2012.01.09	Win32/Ramnit.AJ
F-Prot	4.6.5.141	2012.01.09	W32/Ramnit.E
F-Secure	9.0.16440.0	2012.01.09	Win32.Ramnit.N
Fortinet	4.3.388.0	2012.01.10	W32/Ramnit.B
GData	22	2012.01.09	Win32.Ramnit.N
Ikarus	T3.1.1.109.0	2012.01.10	Virus.Win32.Zbot
Jiangmin	13.0.900	2012.01.09	Win32/PatchFile.gg
K7AntiVirus	9.124.5897	2012.01.09	Trojan
Kaspersky	9.0.0.837	2012.01.10	Trojan.Win32.Patched.md
McAfee	5.400.0.1158	2012.01.10	W32/Ramnit.b
McAfee-GW-Edition	2010.1E	2012.01.09	W32/Ramnit.b
Microsoft	1.7903	2012.01.09	Virus:Win32/Ramnit.AF
NOD32	6780	2012.01.10	Win32/Ramnit.H
Norman	6.07.13	2012.01.09	W32/Ramnit.AB
nProtect	2012-01-09.01	2012.01.10	Win32.Ramnit.N
Panda	10.0.3.5	2012.01.09	W32/Cosmu.L
PCTools	8.0.0.5	2012.01.10	Malware.Ramnit
Rising	23.92.01.01	2012.01.10	Win32.Ramnit.c
Symantec	20111.2.0.82	2012.01.10	W32.Ramnit.B!inf
TrendMicro	9.500.0.1008	2012.01.10	PE_RAMNIT.KC
TrendMicro-HouseCall	9.500.0.1008	2012.01.10	PE_RAMNIT.KC
ViRobot	2012.1.10.4872	2012.01.10	Win32.Ramnit.A
VirusBuster	14.1.158.1	2012.01.09	Win32.Ramnit.Gen.3

Additional information
MD5 : 25f6ee42d37e3f2f7dbe795e836d52e2

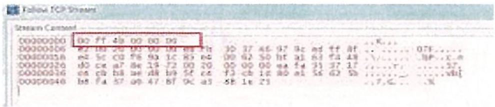
Traffic

607B2219FBCFBFE8E6AC9D7F3FB8D50E - C&C is sinkholedC33E7ED929760020820E8808289C240E - C&C is active

Despite the fact that the C&C for 607B2219FBCFBFE8E6AC9D7F3FB8D50E is sinkholed, it is still interesting to see the malware behavior when it tries to establish a connection with the server.

Ramnit samples used by the same group of attackers have overlapping set of C&C servers - the list is not the same but I found that my samples that are supposedly later version that Ramnit.AK have approximately 80% overlap in C&C list used by this RamnitAK binary described by Sophos . I have combined the two lists and ran WHOIS queries to establish active C&C and their location and registration.

The communications with the sinkholed server below show that once the bot receives SYN command from the C&C, it sends **6 bytes of data.** Exact same behavior is described in this analysis of the binaries from Summer 2011 - with the only difference that the second packet sent by the bot was not 75 bytes but 149 bytes Bot of the Day: Ramnit/NinmulMonday, July 18th, 2011. If connection with the server is established, the traffic continues on on port 443, it is encoded but it is not SSL, it is some sort of custom protocol.



```
00000000  00 ff 4b 00 00 00
```

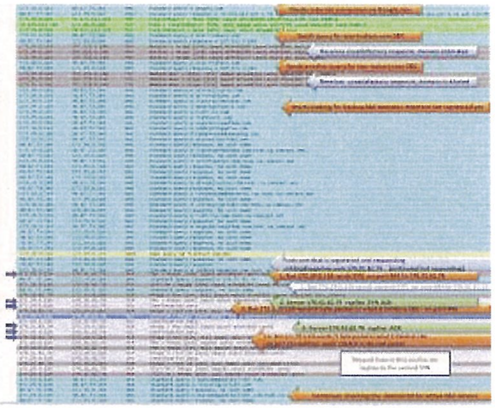
The bot is going through the list of domains trying to find those that are active. Most of the domains are not registered yet but the two currently active domains were registered on **January 5 and 6, 2011.** It appears that the attackers register new domains as soon as the lose any due to sinkholing and domain cancellations. Since all the domains have the most random names, they are not likely to be registered by someone else before they are needed. Having each binary to check a long list of domains makes the bot very noisy (consider making IDS signatures based on UDP port 53 thresholds) but it prevents the death of the botnet in case of the C&C loss. I have complied a list of approximately 400 domains with only 21 of them registered. If you created DNS blocks or sinkhole domains, consider blocking or sinkholing all of them, not only active.

Domain name: rjordulltl.com
89.149.242.185 - Leaseweb Germany GmbH (previously netdirekt e. K.)
Germany
Registrar: Regtime Ltd.
Creation date: 2012-01-05
Expiration date: 2013-01-05

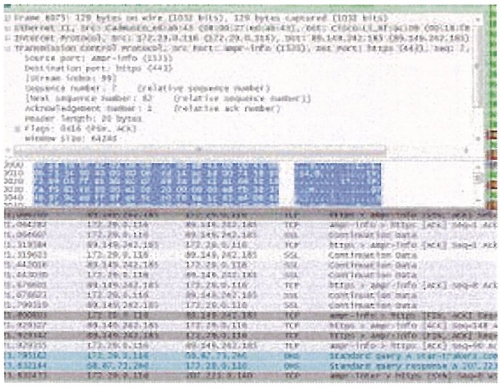
Domain Name: **goopndlgvy.com**
Registrant:
PrivacyProtect.org
Domain Admin (contact@privacyprotect.org)
ID#10760, PO Box 16
Note - All Postal Mails Rejected, visit Privacyprotect.org
Nobby Beach
null,QLD 4218
AU
Tel. +45.36946676
89.149.242.185 - Leaseweb Germany GmbH (previously netdirekt e. K.)
Germany

Creation Date: 06-Jan-2012
Expiration Date: 06-Jan-2013

Communications with a sinkholed C&C and search for a new active server:



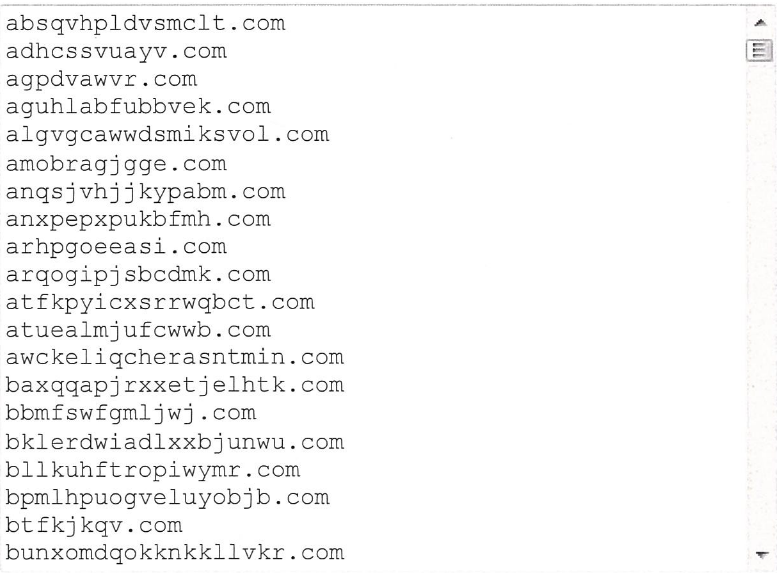
Bot <-> C&C communications on port 443



```
Frame 6075: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits)
Ethernet II, Src: CadmusCo_ed:ab:43 (08:00:27:ed:ab:43), Dst: Cisco-Li_8f:ac:09 (00:18:f8
Internet Protocol, Src: 172.29.0.116 (172.29.0.116), Dst: 89.149.242.185 (89.149.242.185)
Transmission Control Protocol, Src Port: ampr-info (1535), Dst Port: https (443), Seq: 2,
  Source port: ampr-info (1535)
  Destination port: https (443)
  [Stream index: 99]
  Sequence number: 2    (relative sequence number)
  [Next sequence number: 82    (relative sequence number)]
  Acknowledgement number: 1    (relative ack number)
  Header length: 20 bytes
  Flags: 0x18 (PSH, ACK)
  Window size: 64240
```

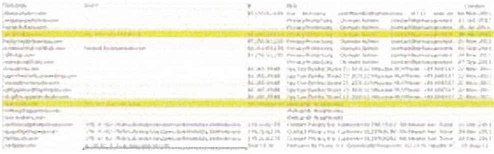
```
1.064282   172.29.0.116     89.149.242.185   TCP   ampr-info > https [ACK] Seq=1 Ack
1.064607   172.29.0.116     89.149.242.185   SSL   Continuation Data
1.319384   89.149.242.185   172.29.0.116     TCP   https > ampr-info [ACK] Seq=1 Ack
1.319623   172.29.0.116     89.149.242.185   SSL   Continuation Data
1.442016   89.149.242.185   172.29.0.116     SSL   Continuation Data
1.443030   172.29.0.116     89.149.242.185   SSL   Continuation Data
1.678601   89.149.242.185   172.29.0.116     TCP   https > ampr-info [ACK] Seq=8 Ack
1.678621   172.29.0.116     89.149.242.185   SSL   Continuation Data
1.799319   89.149.242.185   172.29.0.116     SSL   Continuation Data
1.800033   172.29.0.116     89.149.242.185   TCP   ampr-info > https [FIN, ACK] Seq=
1.929327   89.149.242.185   172.29.0.116     TCP   https > ampr-info [ACK] Seq=148 A
1.929342   89.149.242.185   172.29.0.116     TCP   https > ampr-info [FIN, ACK] Seq=
1.929355   172.29.0.116     89.149.242.185   TCP   ampr-info > https [ACK] Seq=90 Ac
3.795162   172.29.0.116     68.87.73.246     DNS   Standard query A star-traders.com
3.832144   68.87.73.246     172.29.0.116     DNS   Standard query response A 207.223
3.832473   172.29.0.116     207.223.3.140    TCP   ampr-tree > https [SYN] Seq=0 W
```

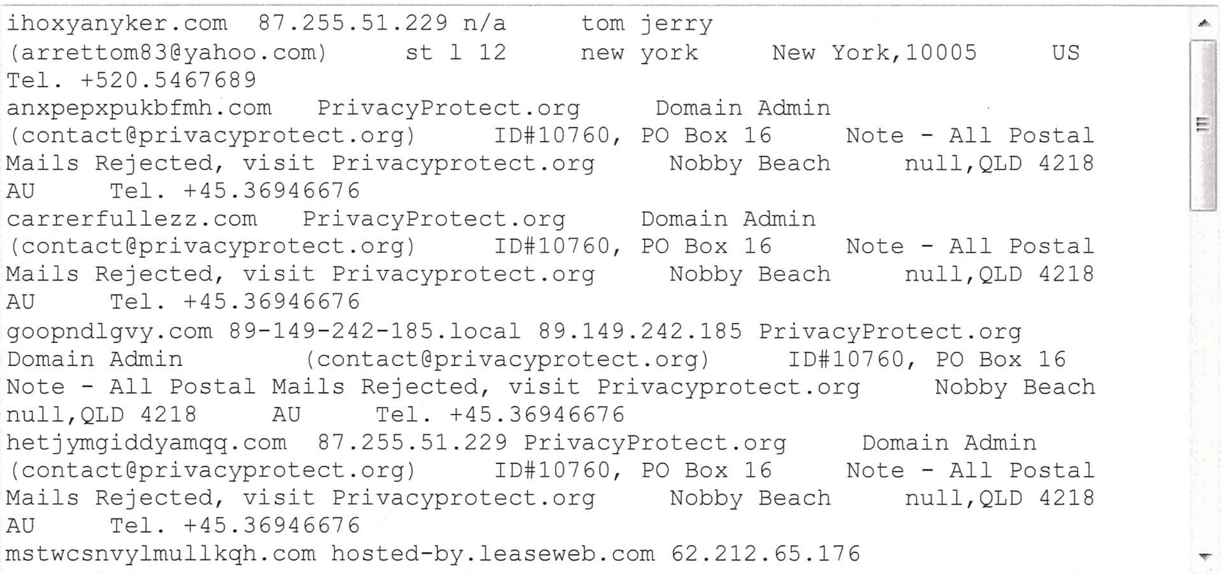
List of domains used by Ramnit binaries - feel free to pre-emptively sinkhole them. Part of them are from this Sophos analysis and part is from running these two binaries



```
absqvhpldvsmclt.com
adhcssvuayv.com
agpdvawvr.com
aguhlabfubbvek.com
algvgcawwdsmiksvol.com
amobragjgge.com
anqsjvhjjkypabm.com
anxpepxpukbfmh.com
arhpgoeeasi.com
arqogipjsbcdmk.com
atfkpyicxsrrwqbct.com
atuealmjufcwwb.com
awckeliqcherasntmin.com
baxqqapjrxxetjelhtk.com
bbmfswfgmljwj.com
bklerdwiadlxxbjunwu.com
bllkuhftropiwymr.com
bpmlhpuogveluyobjb.com
btfkjkqv.com
bunxomdqokknkkllvkr.com
```

Registered domains. See the text version below. The yellow/red entries show active C&C. All others are sinkholed or NXD'd.





```
ihoxyanyker.com  87.255.51.229 n/a     tom jerry
(arrettom83@yahoo.com)     st l 12     new york     New York,10005     US
Tel. +520.5467689
anxpepxpukbfmh.com   PrivacyProtect.org     Domain Admin
(contact@privacyprotect.org)     ID#10760, PO Box 16     Note - All Postal
Mails Rejected, visit Privacyprotect.org     Nobby Beach     null,QLD 4218
AU     Tel. +45.36946676
carrerfullezz.com   PrivacyProtect.org     Domain Admin
(contact@privacyprotect.org)     ID#10760, PO Box 16     Note - All Postal
Mails Rejected, visit Privacyprotect.org     Nobby Beach     null,QLD 4218
AU     Tel. +45.36946676
goopndlgvy.com 89-149-242-185.local 89.149.242.185 PrivacyProtect.org
Domain Admin         (contact@privacyprotect.org)     ID#10760, PO Box 16
Note - All Postal Mails Rejected, visit Privacyprotect.org     Nobby Beach
null,QLD 4218     AU     Tel. +45.36946676
hetjymgiddyamqq.com  87.255.51.229 PrivacyProtect.org     Domain Admin
(contact@privacyprotect.org)     ID#10760, PO Box 16     Note - All Postal
Mails Rejected, visit Privacyprotect.org     Nobby Beach     null,QLD 4218
AU     Tel. +45.36946676
mstwcsnvylmullkqh.com hosted-by.leaseweb.com 62.212.65.176
```

As you notice, many domains are registered by "Aleksandr Bragilevskij"
Registrar: Regtime Ltd.
Creation date: 2011-12-03

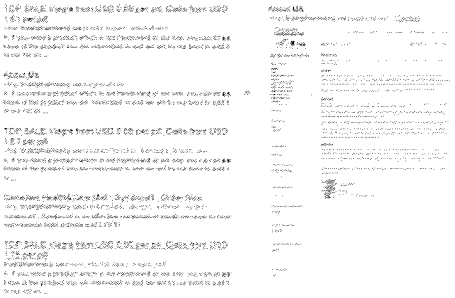
Expiration date: 2012-12-03

Registrant:
Aleksandr Bragilevskij
Email: pfizer.corp@yahoo.com
Organization: Aleksandr Bragilevskij
Address: 333 E 79th St # 1T,
City: New York City
State: NY
ZIP: 10001
Country: UM
Phone: +1.2127332323
Fax: +1.2127332323

Google Search for pfizer.corp@yahoo.com reveals that the same address was used to register fake Canadian pharmacy sites, which makes sense, considering the Viagra spam.

trustpharmacy.us

188.72.200.84
Markus Faizer
Pfizer International
333 E 79th St # 1T,
New York City
NY
10001
United States
Phone: +1.2127332323
Fax: +1.2127332323
E-mail: pfizer.corp@yahoo.com



Mila at2:57 AM

Share g+1 0

No comments:

Post a Comment

Links to this post

Create a Link

‹ Home ›

View web version

Shared by

Mila

@ you can find my email address in my profile

View my complete profile

Powered by Blogger.

MICROSOFT SOFTWARE LICENSE TERMS

WINDOWS 7 HOME PREMIUM

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. Printed-paper license terms, which may come with the software, may replace or modify any on-screen license terms. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, return it to the retailer for a refund or credit. If you cannot obtain a refund there, contact Microsoft or the Microsoft affiliate serving your country for information about Microsoft's refund policies. See www.microsoft.com/worldwide. In the United States and Canada, call (800) MICROSOFT or see www.microsoft.com/info/nareturns.htm.

As described below, using the software also operates as your consent to the transmission of certain computer information during activation, validation and for Internet-based services.

If you comply with these license terms, you have the rights below for each license you acquire.

1. OVERVIEW.

a. Software. The software includes desktop operating system software. This software does not include Windows Live services. Windows Live is a service available from Microsoft under a separate agreement.

b. License Model. Subject to Section 2 (b) below, the software is licensed on a per copy per computer basis. A computer is a physical hardware system with an internal storage device capable of running the software. A hardware partition or blade is considered to be a separate computer.

2. INSTALLATION AND USE RIGHTS.

a. One Copy per Computer. Except as allowed in Section 2 (b) below, you may install one copy of the software on one computer. That computer is the "licensed computer."

b. Family Pack. If you are a "Qualified Family Pack User", you may install one copy of the software marked as "Family Pack" on three computers in your household for use by people who reside there. Those computers are the "licensed computers" and are subject to these license terms. If you do not know whether you are a Qualified Family Pack User, visit go.microsoft.com/fwlink/?Linkid=141399 or contact the Microsoft affiliate serving your country.

c. Licensed Computer. You may use the software on up to two processors on the licensed computer at one time. Unless otherwise provided in these license terms, you may not use the software on any other computer.

d. Number of Users. Unless otherwise provided in these license terms, only one user may use the software at a time.

e. Alternative Versions. The software may include more than one version, such as 32-bit and 64-bit. You may install and use only one version at one time.

3. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. Multiplexing. Hardware or software you use to

- pool connections, or
- reduce the number of devices or users that directly access or use the software

(sometimes referred to as "multiplexing" or "pooling"), does not reduce the number of licenses you need.

b. Font Components. While the software is running, you may use its fonts to display and print content. You may only

- embed fonts in content as permitted by the embedding restrictions in the fonts; and
- temporarily download them to a printer or other output device to print content.

c. Icons, images and sounds. While the software is running, you may use but not share its icons, images, sounds, and media. The sample images, sounds and media provided with the software are for your non-commercial use only.

d. Use with Virtualization Technologies. Instead of using the software directly on the licensed computer, you may install and use the software within only one virtual (or otherwise emulated) hardware system on the licensed computer. When used in a virtualized environment, content protected by digital rights management technology, BitLocker or any full volume disk drive encryption technology may not be as secure as protected content not in a virtualized environment. You should comply with all domestic and international laws that apply to such protected content.

e. Device Connections. You may allow up to 20 other devices to access software installed on the licensed computer to use only File Services, Print Services, Internet Information Services and Internet Connection Sharing and Telephony Services.

f. Remote Access Technologies. You may remotely access and use the software installed on the licensed computer from another computer to share a session using Remote Assistance or similar technologies. A "session" means the experience of interacting with the software, directly or indirectly, through any combination of input, output and display peripherals.

g. Media Center Extender. You may have five Media Center Extender Sessions (or other software or devices which provide similar functionality for a similar purpose) running at the same time to display the software user interface or content on other displays or devices.

h. Electronic Programming Guide. If the software includes access to an electronic programming guide service that displays customized television listings, a separate service agreement applies to the service. If you do not agree to the terms of the service agreement, you may continue to use the software, but you will not be able to use the electronic programming guide service. The service may contain advertising content and related data, which are received and stored by the software. The service is not available in all areas. Please consult the software information for instructions on accessing the service agreement.

i. **Related Media Information.** If you request related media information as part of your playback experience, the data provided to you may not be in your local language. Some countries or regions have laws and regulations which may restrict or limit your ability to access certain types of content.

j. **Worldwide Use of the Media Center.** Media Center is not designed for use in every country. For example, although the Media Center information may refer to certain features such as an electronic programming guide or provide information on how to configure a TV tuner, these features may not work in your area. Please refer to the Media Center information for a list of features that may not work in your area.

4. MANDATORY ACTIVATION.

Activation associates the use of the software with a specific computer. During activation, the software will send information about the software and the computer to Microsoft. This information includes the version, language and product key of the software, the Internet protocol address of the computer, and information derived from the hardware configuration of the computer. For more information, see go.microsoft.com/fwlink/?Linkid=104609. By using the software, you consent to the transmission of this information. If properly licensed, you have the right to use the version of the software installed during the installation process up to the time permitted for activation. **Unless the software is activated, you have no right to use the software after the time permitted for activation.** This is to prevent its unlicensed use. **You are not permitted to bypass or circumvent activation.** If the computer is connected to the Internet, the software may automatically connect to Microsoft for activation. You can also activate the software manually by Internet or telephone. If you do so, Internet and telephone service charges may apply. Some changes to your computer components or the software may require you to reactivate the software. **The software will remind you to activate it until you do.**

5. VALIDATION.

a. Validation verifies that the software has been activated and is properly licensed. It also verifies that no unauthorized changes have been made to the validation, licensing, or activation functions of the software. Validation may also check for certain malicious or unauthorized software related to such unauthorized changes. A validation check confirming that you are properly licensed permits you to continue to use the software, certain features of the software or to obtain additional benefits. **You are not permitted to circumvent validation.** This is to prevent unlicensed use of the software. For more information, see go.microsoft.com/fwlink/?Linkid=104610.

b. The software will from time to time perform a validation check of the software. The check may be initiated by the software or Microsoft. To enable the activation function and validation checks, the software may from time to time require updates or additional downloads of the validation, licensing or activation functions of the software. The updates or downloads are required for the proper functioning of the software and may be downloaded and installed without further notice to you. During or after a validation check, the software may send information about the software, the computer and the results of the validation check to Microsoft. This information includes, for example, the version and product key of the software, any unauthorized changes made to the validation, licensing or activation functions of the software, any related malicious or unauthorized software found and the Internet protocol address of the computer. Microsoft does not use the information to identify or contact you. By using the software, you consent to the transmission of this information. For more information about validation and what is sent during or after a validation check, see go.microsoft.com/fwlink/?Linkid=104611.

c. If, after a validation check, the software is found to be counterfeit, improperly licensed, a non-genuine Windows product, or include unauthorized changes, the functionality and experience of using the software will be affected, for example:

Microsoft may

- repair the software, remove, quarantine or disable any unauthorized changes that may interfere with the proper use of the software, including circumvention of the activation or validation functions of the software, or
- check and remove malicious or unauthorized software known to be related to such unauthorized changes, or
- provide notices that the software is improperly licensed or a non-genuine Windows product

and you may

- receive reminders to obtain a properly licensed copy of the software, or
- need to follow Microsoft's instructions to be licensed to use the software and reactivate,

and you may not be able to

- use or continue to use the software or some of the features of the software, or
- obtain certain updates or upgrades from Microsoft

d. You may only obtain updates or upgrades for the software from Microsoft or authorized sources. For more information on obtaining updates from authorized sources see go.microsoft.com/fwlink/?Linkid=104612.

6. POTENTIALLY UNWANTED SOFTWARE. If turned on, Windows Defender will search your computer for "spyware," "adware" and other potentially unwanted software. If it finds potentially unwanted software, the software will ask you if you want to ignore, disable (quarantine) or remove it. Any potentially unwanted software rated "high" or "severe," will automatically be removed after scanning unless you change the default setting. Removing or disabling potentially unwanted software may result in

- other software on your computer ceasing to work, or
- your breaching a license to use other software on your computer.

By using this software, it is possible that you will also remove or disable software that is not potentially unwanted software.

7. INTERNET-BASED SERVICES. Microsoft provides Internet-based services with the software. It may change or cancel them at any time.

a. **Consent for Internet-Based Services.** The software features described below and in the Windows 7 Privacy Statement connect to Microsoft or service provider computer systems over the Internet. In some cases, you will not receive a separate notice when they connect. In some cases, you may switch off these features or not use them. For more information about these features, see the Windows 7 Privacy Statement at go.microsoft.com/fwlink/?linkid=104604. **By using these features, you consent to the transmission of this information.** Microsoft does not use the information to identify or contact you.

   Computer Information. The following features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the type of operating system, browser and name and version of the software you are using, and the language code of the computer where you installed the software. Microsoft uses this information to make the Internet-based services available to you.

   - Plug and Play and Plug and Play Extensions. You may connect new hardware to your computer, either directly or over a network. Your computer may not have the drivers needed to communicate with that hardware. If so, the update feature of the software can obtain the correct driver from Microsoft and install it on your computer. An administrator can disable this update feature.

   - Windows Update. To enable the proper functioning of the Windows Update service in the software (if you use it), updates or downloads to the Windows Update service will be required from time to time and downloaded and installed without further notice to you.

   - Web Content Features. Features in the software can retrieve related content from Microsoft and provide it to you. Examples of these features are clip art, templates, online training, online assistance and Appshelp. You may choose not to use these web content features.

   - Digital Certificates. The software uses digital certificates. These digital certificates confirm the identity of Internet users sending X.509 standard encrypted information. They also can be used to digitally sign files and macros, to verify the integrity and origin of the file contents. The software retrieves certificates and updates certificate revocation lists over the Internet, when available.

   - Auto Root Update. The Auto Root Update feature updates the list of trusted certificate authorities. You can switch off the Auto Root Update feature.

   - Windows Media Digital Rights Management. Content owners use Windows Media digital rights management technology (WMDRM) to protect their intellectual property, including copyrights. This software and third party software use WMDRM to play and copy WMDRM-protected content. If the software fails to protect the content, content owners may ask Microsoft to revoke the software's ability to use WMDRM to play or copy protected content. Revocation does not affect other content. When you download licenses for protected content, you agree that Microsoft may include a revocation list with the licenses. Content owners may require you to upgrade WMDRM to access their content. Microsoft software that includes WMDRM will ask for your consent prior to the upgrade. If you decline an upgrade, you will not be able to access content that requires the upgrade. You may switch off WMDRM features that access the Internet. When these features are off, you can still play content for which you have a valid license.

   - Windows Media Player. When you use Windows Media Player, it checks with Microsoft for

  - compatible online music services in your region; and

  - new versions of the player.

  For more information, go to go.microsoft.com/fwlink/?Linkid=104605.

- Malicious Software Removal. During setup, if you select "Get important updates for installation", the software may check and remove certain malware from your computer. "Malware" is malicious software. If the software runs, it will remove the Malware listed and updated at www.support.microsoft.com/?kbid=890830. During a Malware check, a report will be sent to Microsoft with specific information about Malware detected, errors, and other information about your computer. This information is used to improve the software and other Microsoft products and services. No information included in these reports will be used to identify or contact you. You may disable the software's reporting functionality by following the instructions found at www.support.microsoft.com/?kbid=890830. For more information, read the Windows Malicious Software Removal Tool privacy statement at go.microsoft.com/fwlink/?LinkId=113995.

- Network Awareness. This feature determines whether a system is connected to a network by either passive monitoring of network traffic or active DNS or HTTP queries. The query only transfers standard TCP/IP or DNS information for routing purposes. You can switch off the active query feature through a registry setting.

- Windows Time Service. This service synchronizes with time.windows.com once a week to provide your computer with the correct time. You can turn this feature off or choose your preferred time source within the Date and Time Control Panel applet. The connection uses standard NTP protocol.

- IPv6 Network Address Translation (NAT) Traversal service (Teredo). This feature helps existing home Internet gateway devices transition to IPv6. IPv6 is next generation Internet protocol. It helps enable end-to-end connectivity often needed by peer-to-peer applications. To do so, each time you start up the software the Teredo client service will attempt to locate a public Teredo Internet service. It does so by sending a query over the Internet. This query only transfers standard Domain Name Service information to determine if your computer is connected to the Internet and can locate a public Teredo service. If you

  - use an application that needs IPv6 connectivity or

  - configure your firewall to always enable IPv6 connectivity

  by default standard Internet Protocol information will be sent to the Teredo service at Microsoft at regular intervals. No other information is sent to Microsoft. You can change this default to use non-Microsoft servers. You can also switch off this feature using a command line utility named "netsh".

- Accelerators. When you click on or move your mouse over an Accelerator in Internet Explorer, any of the following may be sent to the service provider:

  - the title and full web address or URL of the current webpage,

  - standard computer information, and

  - any content you have selected.

If you use an Accelerator provided by Microsoft, use of the information sent is subject to the Microsoft Online Privacy Statement. This statement is available at go.microsoft.com/fwlink/?linkid=31493. If you use an Accelerator provided by a third party, use of the information sent will be subject to the third party's privacy practices.

- Search Suggestions Service. In Internet Explorer, when you type a search query in the Instant Search box or type a question mark (?) before your search term in the Address bar, you will see search suggestions as you type (if supported by your search provider). Everything you type in the Instant Search box or in the Address bar when preceded by a question mark (?) is sent to your search provider as you type. Also, when you press Enter or click the Search button, the text in the Instant Search box or Address bar is sent to the search provider. If you use a Microsoft search provider, use of the information sent is subject to the Microsoft Online Privacy Statement. This statement is available at go.microsoft.com/fwlink/?linkid=31493. If you use a third-party search provider, use of the information sent will be subject to the third party's privacy practices. You can turn search suggestions off at any time. To do so, use Manage Add-ons under the Tools button in Internet Explorer. For more information about the search suggestions service, see go.microsoft.com/fwlink/?linkid=128106.

- Consent to Update Infrared Emitter/Receiver. The software may contain technology to ensure proper functioning of the infrared emitter/receiver device shipped with certain Media Center-based products. You agree that the software may update the firmware of this device.

- Media Center Online Promotions. If you use Media Center features of the software to access Internet-based content or other Internet-based services, such services may obtain the following information from the software to enable you to receive, accept and use certain promotional offers:

  - certain computer information, such as your Internet protocol address, the type of operating system and browser you are using, and the name and version of the software you are using,

  - the requested content, and

  - the language code of the computer where you installed the software.

  Your use of the Media Center features to connect to those services serves as your consent to the collection and use of such information.

b. **Use of Information.** Microsoft may use the computer information, accelerator information, search suggestions information, error reports, and Malware reports to improve our software and services. We may also share it with others, such as hardware and software vendors. They may use the information to improve how their products run with Microsoft software.

c. **Misuse of Internet-based Services.** You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

8. **SCOPE OF LICENSE.** The software is licensed, not sold. This agreement only gives you some rights to use the features included in the software edition you licensed. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not

- work around any technical limitations in the software;

- reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;

- use components of the software to run applications not running on the software;

- make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;

- publish the software for others to copy;

- rent, lease or lend the software; or

- use the software for commercial software hosting services.

9. **MICROSOFT .NET BENCHMARK TESTING.** The software includes one or more components of the .NET Framework (".NET Components"). You may conduct internal benchmark testing of those components. You may disclose the results of any benchmark test of those components, provided that you comply with the conditions set forth at go.microsoft.com/fwlink/?LinkID=66406. Notwithstanding any other agreement you may have with Microsoft, if you disclose such benchmark test results, Microsoft shall have the right to disclose the results of benchmark tests it conducts of your products that compete with the applicable .NET Component, provided it complies with the same conditions set forth at go.microsoft.com/fwlink/?LinkID=66406.

10. **BACKUP COPY.**

    a. **Media.** If you acquired the software on a disc or other media, you may make one backup copy of the media. You may use it only to reinstall the software on the licensed computer.

    b. **Electronic Download.** If you purchased and downloaded the software online, you may make one copy of the software on a disc or other media in order to install the software on a computer. You may also use it to reinstall the software on the licensed computer.

11. **DOCUMENTATION.** Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

12. **NOT FOR RESALE SOFTWARE.** You may not sell software marked as "NFR" or "Not for Resale."

13. **ACADEMIC EDITION SOFTWARE.** You must be a "Qualified Educational User" to use software marked as "Academic Edition" or "AE." If you do not know whether you are a Qualified Educational User, visit www.microsoft.com/education or contact the Microsoft affiliate serving your country.

14. **GEOGRAPHIC RESTRICTIONS.** If the software is marked as requiring activation in a specific geographic region, then you are only permitted to activate this software in the geographic region indicated on the software packaging. You may not be able to activate the software outside of that region. For further information on geographic restrictions, visit go.microsoft.com/fwlink/?LinkId=141397.

15. **UPGRADES.** To use upgrade software, you must first be licensed for the software that is eligible for the upgrade. Upon upgrade, this agreement takes the place of the agreement for the software you upgraded from. After you upgrade, you may no longer use the software you upgraded from.

16. PROOF OF LICENSE.

a. **Genuine Proof of License.** If you acquired the software on a disc or other media, your proof of license is the genuine Microsoft certificate of authenticity label with the accompanying genuine product key, and your proof of purchase. If you purchased and downloaded the software online, your proof of license is the genuine Microsoft product key for the software which you received with your purchase, and your proof of purchase from an authorized electronic supplier of genuine Microsoft software. Proof of purchase may be subject to verification by your merchant's records.

b. **Windows Anytime Upgrade License.** If you upgrade the software using Windows Anytime Upgrade, your proof of license is the proof of license for the software you upgraded from, your Windows Anytime Upgrade product key and your proof of purchase. Proof of purchase may be subject to verification by your merchant's records.

c. To identify genuine Microsoft software, see www.howtotell.com.

17. TRANSFER TO ANOTHER COMPUTER.

a. **Software Other than Windows Anytime Upgrade.** You may transfer the software and install it on another computer for your use. That computer becomes the licensed computer. You may not do so to share this license between computers.

b. **Windows Anytime Upgrade Software.** You may transfer the software and install it on another computer, but only if the license terms of the software you upgraded from allows you to do so. That computer becomes the licensed computer. You may not do so to share this license between computers.

18. TRANSFER TO A THIRD PARTY.

a. **Software Other Than Windows Anytime Upgrade.** The first user of the software may make a one time transfer of the software and this agreement, by transferring the original media, the certificate of authenticity, the product key and the proof of purchase directly to a third party. The first user must remove the software before transferring it separately from the computer. The first user may not retain any copies of the software.

b. **Windows Anytime Upgrade Software.** You may transfer the software directly to a third party only with the licensed computer. You may not keep any copies of the software or any earlier edition.

c. **Other Requirements.** Before any permitted transfer, the other party must agree that this agreement applies to the transfer and use of the software.

19. NOTICE ABOUT THE H.264/AVC VISUAL STANDARD, THE VC-1 VIDEO STANDARD, THE MPEG-4 VISUAL STANDARD AND THE MPEG-2 VIDEO STANDARD. This software includes H.264/AVC, VC-1, MPEG-4 Part 2, and MPEG-2 visual compression technology. MPEG LA, L.L.C. requires this notice:

THIS PRODUCT IS LICENSED UNDER THE AVC, THE VC-1, THE MPEG-4 PART 2 VISUAL, AND THE MPEG-2 VIDEO PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE STANDARDS ("VIDEO STANDARDS") AND/OR (ii) DECODE AVC, VC-1, MPEG-4 PART 2 AND MPEG-2 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERICAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE

OBTAINED FROM MPEG LA, L.L.C. SEE WWW.MPEGLA.COM.

20. **THIRD PARTY PROGRAMS.** The software contains third party programs. The license terms with those programs apply to your use of them.

21. **EXPORT RESTRICTIONS.** The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

22. **SUPPORT SERVICES.** Microsoft provides support services for the software as described at www.support.microsoft.com/common/international.aspx. If you are using software that is not properly licensed, you will not be entitled to receive support services.

23. **ENTIRE AGREEMENT.** This agreement (including the warranty below), additional terms (including any printed-paper license terms that accompany the software and may modify or replace some or all of these terms), and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

24. **APPLICABLE LAW.**

    a. **United States.** If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

    b. **Outside the United States.** If you acquired the software in any other country, the laws of that country apply.

25. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your state or country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your state or country if the laws of your state or country do not permit it to do so.

26. **LIMITATION ON AND EXCLUSION OF DAMAGES. You can recover from Microsoft and its suppliers only direct damages up to the amount you paid for the software. You cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages.**

    This limitation applies to

    - anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and

    - claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

    It also applies even if

    - repair, replacement or a refund for the software does not fully compensate you for any losses; or

    - Microsoft knew or should have known about the possibility of the damages.

    Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. They also may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

****

LIMITED WARRANTY

A. **LIMITED WARRANTY.** If you follow the instructions and the software is properly licensed, the software will perform substantially as described in the Microsoft materials that you receive in or with the software.

B. **TERM OF WARRANTY; WARRANTY RECIPIENT; LENGTH OF ANY IMPLIED WARRANTIES. The limited warranty covers the software for one year after acquired by the first user. If you receive supplements, updates, or replacement software during that year, they will be covered for the remainder of the warranty or 30 days, whichever is longer.** If the first user transfers the software, the remainder of the warranty will apply to the recipient.

To the extent permitted by law, any implied warranties, guarantees or conditions last only during the term of the limited warranty. Some states do not allow limitations on how long an implied warranty lasts, so these limitations may not apply to you. They also might not apply to you because some countries may not allow limitations on how long an implied warranty, guarantee or condition lasts.

C. **EXCLUSIONS FROM WARRANTY.** This warranty does not cover problems caused by your acts (or failures to act), the acts of others, or events beyond Microsoft's reasonable control.

D. **REMEDY FOR BREACH OF WARRANTY. Microsoft will repair or replace the software at no charge. If Microsoft cannot repair or replace it, Microsoft will refund the amount shown on your receipt for the software. It will also repair or replace supplements, updates and replacement software at no charge. If Microsoft cannot repair or replace them, it will refund the amount you paid for them, if any. You must uninstall the software and return any media and other associated materials to Microsoft with proof of purchase to obtain a refund. These are your only remedies for breach of the limited warranty.**

E. **CONSUMER RIGHTS NOT AFFECTED. You may have additional consumer rights under your local laws, which this agreement cannot change.**

F. **WARRANTY PROCEDURES.** You need proof of purchase for warranty service.

1. **United States and Canada.** For warranty service or information about how to obtain a refund for software acquired in the United States and Canada, contact Microsoft at

   - (800) MICROSOFT;
   - Microsoft Customer Service and Support, One Microsoft Way, Redmond, WA 98052-6399; or
   - visit www.microsoft.com/info/nareturns.htm.

2. **Europe, Middle East and Africa.** If you acquired the software in Europe, the Middle East or Africa, Microsoft Ireland Operations Limited makes this limited warranty. To make a claim under this warranty, you should contact either

   - Microsoft Ireland Operations Limited, Customer Care Centre, Atrium Building Block B, Carmanhall Road, Sandyford Industrial Estate, Dublin 18, Ireland; or

- the Microsoft affiliate serving your country (see www.microsoft.com/worldwide).

3. **Outside United States, Canada, Europe, Middle East and Africa.** If you acquired the software outside the United States, Canada, Europe, the Middle East and Africa, contact the Microsoft affiliate serving your country (see www.microsoft.com/worldwide).

G. **NO OTHER WARRANTIES. The limited warranty is the only direct warranty from Microsoft. Microsoft gives no other express warranties, guarantees or conditions. Where allowed by your local laws, Microsoft excludes implied warranties of merchantability, fitness for a particular purpose and non-infringement.** If your local laws give you any implied warranties, guarantees or conditions, despite this exclusion, your remedies are described in the Remedy for Breach of Warranty clause above, to the extent permitted by your local laws.

H. **LIMITATION ON AND EXCLUSION OF DAMAGES FOR BREACH OF WARRANTY. The Limitation on and Exclusion of Damages clause above applies to breaches of this limited warranty.**

This warranty gives you specific legal rights, and you may also have other rights which vary from state to state. You may also have other rights which vary from country to country.

!!!!EULAID!!!!

MICROSOFT SOFTWARE LICENSE TERMS

WINDOWS VISTA BUSINESS

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, return it to the retailer for a refund or credit. If you cannot obtain a refund there, contact Microsoft or the Microsoft affiliate serving your country for information about Microsoft's refund policies. See www.microsoft.com/worldwide. In the United States and Canada, call (800) MICROSOFT or see www.microsoft.com/info/nareturns.htm.

As described below, using the software also operates as your consent to the transmission of certain computer information during activation, validation and for Internet-based services.

If you comply with these license terms, you have the rights below for each license you acquire.

1. **OVERVIEW.**

   a. **Software.** The software includes desktop operating system software. This software does not include Windows Live services. Windows Live is a service available from Microsoft under a separate agreement.

   b. **License Model.** The software is licensed on a per copy per device basis.

2. **INSTALLATION AND USE RIGHTS.** Before you use the software under a license, you must assign that license to one device (physical hardware system). That device is the "licensed device." A hardware partition or blade is considered to be a separate device.

   a. **Licensed Device.** You may install one copy of the software on the licensed device. You may use the software on up to two processors on that device at one time. Except as provided in the Storage and Network Use sections below, you may not use the software on any other device.

   b. **Number of Users.** Except as provided in the Device Connections and Other Access Technologies sections below, only one user may use the software at a time.

   c. **Alternative Versions.** The software may include more than one version, such as 32-bit and 64-bit. You may use only one version at one time.

3. **ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.**

a. **Storage.** You may store one copy of the software on a storage device, such as a network server. You may use that copy to install the software on any other device to which a license has been assigned.

b. **Network Use.** Instead of installing the software on the licensed device, you may install one copy on a storage device, such as a network server. You may use that copy only to run the software on your licensed device over an internal network.

c. **Device Connections.** You may allow up to 10 other devices to access the software installed on the licensed device to use File Services, Print Services, Internet Information Services and Internet Connection Sharing and Telephony Services.

d. **Remote Access Technologies.** You may access and use the software installed on the licensed device remotely from another device using remote access technologies as follows.

- Remote Desktop. The single primary user of the licensed device may access a session from any other device using Remote Desktop or similar technologies. A "session" means the experience of interacting with the software, directly or indirectly, through any combination of input, output and display peripherals. Other users may access a session from any device using these technologies, if the remote device is separately licensed to run the software.

- Other Access Technologies. You may use Remote Assistance or similar technologies to share an active session.

e. **Other Remote Uses.** You may allow any number of devices to access the software installed on the licensed device for purposes other than those described in the Device Connections and Remote Access Technologies sections above, such as to synchronize data between devices.

f. **Use with Virtualization Technologies.** You may use the software installed on the licensed device within a virtual (or otherwise emulated) hardware system. If you do so, you may not play or access content or use applications protected by any Microsoft digital, information or enterprise rights management technology or other Microsoft rights management services or use BitLocker. We advise against playing or accessing content or using applications protected by other digital, information or enterprise rights management technology or other rights management services or using full volume disk drive encryption.

g. **Multiplexing.** Hardware or software you use to

- pool connections, or

- reduce the number of devices or users that directly access or use the software

(sometimes referred to as "multiplexing" or "pooling"), does not reduce the number of licenses you need.

h. **Font Components.** While the software is running, you may use its fonts to display and print content. You may only

- embed fonts in content as permitted by the embedding restrictions in the fonts; and
- temporarily download them to a printer or other output device to print content.

i. **Icons, images and sounds.** While the software is running, you may use but not share its icons, images, sounds, and media.

4. **MANDATORY ACTIVATION.**

Activation associates the use of the software with a specific device. During activation, the software will send information about the software and the device to Microsoft. This information includes the version, language and product key of the software, the Internet protocol address of the device, and information derived from the hardware configuration of the device. For more information, see http://go.microsoft.com/fwlink/?linkid=69497. By using the software, you consent to the transmission of this information. Before you activate, you have the right to use the version of the software installed during the installation process. Your right to use the software after the time specified in the installation process is limited unless it is activated. This is to prevent its unlicensed use. **You will not be able to continue using the software after that time if you do not activate it.** If the device is connected to the Internet, the software may automatically connect to Microsoft for activation. You can also activate the software manually by Internet or telephone. If you do so, Internet and telephone service charges may apply. Some changes to your computer components or the software may require you to reactivate the software. **The software will remind you to activate it until you do.**

5. **VALIDATION.**

a. The software will from time to time validate the software, update or require download of the validation feature of the software. Validation verifies that the software has been activated and is properly licensed. Validation also permits you to use certain features of the software or to obtain additional benefits. For more information, see http://go.microsoft.com/fwlink/?linkid=39157.

b. During a validation check, the software will send information about the software and the device to Microsoft. This information includes the version and product key of the software, and the Internet protocol address of the device. Microsoft does not use the information to identify or contact you. By using the software, you consent to the transmission of this information. For more information about validation and what is sent during a validation check, see http://go.microsoft.com/fwlink/?linkid=69500.

c. If, after a validation check, the software is found not to be properly licensed, the functionality of the software may be affected. For example, you may

- need to reactivate the software, or
- receive reminders to obtain a properly licensed copy of the software,

or you may not be able to

- use or continue to use some of the features of the software, or
- obtain certain updates or upgrades from Microsoft.

d. You may only obtain updates or upgrades for the software from Microsoft or authorized sources. For more information on obtaining updates from authorized sources see http://go.microsoft.com/fwlink/?linkid=69502.

6. **POTENTIALLY UNWANTED SOFTWARE.** If turned on, Windows Defender will search your computer for "spyware," "adware" and other potentially unwanted software. If it finds potentially unwanted software, the software will ask you if you want to ignore, disable (quarantine) or remove it. Any potentially unwanted software rated "high" or "severe," will automatically be removed after scanning unless you change the default setting. Removing or disabling potentially unwanted software may result in

   - other software on your computer ceasing to work, or

   - your breaching a license to use other software on your computer.

   By using this software, it is possible that you will also remove or disable software that is not potentially unwanted software.

7. **INTERNET-BASED SERVICES.** Microsoft provides Internet-based services with the software. It may change or cancel them at any time.

   a. **Consent for Internet-Based Services.** The software features described below and in the Windows Vista Privacy Statement connect to Microsoft or service provider computer systems over the Internet. In some cases, you will not receive a separate notice when they connect. You may switch off these features or not use them. For more information about these features, see the Windows Vista Privacy Statement at http://go.microsoft.com/fwlink/?linkid=20615. **By using these features, you consent to the transmission of this information.** Microsoft does not use the information to identify or contact you.

   Computer Information. The following features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the type of operating system, browser and name and version of the software you are using, and the language code of the device where you installed the software. Microsoft uses this information to make the Internet-based services available to you.

   - Windows Update Feature. You may connect new hardware to your device. Your device may not have the drivers needed to communicate with that hardware. If so, the update feature of the software can obtain the correct driver from Microsoft and install it on your device. You can switch off this update feature.

   - Web Content Features. Features in the software can retrieve related content from Microsoft and provide it to you. Examples of these features are clip art, templates, online training, online assistance and Appshelp. You may choose not to use these web content features.

   - Digital Certificates. The software uses digital certificates. These digital certificates confirm the identity of Internet users sending X.509 standard encrypted information. They also can be used to digitally sign files and macros, to verify the integrity and origin of the file contents. The software retrieves certificates and updates certificate revocation lists over the Internet, when available.

   - Auto Root Update. The Auto Root Update feature updates the list of trusted certificate authorities. You can switch off the Auto Root Update feature.

- Windows Media Digital Rights Management. Content owners use Windows Media digital rights management technology (WMDRM) to protect their intellectual property, including copyrights. This software and third party software use WMDRM to play and copy WMDRM-protected content. If the software fails to protect the content, content owners may ask Microsoft to revoke the software's ability to use WMDRM to play or copy protected content. Revocation does not affect other content. When you download licenses for protected content, you agree that Microsoft may include a revocation list with the licenses. Content owners may require you to upgrade WMDRM to access their content. Microsoft software that includes WMDRM will ask for your consent prior to the upgrade. If you decline an upgrade, you will not be able to access content that requires the upgrade. You may switch off WMDRM features that access the Internet. When these features are off, you can still play content for which you have a valid license.

- Windows Media Player. When you use Windows Media Player, it checks with Microsoft for

  - compatible online music services in your region;

  - new versions of the player; and

  - codecs if your device does not have the correct ones for playing content.

  You can switch off this last feature. For more information, go to http://go.microsoft.com/fwlink/?linkid=44073.

- Malicious Software Removal/Clean On Upgrade. Before installation of the software, the software will check and remove certain malicious software listed at http://www.support.microsoft.com/?kbid=890830 ("Malware") from your device. When the software checks your device for Malware, a report will be sent to Microsoft about any Malware detected or errors that occurred while the software was checking for Malware. No information that can be used to identify you is included in the report. You may disable the software's Malware reporting functionality by following the instructions found at http://www.support.microsoft.com/?kbid=890830.

- Network Connectivity Status Icon. This feature determines whether a system is connected to a network by either passive monitoring of network traffic or active DNS or HTTP queries. The query only transfers standard TCP/IP or DNS information for routing purposes. You can switch off the active query feature through a registry setting.

- Windows Time Service. This service synchronizes with time.windows.com once a week to provide your computer with the correct time. You can turn this feature off or choose your preferred time source within the Date and Time Control Panel applet. The connection uses standard NTP protocol.

- IPv6 Network Address Translation (NAT) Traversal service (Teredo). This feature helps existing home Internet gateway devices transition to IPv6. IPv6 is next generation Internet protocol. It helps enable end-to-end connectivity often needed by peer-to-peer applications. To do so, each time you start up the software the Teredo client service will attempt to locate a public Teredo Internet service. It does so by sending a query over the Internet. This query only transfers standard Domain Name Service information to determine if your computer is connected to the Internet and can locate a public Teredo service. If you

- use an application (e.g. Windows Meeting Space) that needs IPv6 connectivity or
- configure your firewall to always enable IPv6 connectivity

by default standard Internet Protocol information will be sent to the Teredo service at Microsoft at regular intervals. No other information is sent to Microsoft. You can change this default to use non-Microsoft servers. You can also switch off this feature using a command line utility named "netsh".

b. **Use of Information.** Microsoft may use the computer information, error reports, and Malware reports to improve our software and services. We may also share it with others, such as hardware and software vendors. They may use the information to improve how their products run with Microsoft software.

c. **Misuse of Internet-based Services.** You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

8. **SCOPE OF LICENSE.** The software is licensed, not sold. This agreement only gives you some rights to use the software. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. For more information, see http://www.microsoft.com/licensing/userights. You may not

- work around any technical limitations in the software;
- reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
- use components of the software to run applications not running on the software;
- make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
- publish the software for others to copy;
- rent, lease or lend the software; or
- use the software for commercial software hosting services.

9. **MICROSOFT .NET BENCHMARK TESTING.** The software includes one or more components of the .NET Framework 3.0 (".NET Components"). You may conduct internal benchmark testing of those components. You may disclose the results of any benchmark test of those components, provided that you comply with the conditions set forth at http://go.microsoft.com/fwlink/?LinkID=66406. Notwithstanding any other agreement you may have with Microsoft, if you disclose such benchmark test results, Microsoft shall have the right to disclose the results of benchmark tests it conducts of your products that compete with the applicable .NET Component, provided it complies with the same conditions set forth

at http://go.microsoft.com/fwlink/?LinkID=66406.

10. **BACKUP COPY.** You may make one backup copy of the media. You may use it only to reinstall the software.

11. **DOCUMENTATION**. Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

12. **NOT FOR RESALE SOFTWARE.** You may not sell software marked as "NFR" or "Not for Resale."

13. **UPGRADES.** To use upgrade software, you must first be licensed for the software that is eligible for the upgrade. Upon upgrade, this agreement takes the place of the agreement for the software you upgraded from. After you upgrade, you may no longer use the software you upgraded from.

14. **PROOF OF LICENSE.**

    a. **Genuine Proof of License.** If you acquired the software on a disc or other media, a genuine Microsoft proof of license label with a genuine copy of the software identifies licensed software. To be valid, this label must appear on Microsoft packaging. If you receive the label separately, it is invalid. You should keep the packaging that has the label on it to prove that you are licensed to use the software.

    b. **Windows Anytime Upgrade License.** If you upgrade the software using Windows Anytime Upgrade, your proof of license is identified by

       - the genuine Microsoft proof of license label for the software you upgraded from,

       - a digital license stored in the digital locker at Windows Marketplace, and

       - proof of purchase from a Windows Anytime Upgrade merchant that identifies the software.

    c. To identify genuine Microsoft software, see http://www.howtotell.com.

15. **REASSIGN TO ANOTHER DEVICE.**

    a. **Software Other than Windows Anytime Upgrade.** You may uninstall the software and install it on another device for your use. You may not do so to share this license between devices.

    b. **Windows Anytime Upgrade Software.** The first user of the software may reassign the license to another device one time, but only if the license terms of the software you upgraded from allows reassignment.

16. **TRANSFER TO A THIRD PARTY.**

    a. **Software Other Than Windows Anytime Upgrade.** The first user of the software may make a one time transfer of the software, and this agreement, directly to a third party. The first user must uninstall the software before transferring it separately from the device. The first user may not retain any copies.

b. **Windows Anytime Upgrade Software.** You may transfer the software directly to a third party only with the licensed device. You may not keep any copies of the software or any earlier version.

c. **Other Requirements.** Before any permitted transfer, the other party must agree that this agreement applies to the transfer and use of the software. The transfer must include the proof of license.

17. **NOTICE ABOUT THE MPEG-4 VISUAL STANDARD.** This software includes MPEG-4 visual decoding technology. MPEG LA, L.L.C. requires this notice:

    USE OF THIS PRODUCT IN ANY MANNER THAT COMPLIES WITH THE MPEG-4 VISUAL STANDARD IS PROHIBITED, EXCEPT FOR USE DIRECTLY RELATED TO (A) DATA OR INFORMATION (i) GENERATED BY AND OBTAINED WITHOUT CHARGE FROM A CONSUMER NOT THEREBY ENGAGED IN A BUSINESS ENTERPRISE, AND (ii) FOR PERSONAL USE ONLY; AND (B) OTHER USES SPECIFICALLY AND SEPARATELY LICENSED BY MPEG LA, L.L.C.

    If you have questions about the MPEG-4 visual standard, please contact MPEG LA, L.L.C., 250 Steele Street, Suite 300, Denver, Colorado 80206; http://www.mpegla.com.

18. **NOTICE ABOUT THE VC-1 VISUAL STANDARD.** This software may include VC-1 visual decoding technology. MPEG LA, L.L.C. requires this notice:

    THIS PRODUCT IS LICENSED UNDER THE VC-1 PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (A) ENCODE VIDEO IN COMPLIANCE WITH THE VC-1 STANDARD ("VC-1 VIDEO") OR (B) DECODE VC-1 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE VC-1 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE.

    If you have questions about the VC-1 visual standard, please contact MPEG LA, L.L.C., 250 Steele Street, Suite 300, Denver, Colorado 80206; http://www.mpegla.com.

19. **THIRD PARTY PROGRAMS.** The software contains third party programs. The license terms with those programs apply to your use of them.

20. **EXPORT RESTRICTIONS.** The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see http://www.microsoft.com/exporting.

21. **SUPPORT SERVICES.** Microsoft provides support services for the software as described at http://www.support.microsoft.com/common/international.aspx. If you are using software that is not properly licensed, you will not be entitled to receive support services.

22. **ENTIRE AGREEMENT.** This agreement (including the warranty below), additional terms and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

23. **APPLICABLE LAW.**

    a. **United States.** If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. **Outside the United States.** If you acquired the software in any other country, the laws of that country apply.

24. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your state or country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your state or country if the laws of your state or country do not permit it to do so.

25. **LIMITATION ON AND EXCLUSION OF DAMAGES. You can recover from Microsoft and its suppliers only direct damages up to the amount you paid for the software. You cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages.**

This limitation applies to

- anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if

- repair, replacement or a refund for the software does not fully compensate you for any losses; or
- Microsoft knew or should have known about the possibility of the damages.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. They also may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

****

LIMITED WARRANTY

A. **LIMITED WARRANTY.** If you follow the instructions and the software is properly licensed, the software will perform substantially as described in the Microsoft materials that you receive in or with the software.

B. **TERM OF WARRANTY; WARRANTY RECIPIENT; LENGTH OF ANY IMPLIED WARRANTIES. The limited warranty covers the software for one year after acquired by the first user. If you receive supplements, updates, or replacement software during that year, they will be covered for the remainder of the warranty or 30 days, whichever is longer.** If the first user transfers the software, the remainder of the warranty will apply to the recipient.

To the extent permitted by law, any implied warranties, guarantees or conditions last only during the term of the limited warranty. Some states do not allow limitations on how long an implied warranty lasts, so these limitations may not apply to you. They also might not apply to you because some countries may not allow limitations on how long an implied warranty, guarantee or condition lasts.

C. **EXCLUSIONS FROM WARRANTY.** This warranty does not cover problems caused by your acts (or failures to act), the acts of others, or events beyond Microsoft's reasonable control.

D. **REMEDY FOR BREACH OF WARRANTY. Microsoft will repair or replace the software at no charge. If Microsoft cannot repair or replace it, Microsoft will refund the amount shown on your receipt for the software. It will also repair or replace supplements, updates and replacement software at no charge. If Microsoft cannot repair or replace them, it will refund the amount you paid for them, if any. You must uninstall the software and return any media and other associated materials to Microsoft with proof of purchase to obtain a refund. These are your only remedies for breach of the limited warranty.**

E. **CONSUMER RIGHTS NOT AFFECTED. You may have additional consumer rights under your local laws, which this agreement cannot change.**

F. **WARRANTY PROCEDURES.** You need proof of purchase for warranty service.

1. **United States and Canada.** For warranty service or information about how to obtain a refund for software acquired in the United States and Canada, contact Microsoft at

   - (800) MICROSOFT;
   - Microsoft Customer Service and Support, One Microsoft Way, Redmond, WA 98052-6399; or
   - visit http://www.microsoft.com/info/nareturns.htm.

2. **Europe, Middle East and Africa.** If you acquired the software in Europe, the Middle East or Africa, Microsoft Ireland Operations Limited makes this limited warranty. To make a claim under this warranty, you should contact either

- Microsoft Ireland Operations Limited, Customer Care Centre, Atrium Building Block B, Carmanhall Road, Sandyford Industrial Estate, Dublin 18, Ireland; or

- the Microsoft affiliate serving your country (see http://www.microsoft.com/worldwide).

3. **Outside United States, Canada, Europe, Middle East and Africa.** If you acquired the software outside the United States, Canada, Europe, the Middle East and Africa, contact the Microsoft affiliate serving your country (see http://www.microsoft.com/worldwide).

G. **NO OTHER WARRANTIES. The limited warranty is the only direct warranty from Microsoft. Microsoft gives no other express warranties, guarantees or conditions. Where allowed by your local laws, Microsoft excludes implied warranties of merchantability, fitness for a particular purpose and non-infringement.** If your local laws give you any implied warranties, guarantees or conditions, despite this exclusion, your remedies are described in the Remedy for Breach of Warranty clause above, to the extent permitted by your local laws.

H. **LIMITATION ON AND EXCLUSION OF DAMAGES FOR BREACH OF WARRANTY. The Limitation on and Exclusion of Damages clause above applies to breaches of this limited warranty.**

This warranty gives you specific legal rights, and you may also have other rights which vary from state to state. You may also have other rights which vary from country to country.

EULAID:VISTA_RM.0_BUS_RTL_en-US

MICROSOFT SOFTWARE LICENSE AGREEMENT

WINDOWS 8

Thank you for choosing Microsoft Windows 8. This is a license agreement between you and Microsoft Corporation (or, based on where you live, one of its affiliates) that describes your rights to use the Windows 8 software. For your convenience, we've organized this agreement into two parts. The first part includes introductory terms phrased in a question and answer format; the Additional Terms and Limited Warranty follow and contain greater detail. You should review the entire agreement, including any linked terms, because all of the terms are important and together create this contract that applies to you. You can review linked terms by pasting the forward link into your browser window once the software is running. **The Additional Terms contain a binding arbitration clause and class action waiver. If you live in the United States, these affect your rights to resolve a dispute with Microsoft, and you should read them carefully.**

By accepting this agreement or using the software, you agree to all of these terms and consent to the transmission of certain information during activation and for Internet-based features of the software. If you do not accept and comply with these terms, you may not use the software or features. Instead, you should return it to the retailer or other place where you purchased the software license, for a refund or credit.

How can I use the software? We do not sell our software or your copy of it – we only license it. Under our license, we grant you the right to install and run that one copy on one computer (the licensed computer), for use by one person at a time, but only if you comply with all the terms of this agreement. Typically, this means you can install one copy of the software on a personal computer and then you can use the software on that computer. The software is not licensed to be used as server software or for commercial hosting - so you may not make the software available for simultaneous use by multiple users over a network. For more information on multiple user scenarios and virtualization, see the Additional Terms.

May I make a backup copy? Yes, you may make a single copy of the software for backup purposes, and use that backup copy as described below.

What about upgrading the software? The software covered by this agreement is an upgrade to your existing operating system software, so the upgrade replaces the original software that you are upgrading. You do not retain any rights to the original software after you have upgraded and you may not continue to use it or transfer it in any way. This agreement governs your rights to use the upgrade software and replaces the agreement for the software from which you upgraded. After you complete your upgrade, additional software will be required to playback or record certain types of media, including DVDs.

Can I transfer the software to another computer or user? You may transfer the software to another computer that belongs to you. You may also transfer the software (together with the license) to a computer owned by someone else if a) you are the first licensed user of the software and b) the new user agrees to the terms of this agreement. To make that transfer, you must transfer the original media, the certificate of authenticity, the product key and the proof of purchase directly to that other person, without retaining any copies of the software. You may use the backup copy we allow you to make or the media that the software came on to transfer the software. Anytime you transfer the software to a new computer, you must remove the software from the prior computer. You may not transfer the software to share licenses between computers. You may transfer Get Genuine Windows software, Pro Pack or Media Center Pack software only together with the licensed computer.

How does Internet activation work? The first time you connect to the Internet while using the software, the software will automatically contact Microsoft or its affiliate to confirm the software is genuine, and the license is associated with the licensed computer. This process is called "activation." Because activation is meant to identify unauthorized changes to the licensing or activation functions of the software, and to otherwise prevent unlicensed use of the software, **you may not bypass or circumvent activation**.

Does the software collect my personal information? If you connect your computer to the Internet, some features of the software may connect to Microsoft or service provider computer systems to send or receive information, including personal information. You may not always receive a separate notice when they connect. If you choose to use any of these features, you agree to send or receive this information when using that feature. Many of these features can be switched off or you can choose not to use them.

How do we use your information? Microsoft uses the information it collects through the software features to upgrade or fix the software and otherwise improve our products and services. In certain circumstances, we also share it with others. For example, we share error reports with relevant hardware and software vendors, so that they can use the information to improve how their products run with Microsoft products. You agree that we may use and disclose the information as described in our Privacy Statement, at go.microsoft.com/fwlink/?linkid=190175.

What does this agreement apply to? This agreement applies to the software, the media on which you received the software, and also any Microsoft updates, supplements, and services for the software, unless other terms come with them. It also applies to Windows apps that are included with Windows, which are separate from the software features.

Are there things I'm not allowed to do with the software? Yes. Because the software is licensed, not sold, Microsoft reserves all rights (such as rights under intellectual property laws) not expressly granted in this agreement. In particular, this license does not give you any right to, and you may not: use or virtualize features of the software separately, publish, copy (other than the permitted backup copy), rent, lease, or lend the software; transfer the software (except as permitted by this agreement), attempt to circumvent technical protection measures in the software, reverse engineer, decompile, or disassemble the software, except if the laws where you live permit this even when our agreement does not. In that case, you may do only what your law allows. When using Internet-based features or Microsoft Family Safety, you may not use those features in any way that could interfere with anyone else's use of them, or to try to gain access to any service, data, account or network, in an unauthorized manner.

ADDITIONAL TERMS

1. License Rights and Multi User Scenarios

a. Computer. In this agreement, "computer" means a hardware system (whether physical or virtual) with an internal storage device capable of running the software. A hardware partition or blade is considered to be a computer. The software is licensed to run on only one processor on the licensed computer.

b. Multiple versions. The software includes multiple versions (such as 32-bit and 64-bit versions), and you may install only one of those versions.

c. Multiple or pooled connections. Hardware or software you use to multiplex or pool connections, or reduce the number of devices or users that access or use the software does not reduce the number of licenses you need. You may only use such hardware or software if you have a license for each copy of the software you are using.

d. Device connections**.** You may allow up to 20 other devices to access the software installed on the licensed computer for the purpose of using file services, print services, Internet information services, and Internet connection sharing and telephony services on the licensed computer. You may allow any number of devices to access the software on the licensed computer to synchronize data between devices. This section does not mean, however, that you have the right to install the software, or use the primary function of the software (other than the features listed in this section) on any of these other devices.

e. Use in a virtualized environment. If you use virtualization software to create one or more virtual computers on a single computer hardware system, each virtual computer, and the physical computer, is considered a separate computer for purposes of this agreement. This license allows you to install only one copy of the software for use on one computer, whether that computer is physical or virtual. If you want to use the software on more than one virtual computer, you must obtain separate copies of the software and a separate license for each copy. Content protected by digital rights management technology or other full-volume disk drive encryption technology may be less secure in a virtualized environment.

f. Remote access. The software contains Remote Desktop and Remote Assistance technologies that enable the software or applications installed on the licensed computer to be accessed remotely from other devices.

- Remote Desktop. Remote Desktop or similar technologies is licensed for outbound use from this computer. You may access certain editions of Windows software running on a separately licensed host pc from this computer, by using Remote Desktop.

- Remote Assistance. You may use Remote Assistance or similar technologies to share an active session without obtaining any additional licenses for the software. Remote Assistance allows one user to directly connect to another user's computer, usually to correct problems.

2. Binding Arbitration and Class Action Waiver

a. Application. This Section 2 applies to any dispute **EXCEPT IT DOES NOT INCLUDE A DISPUTE RELATING TO THE ENFORCEMENT OR VALIDITY OF YOUR, MICROSOFT'S, OR EITHER OF OUR LICENSORS' INTELLECTUAL PROPERTY RIGHTS.** Dispute means any dispute, action, or other controversy between you and Microsoft concerning the software (including its price) or this agreement, whether in contract, warranty, tort, statute, regulation, ordinance, or any other legal or equitable basis. "Dispute" will be given the broadest possible meaning allowable under law.

b. Notice of dispute. In the event of a dispute, you or Microsoft must give the other a Notice of Dispute, which is a written statement of the name, address and contact information of the party giving it, the facts giving rise to the dispute, and the relief requested. You must send any Notice of Dispute by U.S. Mail to **Microsoft Corporation, ATTN: LCA ARBITRATION, One Microsoft Way, Redmond, WA 98052-6399. A form is available at go.microsoft.com/fwlink/?linkid=245499.** Microsoft will send any Notice of Dispute to you by U.S. Mail to your address if we have it, or otherwise to your e-mail address. You and Microsoft will attempt to resolve any dispute through informal negotiation within 60 days from the date the Notice of Dispute is sent. After 60 days, you or Microsoft may commence arbitration.

c. Small claims court. You may also litigate any dispute in small claims court in your county of residence or King County, Washington, if the dispute meets all requirements to be heard in the small claims court. You may litigate in small claims court whether or not you negotiated informally first.

d. Binding arbitration. **If you and Microsoft do not resolve any dispute by informal negotiation or in small claims court, any other effort to resolve the dispute will be conducted exclusively by binding arbitration. You are giving up the right to litigate (or participate in as a party or class member) all disputes in court before a judge or jury.** Instead, all disputes will be resolved before a neutral arbitrator, whose decision will be final except for a limited right of appeal under the Federal Arbitration Act. Any court with jurisdiction over the parties may enforce the arbitrator's award.

e. Class action waiver. **Any proceedings to resolve or litigate any dispute in any forum will be conducted solely on an individual basis. Neither you nor Microsoft will seek to have any dispute heard as a class action, private attorney general action, or in any other proceeding in which either party acts or proposes to act in a representative capacity. No arbitration or proceeding will be combined with another without the prior written consent of all parties to all affected arbitrations or proceedings.**

f. Arbitration procedure, costs, fees and incentives. Any arbitration will be conducted by the American Arbitration Association (the "AAA") under its Commercial Arbitration Rules and in many cases its Supplementary Procedures for Consumer-Related Disputes. For more information, see adr.org or call 1-800-778-7879. In a dispute involving $75,000 or less, Microsoft will promptly reimburse your filing fees and pay the AAA's and arbitrator's fees. You and Microsoft agree to the terms governing procedures, fees and incentives at go.microsoft.com/fwlink/?linkid=245495. To commence arbitration, submit the form available at go.microsoft.com/fwlink/?linkid=245497 to the AAA. You agree to commence arbitration only in your county of residence or in King County, Washington. Microsoft agrees to commence arbitration only in your county of residence.

g. Claims or disputes must be filed within one year. To the extent permitted by law, any claim or dispute under this agreement to which Section 2 applies must be filed within one year in small claims court (Section 2.c) or in arbitration (Section 2.d). The one-year period begins when the claim or dispute first could be filed. If such a claim or dispute is not filed within one year, it is permanently barred.

h. Severability. If the class action waiver in Section 2.e is found to be illegal or unenforceable as to all or some parts of a dispute, then Section 2 (arbitration) will not apply to those parts. Instead, those parts will be severed and proceed in a court of law, with the remaining parts proceeding in arbitration. If any other provision of Section 2 is found to be illegal or unenforceable, that provision will be severed with the remainder of Section 2 remaining in full force and effect.

3. CHOICE OF LAW

The laws of the state or country where you live govern all claims and disputes under this agreement, including breach of contract claims and claims under state consumer protection laws, unfair competition laws, implied warranty laws, for unjust enrichment, and in tort. If you acquired the software in any other country, the laws of that country apply. This agreement describes certain legal rights. You may have other rights, including consumer rights, under the laws of your state or country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change those other rights if the laws of your state or country do not permit it to do so.

4. ACTIVATION

a. More on how activation works. The software will notify you whether the installed copy of the software is properly licensed. During activation, the software will send information about the software and your computer to Microsoft. This information includes the version, language, and product key of the software, the Internet protocol address of the computer, and information derived from the hardware configuration of the computer. For more information about activation, see go.microsoft.com/fwlink/?linkid=190175. If the licensed computer is connected to the Internet, the software will automatically connect to Microsoft for activation. You can also activate the software manually by Internet or telephone. In either case, Internet and telephone service charges may apply.

b. Re-activation. Some changes to your computer components or the software may require re-activation of the software.

c. Activation failure. During online activation, if the licensing or activation functions of the software are found to be counterfeit, improperly licensed, or include unauthorized changes, activation will fail and the software will attempt to repair itself by replacing any tampered Microsoft software with genuine Microsoft software. The software will notify you if the installed copy of the software is improperly licensed or includes unauthorized changes. In addition, you may receive reminders to obtain a properly licensed copy of the software. You may not be able to obtain certain updates or upgrades from Microsoft if your copy of the software is found to be improperly licensed.

5. INTERNET-BASED FEATURES; PRIVACY

The following software features use Internet protocols, which send to Microsoft (or its suppliers or service providers) computer information, such as your Internet protocol address, the type of operating system, browser and name and version of the software you are using, and the language code of the computer where you installed the software. Microsoft uses this information to make the Internet-based features available to you, in accordance with the Windows 8 Privacy Statement, at go.microsoft.com/fwlink/?linkid=190175. Some Internet-based features may be delivered at a later date via Microsoft's Windows Update service--if, for example, you acquire an application that relies on one of those services.

a. Windows Update. If you use the Windows Update service in the software, updates or downloads to the Windows Update service will be required for proper functioning of the service, from time to time, and will be downloaded and installed without further notice to you.

b. Windows Digital Rights Management technology. Some content owners use Windows digital rights management technology (WDRM) to protect their copyrights and other intellectual property, including by disabling the software's ability to play protected content if WDRM fails. You agree that Microsoft may include a revocation list with the licenses.

c. Windows Media Player. When you use Windows Media Player, it checks with Microsoft for compatible online music services in your region and new versions of the player. You may only use Windows Media Player as described at go.microsoft.com/fwlink/?linkid=104605.

d. Windows Defender. If turned on, Windows Defender will search your computer for many types of malicious software, including viruses, worms, bots, rootkits, "spyware", "adware" and other potentially unwanted software. If you choose the "recommended" security settings when you first start using the software, such malware and other potentially unwanted software rated "high" or "severe" will automatically be removed. This removal may result in other software on your computer ceasing to work or your breaching a license to use that software. It is possible that software that is not unwanted may be removed or disabled. If you use Windows Defender and Windows Update, Windows Defender is regularly updated through Windows Update.

e. Malicious software removal. If you use Windows Update, at least once each month the software will scan for and remove from your computer the malware listed at go.microsoft.com/fwlink/?linkid=241725. After the scan completes, a report will be sent to Microsoft with specific information about malware detected, errors, and other information about your computer. This information is used to improve the software and other Microsoft products. You may disable the software's reporting functionality by following the instructions found at go.microsoft.com/fwlink/?linkid=241725.

f. SmartScreen Filter. If enabled, the SmartScreen Filter will check the addresses of webpages and downloads you attempt to view against a frequently updated list of webpages and downloads that have been reported to Microsoft as unsafe or suspicious. SmartScreen will also check downloaded programs that you attempt to run against a list of commonly downloaded or run programs to help you make more informed trust decisions. More information can be found by visiting the Internet Explorer Privacy Statement go.microsoft.com/fwlink/?linkid=239590. By enabling SmartScreen in either Windows or Internet Explorer, you consent to this feature, and you agree to use the SmartScreen Filter only in conjunction with Windows or Internet Explorer. You may not, either manually or by enabling or authorizing any software or service, copy, display, distribute, collect or store any data provided by the SmartScreen Filter.

g. IPv6 Network Address Translation (NAT) Traversal service (Teredo). Each time you start your licensed computer, Teredo will attempt to locate a public Internet Protocol version 6 (IPv6) service on the Internet. This occurs automatically when your licensed computer is connected to a public or private network, but does not occur on managed networks such as enterprise domains. If you use a program that requires Teredo to use IPv6 connectivity, or if you configure your firewall to always enable IPv6 connectivity, then Teredo will periodically contact the Microsoft Teredo service over the Internet. The only information sent to Microsoft is standard computer information and the name of the service requested (for example teredo.ipv6.microsoft.com). The information sent from your computer by Teredo is used to determine if your computer is connected to the Internet and if it can locate a public IPv6 service. Once the service is located, information is sent to maintain a connection with the IPv6 service.

h. Plug and Play and Plug and Play Extensions. Your computer may not have the drivers needed to communicate with hardware that you connect to your computer. If so, the update feature of the software can obtain and install the correct driver on your computer. An administrator can disable this update feature.

i. Digital certificates. The software uses digital certificates to confirm the identity of Internet users sending X.509 standard encrypted information, to digitally sign files and macros, and to verify the integrity and origin of file contents. The software may retrieve and update certificates, certificate revocation lists, and the list of trusted certification authorities, over the Internet.

j. Network awareness. This feature determines whether a system is connected to a network by either passive monitoring of network traffic or active DNS or HTTP queries. The query transfers only standard TCP/IP or DNS information for routing purposes. You can switch off the active query feature through a registry setting.

k. Accelerators. When you click on or move your mouse over an Accelerator in Internet Explorer, any of the following may be sent to the applicable service provider (which may not be Microsoft): the title and full web address or URL of the current webpage, standard computer information, and any content you have selected. For more information, see go.microsoft.com/fwlink/?linkid=239590.

l. Search provider update. The software will download an update to the data on your computer about search providers. This update upgrades your providers with the latest features, such as new icons or search suggestions. This is a one-time update, but the software will try to perform the update several times if it does not successfully download the update. For more information, see go.microsoft.com/fwlink/?linkid=239590.

m. Cookies. If you choose to use online features in the software, such as online Help and Support, cookies may be set. To learn how to block, control and delete cookies, please read the cookies section of the privacy statement at go.microsoft.com/fwlink/?linkid=74170.

n. Windows Store. In addition to the terms of this agreement for Internet based features, you may only use the Windows Store under the terms available at go.microsoft.com/fwlink/?linkid=246694. Those terms also contain information about Windows Notification Service. Windows apps or any preinstalled apps in your Start may use Windows Notification Service. You agree that we may send you notifications as described in the Windows 8 Privacy Statement and Windows Store terms of service.

6. WINDOWS APPS

Windows apps (such as Mail, Messaging, Calendar and People) are apps that are developed by Microsoft, included with Windows, and licensed to you under this agreement. You can access each Windows app from its corresponding tile in Start. Some of the Windows apps provide an access point to online services, and the use of those services is sometimes governed by separate terms and privacy policies. You can view these terms and policies by looking at the app's settings. Unless other terms are displayed to you or presented in the app's settings, you agree the services that you access from the Windows apps are governed by the Microsoft Services Agreement at go.microsoft.com/fwlink/?linkid=246338, or for Windows apps that access Xbox services, the xbox.com/legal/livetou. We continuously work to improve the services and we may change the services at any time. The services may not be available in certain countries. You may choose to uninstall any Windows app at any time, and you may also choose to reinstall any Windows app by downloading it from the Windows Store. Some Windows apps include advertising. You may choose to opt out of personalized advertising by visiting choice.live.com.

7. PROOF OF LICENSE

If you acquired the software on a disc or other physical media, your proof of license is the genuine Microsoft certificate of authenticity label with the accompanying genuine product key, and your proof of purchase. If you acquired and downloaded the software online, your proof of license is the genuine Microsoft product key for the software that you received with your purchase, and your proof of purchase from an authorized electronic supplier of genuine Microsoft software. Proof of purchase may be subject to verification by your merchant's records.

8. UPDATES AND UPGRADES

You may only obtain updates or upgrades for the software from Microsoft or authorized sources. Certain upgrades, support, and other services may be offered only to users of genuine Microsoft software. For more information about Genuine Windows, see go.microsoft.com/fwlink/?linkid=104612. To identify genuine Microsoft software, see howtotell.com.

9. LIMITED RIGHTS VERSIONS

Some versions of the software, like Not for Resale and Academic Edition software, are distributed for limited purposes. You may not sell software marked as "NFR" or "Not for Resale", and you must be a Qualified Educational User to use software marked as "Academic Edition" or "AE." If you want to find out more about academic software, or you want to find out if you are a Qualified Educational User, visit microsoft.com/education or contact the Microsoft affiliate serving your country for more information.

10. FONTS, ICONS, IMAGES, AND SOUNDS

a. Font components. While the software is running, you may use its fonts to display and print content. You may temporarily download the fonts to a printer or other output device to print content, and you may embed fonts in content only as permitted by the embedding restrictions in the fonts.

b. Icons, images, and sounds. While the software is running, you may access and use its icons, images, sounds, and media only from the licensed computer. You may not share the sample images, sounds and media provided with the software or use them for any other purpose.

11. .NET FRAMEWORK

The software includes one or more components of the .NET Framework, which you may use only as described at go.microsoft.com/fwlink/?linkid=66406, if you use the .NET Framework components to conduct internal benchmark testing.

12. H.264/AVC AND MPEG-4 VISUAL STANDARDS AND VC-1 VIDEO STANDARDS

THIS PRODUCT IS LICENSED UNDER THE AVC, THE VC-1, AND THE MPEG-4 PART 2 VISUAL PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE STANDARDS ("VIDEO STANDARDS") AND/OR (ii) DECODE AVC, VC-1, AND MPEG-4 PART 2 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERICAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C SEE MPEGLA.COM.

13. ADOBE FLASH PLAYER

The software may include a version of Adobe Flash Player. You agree that your use of the Adobe Flash Player is governed by the license terms for Adobe Systems Incorporated, at go.microsoft.com/fwlink/?linkid=248532. Adobe and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

14. GEOGRAPHIC AND EXPORT RESTRICTIONS

If there is a geographic region indicated on your software packaging, then you may activate the software only in that region. You must also comply with all domestic and international export laws and regulations that apply to the software, which include restrictions on destinations, end users, and end use. For further information on geographic and export restrictions, visit go.microsoft.com/fwlink/?linkid=141397 and microsoft.com/exporting.

15. SUPPORT AND REFUND PROCEDURES

Microsoft provides limited support services for properly licensed software as described at support.microsoft.com/common/international.aspx.

If you are seeking a refund, and you cannot obtain one where you acquired the software, contact Microsoft for information about Microsoft's refund policies. See microsoft.com/worldwide, or in North America, call (800) MICROSOFT or see microsoft.com/info/nareturns.htm.

16. ENTIRE AGREEMENT

This agreement (together with terms accompanying any software supplements, updates, and services that are provided by Microsoft and that you use), and the terms contained in web links listed in this agreement, are the entire agreement for the software and any such supplements, updates, and services (unless Microsoft provides other terms with such supplements, updates, or services). You can review this agreement after your software is running by going to microsoft.com/about/legal/en/us/intellectualproperty/useterms/default.aspx or by following the instructions in the Action Center-Windows Activation within the software. You can also review the terms at any of the links in this agreement after your software is running by typing the urls into your browser address bar, and you agree to do so. You agree that for each service or included app that is governed by this agreement and also specific terms linked in this agreement, you will read the terms for that service before using the service. You understand that by using the service, you ratify this agreement and the linked terms. There are also informational links in this agreement. The links containing terms that bind you and us are:

- go.microsoft.com/fwlink/?linkid=190175 (Windows 8 Privacy Statement);
- go.microsoft.com/fwlink/?linkid=245495 (Arbitration Procedure)
- go.microsoft.com/fwlink/?linkid=104605 (Windows Media Player)
- go.microsoft.com/fwlink/?linkid=246694 (Windows Store Terms of Use)
- go.microsoft.com/fwlink/?linkid=246338 (Microsoft Services Agreement)
- xbox.com/legal/livetou (XBox Live Terms of Use)
- go.microsoft.com/fwlink/?linkid=66406 (.NET Framework Terms)
- go.microsoft.com/fwlink/?linkid=248532 (Adobe Flash Player License Terms)

LIMITED WARRANTY

Does Microsoft provide a LIMITED WARRANTY for the software? Yes. Microsoft warrants that properly licensed software will perform substantially as described in any Microsoft materials that accompany the software. This limited warranty does not cover problems that you cause, or that arise when you fail to follow our instructions, or that are caused by events beyond Microsoft's reasonable control. The limited warranty starts when the first user of your copy of the software acquires that copy, and lasts for one year. Any supplements, updates, or replacement software that you may receive from Microsoft during that year are also covered, but only for the remainder of that one year period or for 30 days, whichever is longer. Transferring the software will not extend the term of the limited warranty. Microsoft gives no other express warranties, guarantees, or conditions. **Microsoft excludes all implied warranties, including those of merchantability, fitness for a particular purpose, and non-infringement. If your local law does not allow Microsoft's exclusion of implied warranties, then any implied warranties, guarantees, or conditions last only during the term of the limited warranty and are limited as much as your local law allows. If your local law requires a longer limited warranty term, despite this agreement, then that longer term will apply, but you can recover only the remedies that are described in this agreement.** A section near the end of this agreement explains how you can make a claim under the limited warranty.

What if Microsoft breaches its warranty? If Microsoft breaches its limited warranty, your only remedy is the repair or replacement of the software. We also have the option to refund to you the price you paid for the software instead of repairing or replacing it. Prior to refund, **you must uninstall the software and return it to Microsoft with proof of purchase.**

What if Microsoft breaches any part of this agreement? If you have any basis for recovering damages from Microsoft, you can recover only direct damages up to the amount that you paid for the software. **You may not recover any other damages, including consequential, lost profits, special, indirect, or incidental damages.** The damage exclusions and limitations in this agreement apply even if repair, replacement or a refund for the software does not fully compensate you for any losses or if Microsoft knew or should have known about the possibility of the damages. Some states and countries do not allow the exclusion or limitation of incidental, consequential, or other damages, so those limitations or exclusions may not apply to you. **If your local law allows you to recover other damages from Microsoft even though we do not, you cannot recover more than you paid for the software.**

WARRANTY PROCEDURES

You need proof of purchase for service under the limited warranty.

1. United States and Canada. For limited warranty service or information about how to obtain a refund for software acquired in the United States and Canada, contact Microsoft via telephone at (800) MICROSOFT; via mail at Microsoft Customer Service and Support, One Microsoft Way, Redmond, WA 98052-6399; or visit microsoft.com/info/nareturns.htm.

2. Europe, Middle East and Africa. If you acquired the software in Europe, the Middle East, or Africa, Microsoft Ireland Operations Limited makes the limited warranty. To make a claim under the limited warranty, you must contact either Microsoft Ireland Operations Limited, Customer Care Centre, Atrium Building Block B, Carmanhall Road, Sandyford Industrial Estate, Dublin 18, Ireland, or the Microsoft affiliate serving your country (see microsoft.com/worldwide).

3. Australia. If you acquired the software in Australia, contact Microsoft to make a claim at 13 20 58; or Microsoft Pty Ltd, 1 Epping Road, North Ryde NSW 2113 Australia.

4. Other Countries. If you acquired the software in another country, contact the Microsoft affiliate serving your country (see microsoft.com/worldwide).

EULAID:Win_RM_2_CC_R_en-us

Microsoft

Community

Sign in

Home Categories Participate Additional Support

Announcements: 1

Virus and Malware

Applies to: Virus and Malware | Microsoft Security Essentials | Scanning, Detecting, and Removing Threats | Windows 7

Question

[redacted] asked on November 18, 2013 | 64 views

1 Had this question Me Too

Win32/Ramnit

Hi there,

I have receiced a message from Microsoft Action Centre today telling me M.Security Essentials had found 'Win32/Ramnit' on my computer & had removed it. They say:
'We strongly recommend that you change all passwords immediately for websites that require a password, especially banking websites and other sites that store personal info.'
I understand they wouldn't suggest this for the fun of it but is it entirely necessarry to do this for ALL passwords as I have so many? Surely this malware removed by M.S.Essentials is gone for good or would remove it again if it reared its ugly head at a later date? If I have to change them all I will (I have changed some already) but I am wondering if anyone else out there is more clued up on this issue & can advise otherwise? Hope someone can be of help. Thanks a lot :o)

Reply | Reply with quote | Report abuse | Subscribe to updates

Answer

[redacted] replied on November 18, 2013

1 Found this helpful Me Too

Hi,

This is a pretty standard recommendation in the IT world. The main idea is you had something on your

Related Content

Win32/Ramnit.A

Please help MSE will not remove Win32/Ramnit trojan?

WSE won't remove Virus:Win32/Ramnit.B

MSE detects and removes Win32\Ramnit.gen!B, but it keeps returning.

Trojan:Win32/Ramnit.A keeps coming back

system that made it insecure. In general when you have one security issue the chance of you having others is much higher. So I hoped after finding something you used other scanners to make sure you were clean. As no one scanner is 100% effective.

All that being said the other reason you hear this recommendation allot is that people have very bad password habits, often using just one password or a simple variation of one password for all their online accounts.

So once a hacker gets your email address and password from a virus that collects your data and keystrokes, they can then head off to all the popular websites and test if your email and password also works on other sites.

This is the main reason people will tell you to change your password after this sort of event. Also how do you know how long the virus has been logging your data on your system? And what passwords might have been logged?

You should be changing your passwords a few times a year at least anyway. And make sure each account has a different "STRONG" password.

I made a password creation utility on my website if you need help making up new strong passwords...

[redacted]

Also if you have not rescanned your computer with alternate scanners this small list may help you find what you need....

Malwarebytes Anti-malware
http://www.malwarebytes.org/

Junkware Removal
http://www.bleepingcomputer.com/download/junkware-removal-tool/

AdwCleaner
http://www.bleepingcomputer.com/download/adwcleaner/

Hitman Pro
http://www.surfright.nl/en/hitmanpro/

Goog luck

Reply | Reply with quote | Report abuse ▾

All Replies (5)

[redacted] replied on November 18, 2013 ▾

0 Found this helpful
Me Too

In reply to [redacted] post on November 18, 2013

Thanks [redacted]

For your quick advice & list of alternate scanners.
Can I just ask you question you further...Does Microsoft Security Essentials only scan, find & remove the malware, then obviously warn & advise you. Does it not prevent it from 'reading', scanning or logging my data from the very start? Sorry I'm not totally clued up or fully understand most of these security issues :o/
Regards [redacted]

Reply | Reply with quote | Report abuse

[redacted] replied on November 18, 2013

1 Found this helpful
Me Too

In reply to [redacted] post on November 18, 2013

Hi,

Not necessarily. Microsoft Security Essentials is free (bear that in mind) and it really depends on how you have configured it. By default, the program should disable threats and prompt the user on what to do. So, it <u>may</u> have stopped the malware from logging any data, but there is the threat of times in which the protection was not running, malfunctioning or disabled. So I would advise you to change at least all the passwords or any sensitive data that you entered on the insecure computer while it was infected. But if I was you, I would change them all. Just to be safe.

Regards,

[redacted]

Reply | Reply with quote | Report abuse

[redacted] replied on November 18, 2013

0 Found this helpful
Me Too

In reply to [redacted] post on November 18, 2013

Thanks [redacted] I will do then! Very much appreciated. Tina

Reply | Reply with quote | Report abuse

[redacted] replied on November 18, 2013

In reply to [redacted] post on November 18, 2013

1 Found this helpful
Me Too

It's no problem at all. I hope I helped.

[redacted]

Reply | Reply with quote | Report abuse

English

Microsoft Community Code of Conduct Community Participation Center
Trademarks Privacy & Cookies Terms of Use

Microsoft

Register a free account to unlock additional features at BleepingComputer.com

Welcome to **BleepingComputer**, a free community where people like yourself come together to discuss and learn how to use their computers. Using the site is easy and fun. As a guest, you can browse and view the various discussions in the forums, but can not create a new topic or reply to an existing one unless you are logged in. Other benefits of registering an account are subscribing to topics and forums, creating a blog, and having **no ads** shown anywhere on the site.

Click here to Register a free account now! or read our **Welcome Guide** to learn how to use this site.

Ramnit infection

Started by agre , Sep 26 2010 09:22 PM

agre

Posted 26 September 2010 - 09:22 PM

Well, I know I am infected and am wondering what (if anything) I can do. I have a Lenovo ThinkPad T61 running Windows XP SP3.

Earlier this week one of the kids called to tell me about a pop-up indicating an infection. Thinking the pop-up itself could be generated by malware, I had him shut the machine down and initiated a full scan with Symantec Endpoint Protection when I got back to the house. It went through about 8,000 files before hitting on a file called Ramnit. The next 700 files or so were also Ramnit hits. Although Symantec claimed it was quarantining each hit, I thought it might be propogating itself so I stopped the scan and tried to restore the system to last weekend when it seemed to be running fine.

After the next start-up, and on every start-up since, I received the following message: "The file or directory c:/Program Files/Common Files/Symantec Shared/ EENGINE/EPERSIST.DAT is corrupt and unreadable. Please run the chkdisk utility." When trying to run chkdisk from Windows it tells me some files are in use and I need to run it on my next re-start. On re-start I'm told, "Can not open volume for direct access. Windows has finished checking the disk." The machine also runs very slowly, and sometimes it boots to a blue screen with no icons (although I can generate the task manager via CTRL-ALT-DEL and view processes when this happens.)

I've seen a number of threads here that suggest reformatting is the only option. Is this truly a unanimous consensus?

Thanks in advance for any assistance that can be provided.

BC AdBot (Login to Remove)

boopme

Posted 26 September 2010 - 10:08 PM

It truly is... ☹
RAMNIT = VIRUT
Trojan SHeur3.AQRA (AVG)
TR/Spy.Gen (Avira)
Win32.Rmnet (Dr.Web)
Trojan-Spy (Ikarus)
Mal/SillyFDC-A (Sophos)
W32.Ramnit!html (Symantec)

I'm afraid I have very bad news.

Your system is infected with a **Win32/Ramnit.A!dll (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Virus%3AWin32%2FRamnit.A!dll)** , a file infector (http://www.virusbtn.com/resources/glossary/file_infector_virus.xml) with IRCBot (http://en.wikipedia.org/wiki/IRC_bot) functionality which **infects .exe, .dll and .HTML files** and **opens a back door** that **compromises your computer**.

Ramnit.A!dll is a component injected into the default web browser by Worm:Win32/Ramnit.A (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fRamnit.A) which is dropped by a Win32/Ramnit.A (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Virus%3aWin32%2fRamnit.A) infected executable file. Ramnit.A also **infects .exe, and .HTML/HTM files**, downloads more malicious files to your system, and **opens a back door** that **compromises your computer**. The infected .HTML or .HTM files may be detected as Virus:VBS/Ramnit.A (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Virus%3aVBS%2fRamnit.A)

In many cases the infected files **cannot be disinfected** properly by your anti-virus. When disinfection is attempted, the files become corrupted and the system may become **irreparable**. The longer Ramnit.A remains on a computer, the more files will become infected and corrupt so the degree of infection can vary.

Ramnit.A is commonly spread via a flash drive (http://en.wikipedia.org/wiki/USB_flash_drive) (usb, pen, thumb, jump) **infection** which is often **contracted and spread by visiting remote**, crack (http://en.wikipedia.org/wiki/Cracker_(computing)) and keygen (http://wiki.answers.com/Q/What_is_a_keygen) sites. These type of sites are **infested with a smörgåsbord of malware** and a major source of system infection.

In my opinion, **Ramnit.A is not effectively disinfectable**, so your best option is to perform a full reformat as there is **no guarantee this infection can be completely removed**. In most instances it may have caused so much damage to your system files that it cannot be completely cleaned or repaired. In many cases the infected files *cannot be deleted* and anti-malware scanners cannot disinfect them properly. Many experts in the security community believe that once infected with this type of malware, the best course of action is to wipe the drive clean, reformat (http://wiki.answers.com/Q/What_does_it_mean_to_reformat_a_computer) and reinstall the OS. Please read:

- **When should I re-format? How should I reinstall? (http://www.dslreports.com/faq/10063)**
- **Where to draw the line? When to recommend a format and reinstall? (http://mickiemoes.blogspot.com/2008/06/malware-removal-where-to-draw-line.html)**

> *Quote*
>
> Whenever a system has been compromised by a backdoor payload, it is impossible to know if or how much the backdoor has been used to affect your system...There are only a few ways to return a compromised system to a confident security configuration. These include:
> • Reimaging the system
> • Restoring the entire system using a full system backup from before the backdoor infection
> • Reformatting and reinstalling the system

Backdoors and What They Mean to You (http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008120313315548)

This is what Jesper M. Johansson at Microsoft TechNet has to say: **Help: I Got Hacked. Now What Do I Do? (http://technet.microsoft.com/en-us/library/cc512587.aspx)** .

> *Quote*
>
> The only way to clean a compromised system is to **flatten and rebuild**. That's right. If you have a system that has been completely compromised, the only thing you can do is to flatten the system (reformat the system disk) and rebuild it from scratch (reinstall Windows and your applications).

agre

Ah, well. At least having that in the back of my mind softened the blow. Posted 27 September 2010 - 09:32 AM

A couple of follow-up questions:

--You were very descriptive about the file types that are infected by this thing. Does it also infect Office documents, text documents, PDFs and multimedia (specifically JPG/MPG/AVI)? There are a few files of this type I'd like to take with me but if there's any chance they're infected I will cut my losses.

--Assuming I have an up-to-date virus scanner, is there a known delta between time of infection and time of detection?

Thanks again.

boopme

Posted 27 September 2010 - 10:55 PM

Those files should be fine.

Not an unwise decision to make. In some instances an infection may have caused so much damage to your system that it cannot be completely cleaned or repaired. Wiping your drive, reformatting, and performing a clean install of the OS or doing a factory restore removes everything and is the safest action but I cannot make that decision for you.

Reformatting a hard disk deletes all data. If you decide to reformat, you can back up all your important documents, data files and photos. The safest practice is not to backup any autorun.ini or .exe files because they may be infected. Some types of malware may disguise itself by adding and hiding its extension to the existing extension of files so be sure you take a close look at the full name. After reformatting, as a precaution, make sure you scan these files with your anti-virus prior to copying them back to your hard drive.

The best proceedure is a low level format. This completely wipes the drive. Then reinstall the OS.
Use the free version of Active@ KillDisk (http://www.killdisk.com/downloadfree.htm) .
Or Darik's Boot And Nuke (http://www.dban.org/)

The best sources of Information on this are
Reformatting Windows XP (http://spyware-free.us/tutorials/reformat/)
Michael Stevens Tech (http://www.michaelstevenstech.com/)
Windows XP: Clean Install (http://web.mit.edu/ist/products/winxp/advanced/reinstall-format.html)

Of course also feel free to ask anything on this in the XP forum. They'd be glad to help.

==============================

2 guidelines/rules when backing up

1) Backup all your important data files, pictures, music, work etc... and save it onto an external hard-drive. These files usually include .doc, .txt, .mp3, .jpg etc...
2) Do not backup any executables files or any window files. These include .exe/.scr/.htm/.html/.xml/.zip/.rar files as they may contain traces of malware. Also, .html or .htm files that are webpages should also be avoided.

Download **Belarc Advisor** (http://www.belarc.com/free_download.html) - builds a detailed profile of your installed software and hardware, including Microsoft Hotfixes, and displays the results in your Web browser.
Run it and then print out the results, they may be handy.

We should take some precautions before we attempt to move files from the infected machine. Run the following on your clean computer, and make sure you insert your flash drives at the prompt.
Download and Run FlashDisinfector

Please download **Flash_Disinfector.exe (http://download.bleepingcomputer.com/sUBs/Flash_Disinfector.exe)** by sUBs and save it to your desktop.

- Double-click **Flash_Disinfector.exe** to run it and follow any prompts that may appear.
- The utility may ask you to insert your flash drive and/or other removable drives. Please do so and allow the utility to clean up those drives as well.
- Hold down the **Shift** key when inserting the drive until Windows detects it to keep autorun.inf from executing if it is present.
- Wait until it has finished scanning and then exit the program.
- Reboot your computer when done.

*Note: As part of its routine, Flash_Disinfector will create a hidden folder named autorun.inf in each partition and every USB drive that was plugged in when you ran it. **Do not delete this folder**...it will help protect your drives from future infection by keeping the autorun file from being installed on the root drive and running other malicious files.*

Reinstall Windows Vista (http://www.smartcomputing.com/editorial/article.asp?guid=&bJumpto=true&Isfrm=IN&article=articles/webonly/techsupport/490w10/490w10.asp&ArticleID=52007)

Note: Windows 7 Professional instructions recommend you DO NOT use a third-party software to format the drive.

quietman7

Posted 28 September 2010 - 12:40 PM

With this infection **do not** back up any .dll, .htm, .html files as well as the others boopme advised you about.

Back to Am I infected? What do I do?

BleepingComputer.com → Security → Am I infected? What do I do?

avast! Forum be free

Avast community forum

Search

HOME | HELP | SEARCH | LOGIN | REGISTER

Avast WEBforum » viruses and worms » viruses and worms (Moderators: Pavel, Maxx_original, misak) » Win32:Ramnit-B infection

« previous next »

Pages: [1] Go Down

PRINT

Author Topic: Win32:Ramnit-B infection (Read 7732 times)

0 Members and 1 Guest are viewing this topic.

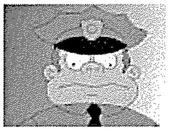
paulos333
Newbie
Posts: 9

Win32:Ramnit-B infection
« **on:** September 30, 2010, 08:19:05 PM »

I have been infected by Win32:Ramnit-B and avast is going crazy! Any ideas how to get rid of this without deleting half my harddrive? Please help!

Logged

Pondus
Avast Überevangelist
Maybe Bot



Posts: 25809

Re: Win32:Ramnit-B infection
« **Reply #1 on:** September 30, 2010, 08:21:22 PM »

http://forum.avast.com/index.php?topic=64427.0

Logged

Chief Wiggum: Uh, no, you got the wrong number. This is 9-1...2.

MC Shield TRANSLATOR

paulos333
Newbie
Posts: 9

Re: Win32:Ramnit-B infection
« **Reply #2 on:** September 30, 2010, 08:28:10 PM »

Thanks for that. It says my chest is full but i have set it to its biggest size. Should i just run malwarebytes first and leave avast going off all the time?

Logged

paulos333
Newbie
Posts: 9

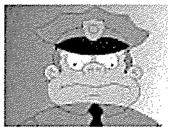
Re: Win32:Ramnit-B infection
« **Reply #3 on:** September 30, 2010, 08:32:11 PM »

it actually says there is not enough space on the disk - which i don't understand

Logged

□ **Pondus**

Avast Überevangelist
Maybe Bot



Posts: 25809

Re: Win32:Ramnit-B infection
« **Reply #4 on:** September 30, 2010, 08:40:49 PM »

Try MBAM and see what happens, remember to update before you scan

Logged

Chief Wiggum: Uh, no, you got the wrong number. This is 9-1...2.

MC Shield
TRANSLATOR

□ **essexboy**

Malware removal instructor
Avast Überevangelist
Probably Bot

Posts: 34981

Dragons by Sasha

Re: Win32:Ramnit-B infection
« **Reply #5 on:** September 30, 2010, 08:42:47 PM »

This is not a pretty virus/malware

Download **Dr.Web CureIt** to the desktop.

- Doubleclick the **drweb-cureit.exe** file, then on **Start** and allow to run the express scan
- This will scan the files currently running in memory and when something is found, click the **yes** button when it asks you if you want to cure it. This is only a short scan.
- Once the short scan has finished, chose the **Complete Scan**.
- Select all drives. A red dot shows which drives have been chosen.
- Click the green arrow ☒ at the right, and the scan will start.
- Click **'Yes to all'** if it asks if you want to cure/move the file.
- When the scan has finished, look and see if you can click the following icon next to the files found:

☒

- If so, click it and then click the next icon right below and select Move incurable as you'll see in next image:

☒

- This will move it to the **%userprofile%\DoctorWeb\quarantine-folder** if it can't be cured. (this in case if we need samples)
- After selecting, in the **Dr.Web CureIt** menu on top, click file and choose save report list
- Save the report to your desktop. The report will be called **DrWeb.csv**
- **Close Dr.Web Cureit**.
- **Reboot your computer** to allow files that were in use to be moved/deleted during reboot.
- After reboot, post the contents of the log from **Dr.Web** you saved previously in your next reply along with a new **OTL log**.

NOTE: *During the scan, a pop-up window will open asking for full version purchase. Simply close the window by clicking on **X** in upper right corner.*

Logged

□ **paulos333**

Newbie

☆

Posts: 9

Re: Win32:Ramnit-B infection
« **Reply #6 on:** October 02, 2010, 01:10:30 AM »

I have run MBAM and that seems to have helped - I haven't got any pop up avast warnings since. However I haven't run a full scan on avast again yet.

I have scanned with Dr. Web CureIt - it found a lot! I'll try and post the report but its huge...

Logged

□ **paulos333**

Newbie

Posts: 9

Re: Win32:Ramnit-B infection
« **Reply #7 on:** October 02, 2010, 01:37:39 AM »

```
=====================================================
Dr.Web Scanner for Windows v6.00.05 (6.00.05.08310)
(c) Doctor Web, Ltd., 1992-2010
Log generated on: 2010-10-01, 00:36:40 [COMPUTER][Owner]
Command line: "C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2
\14692_xp.exe" /lng /ini:setup_xp.ini /fast
Operating system: Windows XP Home Edition x86 (Build 2600), Service Pack 3
=====================================================
DwShield started
Engine version: 5.00 (5.00.2.03300)
Engine API version: 2.02
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\f3ff24dc - 1974
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\fa933f13 - 2564
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\b107db8a - 11383
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\d413d6e6 - 8957
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\9f6b9028 - 11015
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\75e6f6da - 11168
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\4b234184 - 7798
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\e7052795 - 7873
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\2f58102b - 6904
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\2b98a5ae - 6503
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\abba50d4 - 9823
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\64792b90 - 7572
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\6a83301b - 6996
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\5f976efb - 16360
virus records
[Virus database] C:\Documents and Settings\Owner\Local
Settings\Temp\2FC52A2A-7A6A48A4-77D1F932-9BC9EFE2\a111d8af - 29168
```

Microsoft

Sign in

Community

Home Categories Participate Additional Support

Announcements: 1

Windows

Applies to: Windows | Windows 7 | Email and Communications

[redacted]

Question

1 Had this question
Me Too

[redacted] asked on December 5, 2014 | 37 views

Download, Upload, - PC suddenly unable to do AND Windows Live Email Freezes

Related Content

Windows suddenly not genuine. No installation code to activate.

2 different Blue Screens within 1 hour of each other + unable to...

Blue Screen STOP error 0x0000008E

Receiving

Hi -

For no apparent reason I seem to have a problem with my home computer that runs Windows 7.
Firstly I found that on opening Windows Live Mail - it would freeze ; I cant access mail.
Usually the note is that 'Windows Live Mail' did not shut down correctly last time I used it. -
I can however go to mail.live.com and log in there OK.
I then thought I would do a basic system restore - but for some reason the last restore point I now have is only a day old ; when the problem began.
I have had the same computer/system operating fine for many years.
I wondered if a firewall was stopping something - so temporarily deleted AVG ; That didn't help at all, so I went to download it back again - but cant.
Likewise I cant download pictures to facebook for example, although I canopen Fb OK and write/post there.
I checked that I had ample space on the computer, as a reason I can no longer download things - and yes, that is fine, ample space left.

To summarize ; I cant download anything, upload anything, and windows live freezes a minute after I open it, not letting me read emails or do anything.
Apart from that, as far as Browsing/google etc all else is fine- as normal.
I can not think of any activity Ive done to alter settings, and rarely look at/download anything that may have been infected or caused the problem.

Any suggestions greatly appreciated !
[redacted]

Reply | Reply with quote | Report abuse ▾ | Subscribe to updates

[redacted]

Answer

0 Found this helpful
Me Too

[redacted] replied on December 6, 2014 ▾

In reply to [redacted] post on December 6, 2014

Hi ;
Thanks so much for taking the time to reply - much appreciated.
As I suspected, being unable to turn on the security center service plus having difficulty downloading - the problem was not with Windows live itself but a virus.
I was fortunately able to find and download free Microsoft Security Essentials which following an overnight scan detected " win32/Ramnit.A" virus that it got rid of for me - and things thankfully returned to normal.
[redacted]

Reply | Reply with quote | Report abuse ▾

All Replies (3)

[redacted] replied on December 6, 2014

Microsoft Support Engineer

0 Found this helpful
Me Too

Hi,
Thank you for posting in Microsoft Community.

I understand the inconvenience caused. I will be glad to assist you.

1. Have you made any changes to Windows Live Mail?

The issue could be due to Windows Live mail client corruptions.

I recommend you to refer to the suggestions from [redacted]replied on May 7, 2013
http://answers.microsoft.com/en-us/windowslive/forum/livemail-people/windows-live-mail-freezes-upon-clicking-of/ba60ed6a-cb6f-4436-8821-5597a83914b2

If the issue still persists, then I suggest you to put the computer in clean boot state and check if the issue persists.

How to put the computer in clean boot?
https://support.microsoft.com/kb/929135?wa=wsignin1.0

Disclaimer: After troubleshooting, ensure that you put the computer in normal mode. To do that, please follow the steps given in the Clean boot link above which says "How to reset the computer to start normally after clean boot troubleshooting."

Please do reply with the status of the issue so that we can help you further.

Reply | Reply with quote | Report abuse

[redacted]

Answer

0 Found this helpful
Me Too

[redacted] replied on December 6, 2014

In reply to [redacted] post on December 6, 2014

Hi ;
Thanks so much for taking the time to reply - much appreciated.
As I suspected, being unable to turn on the security center service plus having difficulty downloading - the problem was not with Windows live itself but a virus.
I was fortunately able to find and download free Microsoft Security Essentials which following an overnight scan detected " win32/Ramnit.A" virus that it got rid of for me - and things thankfully returned to normal.
[redacted]

Reply | Reply with quote | Report abuse

[redacted] replied on December 9, 2014

Microsoft **Support Engineer**

0 Found this helpful
Me Too

In reply to [redacted] post on December 6, 2014

Hi,

Thank you for your response. Glad to know that the issue is fixed and we appreciate your efforts in resolving the issue. I am sure that this will help other Community Members who are facing similar problems.

Please post in Microsoft Community for any help on Windows in future and we will be glad to assist you.

Reply | Reply with quote | Report abuse

English

Microsoft Community Code of Conduct Community Participation Center

Trademarks Privacy & Cookies Terms of Use

Microsoft

By using this site you agree to the use of cookies for analytics, personalized content and ads. Learn More ✕

Microsoft

Community

Sign in

Home Categories Participate Additional Support

Announcements: 1

Virus and Malware

Applies to: Virus and Malware | Other | Scanning, Detecting, and Removing Threats | Windows Vista

Question

[redacted] asked on July 18, 2014 ▾ | 159 views

1 Had this question Me Too

Unable to turn on firewall

I can not turn on my firewall and all scans state there is no virus or malware within my computer

<IE9>
Original Title: firewall blocked off

Reply | Reply with quote | Report abuse ▾ | Subscribe to updates

[redacted]

Answer

[redacted] replied on July 24, 2014 ▾

MVP ★

0 Found this helpful Me Too

In reply to [redacted] post on July 24, 2014

NEVER, *EVER* POST SUCH DANGEROUS, CLICKABLE LINKS IN A PUBLIC FORUM!

[A Moderator removed the dangerous link from your post after I posted this reply.]

You are seeing the effects of an ongoing & longstanding hijackware infection, most likely compounded by a W32/Alureon-variant rootkit infection! See...

Related Content

I am unable to update virus definitions and my firewall wont turn on I...

Unable to turn on Windows Defender or Firewall program. Error code:...

Error code 0x80070070 unable to turn on firewall

Unable to turn on defender or firewall even after running a full scan...

Unable to turn on Firewall

- Help: I Got Hacked. Now What Do I Do? {AKA Cleaning a Compromised System}
  http://technet.microsoft.com/en-us/library/cc700813.aspx

Then see the (my) ANSWER post in this thread and follow those instructions (*to-the-letter* & *in order!*) to return your computer to a secure & functional state: http://answers.microsoft.com/thread/c44429fb-3f7c-4646-8529-5a97bb3cd0eb

If you need additional assistance with the clean install, please begin *your own new thread* in this forum & ask for guidance: http://answers.microsoft.com/en-us/windows/forum/windows_vista-system

If these procedures are outside of your technical "comfort zone" - and there is no shame in admitting this isn't your cup of tea - take the computer to a local, reputable and *independent* (i.e., not a "BigBoxStore" or the Geek Squad!) computer repair shop & let them do the work.

Note: The computer should NOT be connected to the internet *or any local networks* (i.e., other computers) in its current state. All of your personal data (e.g., online banking & credit-card passwords) should be considered at-risk, if not already compromised.

Wish I'd had better news for you. Good luck!

Cite:

- Help prevent malware infection on your PC
  http://www.microsoft.com/security/portal/mmpc/shared/prevention.aspx

[redacted]
MS MVP-Windows Client (Security, Update Services, IE & Mail) since 2002

Reply | Reply with quote | Report abuse ▾

All Replies (14)

[redacted] replied on July 19, 2014 ▾
Community Moderator Wiki Author ★

0 Found this helpful
Me Too

Hi

Are you referring to the built-in Windows Firewall? If yes, this can be automatically disabled by some 3rd party security software that has its own firewall. This is by design and intended to avoid conflicts caused by having two firewalls running. Could this explain your situation?

Disclaimer: You use my posts entirely at your own risk. I do not work for or represent Microsoft.

Reply | Reply with quote | Report abuse ▾

[redacted]replied on July 19, 2014

0 Found this helpful
Me Too

In reply to [redacted] post on July 19, 2014

Good day [redacted]. Thank you for your reply. I am referring to the built in firewall and only found the firewall was switched off because I tried to do a full micro soft security scan to cure self presenting email sites coming up on my monitor and one in particular being difficult to delete. Each time it did go away it immediately returned of it's own accord. I decided to use Microsoft safety scanner on a full scan and this informed me that it had detected intruders and had managed to remove most, but not all, of them. I thought I would do a system restore to get to a time prior to these sites intruding but the system restore programme informed me it could not carry out my wishes due to some necessary data missing i.e. quote " This application has failed to startbecause ccL7OU.dll wasnot found Re installing the applicationmay fix this proble Deleting this screen label gives me another behind it which says Symatec Service Framework has stopped working A problem has stopped the programme working Windows will close the programme and notify you if a solution is available "I went to Help and support and was advised I needed to eraser my restore points and enter a new restore point and label it initial. The computer virtually finished this resetting for me but the old restore points remained on the programme. On retrying to carry out a system restore it worked and I thought 'Problem solved'. This was not to be. Again I tried another system restore and again found it could not carry out this function for the same reasons.. Reading that a system restore facility is important for the safety of my computer I again referred to Help and Support and eventually found a site where I could see my firewall was switched off and I was being advised this was a bad decision and to get it switched on . Clicking on the 'On' button produced no effect , the firewall remained off. I eventually found a site where I could contact Micro soft. I sent them an email on their form and received the below text this morning.

Thank you for contacting Microsoft Security Essentials support site.
We regret to inform you that the email support for Microsoft Security Essentials is not available anymore.
To get help on the issue you reported, you may call us on 1-800-MICROSOFT (1-800-642-7676) or contact Microsoft Community.
Please follow the steps below to seek help from Microsoft Community:
1. Go to Microsoft Community (http://answers.microsoft.com/en-us/protect/forum/mse).
2. Sign In using your Microsoft account.
3. Post your question and we will get back to you with a response.
Thanks for choosing Microsoft Support.
Please note: this email was automatically generated--replies won't be received.

This would appear to answer the question but what it does not do is give any advise re the problems I am having and how to solve them and all I can get from help and support is that in the normal run of things the firewall on is the default position. I carried out another Micro soft safety scan, the short form, and this tells me my computer is clear of any untoward intruders My health check says the computer is functioning fine All this information contradicts my actual experience which as a novice leaves me completely baffled and no idea of what to do next. Every site I get has a strip notice along the bottom telling me Internet Explorer has blocked this site because of an inappriate security ratig and to attempt to risk opening the site meets with failure. Even on this script I am trying to highlight and then changed to the same font as above which it does until the highlight goes at which time it reverts to what you see now.
Regards
[redacted]

Reply | Reply with quote | Report abuse

[redacted] replied on July 20, 2014

Community Moderator **Wiki Author**

0 Found this helpful
Me Too

In reply to [redacted] post on July 19, 2014

Hi

I am moving your thread to the Virus and Malware forum so that the people there can advise on confirming that your system is clear of malware which must be a priority.

You mentioned, "...Symatec Service Framework ...". Does this mean that you have a Norton product currently on your system? Please tell us which antimalware/security software is currently installed on your computer and which has been in the past.

Disclaimer: You use my posts entirely at your own risk. I do not work for or represent Microsoft.

Reply | Reply with quote | Report abuse

[redacted]

[redacted] replied on July 20, 2014

MVP

0 Found this helpful
Me Too

Is it the same computer (not necessarily the same problem) as in this previous thread of yours? =>
http://answers.microsoft.com/en-us/windows/forum/windows_vista-winapps/non-sleeping-desk-top-and-difficult-to-find/5cc2e1ff-f5f6-495c-ab27-346dd2caec81

[redacted]
MS MVP-Windows Client (Security, Update Services, IE & Mail) since 2002

Reply | Reply with quote | Report abuse

[redacted] replied on July 21, 2014

0 Found this helpful
Me Too

In reply to [redacted] post on July 20, 2014

The answer to both questions is contained within this submission My computer is an HP- Pavilion operating on Microsoft Windows Vista-Home Premium(x64) Model a 6541 It is set on Automatic download and install and using the info. from the Help and Support it has two firewalls. Windows, with the status being on despite the text above which I received from Microsoft and Norton Internet Security 15..5.0.23 (Symantec Corporation) with this also on. I incidentally contacted my ISP yesterday, Sunday to see if they had any reports from clients having the same problems as myself and was told by their Broadband dept. that their system was functioning normally. On further discussion I mentioned

the message ccL70U.dll I was receiving on attempting a system restore and was told this was a virus contained within Symantec and I needed to clear this Symantec from my computer. I found this confusing as this programme was present at time of purchase and had received no input from me or caused problems before. Not having the expertise to dispute this opinion I followed the advisers instructions and deleted this program from my programmes which proved involved and does not stop the computer from telling me it is still there and operative. I was eventually passed to another adviser who took me through a set of actions too numerous to recall but ended with me resetting my computer to an earlier set of settings. Initially things went well but soon returned to the previous state of computer crashes uninvited web pages and no system restore facility. I am unclear as to what else I can supply in terms of useful diagnostic information and really need questions asked to determine what more would be helpful. As a passing interest I suffered one crash on this site writing this response and having almost completed it . To avoid the same loss again I I switched to google drive where text is not lost and experienced two internet losses by my modem. This may not in anyway be connected but I'm not in a posiotion to know whether anything can be discounted

Regards

[redacted]

Reply | Reply with quote | Report abuse

[redacted]

[redacted] replied on July 21, 2014

MVP

0 Found this helpful

Me Too

In reply to [redacted] post on July 21, 2014

Answer-by-number:

1. Is it or is it not the same computer as in this previous thread of yours?

2. How long has Norton Internet Security been installed and when (exact date) does your current subscription expire?

3. Are you *certain* that Norton Internet Security v15.x (NIS 2008) is installed?

4. Has any other Norton application *or a McAfee application* ever been installed on the computer *since you bought it?*

5. Did a Norton free-trial *or a McAfee free-trial* [PICK ONE] come preinstalled the computer *when you bought it?* (Doesn't matter if you never used it.)

6. Is the computer fully-patched at Windows Update as far as you know?

COMMENTS:

- Norton Internet Security (NIS) v15.x is fairly outdated (but still supported AFAIK).
- Fact: Norton (and McAfee) applications are notorious for not uninstalling (or upgrading) cleanly. The "leftovers" may be your troublemaker here.

- NIS includes a firewall. When NIS is installed, the Windows Firewall is *disabled* by default. If you can't turn on the Norton Personal Firewall, you have a big problem. If you can't turn on the Windows Firewall (but the Norton firewall is turned on), WYSIWYG.

- Your ISP provides your internet connection. If you have questions about a Norton application, contact Norton Support. If you have questions about Windows, post them in these forums or contact the Answer Desk. [ccL70U.dll is not a "virus" nor do you need to necessarily "clear...Symantec from your computer."]

[redacted]
MS MVP-Windows Client (Security, Update Services, IE & Mail) since 2002

Reply | Reply with quote | Report abuse ▾

[redacted] replied on July 22, 2014 ▾

0 Found this helpful
Me Too

In reply to [redacted] post on July 21, 2014

Good day
1
Yes the computer is the same one that would not sleep but contacting my ISP for a different reason they informed me without prompting that my router wasn't working coirrectly and they would send me a new one . When this new router was installed the problems I had been having re. non sleeping were resolved.

2
I have not installed any security system on my computer any system would have been installed prior to purchase. I was asked ,circa weekly, to renew my subscription immediately or be reminded later. I always chose later, and circa once a week I found my computer was scanned and I was given the results of that scanning. This routine has been continuous for in excess of three years. it was done to my belief by either Norton or Mcafee or whoever they call themselves, I have never paid that much attention to it as it over time it just is accepted and ignored.

3
I wouldn't know precisely what version of anything is installed so can not answer this question

4
As said above, I have not installed anything by way of security since purchase Using Help and Support I found I had firewalls operative, I had the computer on automatic updates and their installation, I preset regular hardware system checks and de fragmentation was a preset programme also as periodic scans I carried out using Microsoft if I thought the computer was running slow and wanted to check there was no untoward cause for this, I trust this answers this question

5
I either answered this in answer four as ,all updates are automatically installed, or failing this I have not understood the question.

If as you say quote " ccL70U.dll is not a "virus" nor do you need to necessarily "clear...Symantefrom your computer."] ""end of quote and on attempting to carry out a systems restore my computer is informing me that it can not complete the task because it can not locate ccL7OU.dll then how do I reinstall said ccL7OU.dll to hopefully enable this system restore to complete as in my intention?

Note. please translate WYSIWYG as to me this has no meaning

Regards
[redacted]

Reply | Reply with quote | Report abuse ▾

[redacted]

[redacted] replied on July 22, 2014 ▾

MVP ★

| 0 | Found this helpful
Me Too |

In reply to [redacted] post on July 22, 2014

Answer-by-number in your very next reply, preferably without quoting this post:

1. A Norton Internet Security v15..5.0.23 [AKA **NIS 2008**] free-trial came preinstalled on the computer when you bought it roughly six or seven years ago and you never purchased a subscription or installed any other anti-virus application or security suite, is that correct?

2. Is it a Vista 32-bit or a 64-bit computer? See http://support.microsoft.com/kb/827218

3a. Is KB2962872, KB2971850, KB2973201, KB2961072 and/or KB2972280 listed in **Installed Updates** (*not **Update History***)? [1]

3b. How about KB2957689, KB2957503, KB2957509, KB2939576, KB2957189 and/or KB2926765?

3c. How about KB2893294, KB2892075, KB2887069 and/or KB971029?

4. *Assuming Java is installed*, is **Java Version 7 Update 65** (or higher) installed? TEST HERE USING INTERNET EXPLORER *ONLY!* => http://java.com/en/download/uninstallapplet.jsp [2]

7. Is **Adobe Flash Player v14.0.0.145** (or higher) installed? TEST HERE USING INTERNET EXPLORER *ONLY!* => http://www.adobe.com/software/flash/about/

8a. Is IE7, IE8 or IE9 installed?

8b. Is Firefox, Chrome or any other alternate browser installed?

9. Are you in the habit of using "Registry cleaners" (e.g., Registry Mechanic;*System Mechanic*; RegCure; RegClean Pro; Advanced SystemCare; Registry Booster; Glary Utilities; McAfee QuickClean; AVG PC TuneUp; Norton Registry Cleaner; PCTools Optimiser; SpeedUpMyPC; PC Doctor; TuneUp Utilities; WinMaximizer;

WinSweeper; Comodo System Cleaner; Advanced System Optimizer; CCleaner's *Registry Cleaner* component)?

WYWIWYG => http://en.wikipedia.org/wiki/WYSIWYG

==

[1] **Start | Control Panel | Programs and Features | View installed updates** (in left-hand menu)
[2] No need to install Java if it's not *already* installed!

[redacted]
MS MVP-Windows Client (Security, Update Services, IE & Mail) since 2002

Reply | Reply with quote | Report abuse ▾

[redacted] replied on July 24, 2014 ▾

0 Found this helpful
Me Too

In reply to [redacted] post on July 22, 2014

Answer to questions
1 That is correct, I have not .Computer bought new 2009
2 The computer is a Vista-64 bit
3a
The computer is set, and always has been since purchase, to automatically receive and install updates as and whern tyhey become available
3b
I see the answer to 3a applying here also
3c
Again I would see that the answer in 3a applies.
4
Using this address Ihttp://java.com/en/download/uninstallapplet.jsp
I received a Java page with the message
copied and pasted from site
Sorry! We couldn't find the document requested.
The file that you requested could not be found on this server. If you provided the URL, please check to ensure that it is correct.
7
Using http://www.adobe.com/software/flash/about/
I received the following which is a copy and paste from that screen
Sorry, this page is not available
This URL does not exist. Adobe checks periodically for any 404 errors but they do occur occasionally so we apologize for the inconvenience
8a I am unable to find any reference to these so can not provide an answer
8b.
There are no other browsers installed on the computer other than Internet Explorer its, time of purchase, browser
9
I used http://en.wikipedia.org/wiki/WYSIWYG **and after a cursory glance saw this is not the sort of programme I would go near other than out of curioity but I do not act on anything I read on any such site. unwanted software**

If my computer acts out of character I would normally carry out a systems restore to get back to a time when it was behaving normally or else I may carry out a Microsoft Safety Scan to re assure myself that all was healthy within the computer .

=======================

I have included below as Item b a copy of what the last Microsoft Safety Scan found on the computer and what is probably causing my current problem Also, immediately below, as Item
a. a site which persists on presenting itself on my screen at frequent intervals through any period of computer use, including several times during this period of use. I am not au fait with computers but would consider this suspect at least
Item a
Persistent intruder,property of Tesco's supposedly, advising me I am the potential winner of some exorbitant prize Is obviously ignored as I do not believe in Father Christmas at my age.
[link removed]

Item b Microsoft Safety Scan results pages verbatim
To view manual steps,click the name of the viruses,spyware, or potentially

Malware .	**Scan results**
Trojan:Win 32/ Ramnit.A	**Partially removed full scan**
Exploit:Java/CVE-2012=4681	**Partially removed**
Exploit:Java/CVE-2013-2465	**Partially removed**
TrojanDownloader;Win32/Filcout.A	**Partially removed**
Exploit:Java/Obfuscator.R	**Detected, n ot removed**
VirTool;JS/Obfuscator.FN	**Detected, not removed**

[redacted]

Reply | Reply with quote | Report abuse ▾

[redacted]

Answer

0 Found this helpful
Me Too

[redacted] replied on July 24, 2014 ▾

MVP ★

↪ In reply to [redacted] post on July 24, 2014

NEVER, *EVER* POST SUCH DANGEROUS, CLICKABLE LINKS IN A PUBLIC FORUM!

[*A Moderator removed the dangerous link from your post after I posted this reply.*]

You are seeing the effects of an ongoing & longstanding hijackware infection, most likely compounded by a W32/Alureon-variant rootkit infection! See...

- Help: I Got Hacked. Now What Do I Do? [AKA Cleaning a Compromised System}
  http://technet.microsoft.com/en-us/library/cc700813.aspx

Then see the (my) ANSWER post in this thread and follow those instructions (*to-the-letter* & *in order!*) to return your computer to a secure & functional state: http://answers.microsoft.com/thread/c44429fb-

3f7c-4646-8529-5a97bb3cd0eb

If you need additional assistance with the clean install, please begin *your own new thread* in this forum & ask for guidance: http://answers.microsoft.com/en-us/windows/forum/windows_vista-system

If these procedures are outside of your technical "comfort zone" - and there is no shame in admitting this isn't your cup of tea - take the computer to a local, reputable and *independent* (i.e., not a "BigBoxStore" or the Geek Squad!) computer repair shop & let them do the work.

Note: The computer should NOT be connected to the internet *or any local networks* (i.e., other computers) in its current state. All of your personal data (e.g., online banking & credit-card passwords) should be considered at-risk, if not already compromised.

Wish I'd had better news for you. Good luck!

Cite:

- Help prevent malware infection on your PC
  http://www.microsoft.com/security/portal/mmpc/shared/prevention.aspx

[redacted]
MS MVP-Windows Client (Security, Update Services, IE & Mail) since 2002

Reply | Reply with quote | Report abuse ▾

Previous Page 1 of 2 Next

English

Microsoft Community Code of Conduct Community Participation Center Microsoft

Trademarks Privacy & Cookies Terms of Use

U.S.

- All Topics
- Newsletters
- Photos
- Forums
- Resource Library
- Research

- CXO
- Software
- Startups
- Cloud
- Data Center
- Mobile
- Microsoft
- Apple
- Google

Security

Facing down the Ramnit virus on Facebook: Tips for protection and clean-up

By Bob Eisenhardt in IT Security, January 23, 2012, 4:55 AM PST

Bob Eisenhardt explains how the Facebook virus Ramnit works, why it's so bad, and how it can affect much more than a Facebook account.

Ramnit is advertised as a lethal virus for attacking Facebook, having stolen 45,000 accounts and passwords. The virus itself is actually pulled from a used parts bin of older virus infestations such as the Zeus botnet. But it can now be controlled remotely for all kinds of mayhem too. According to Amit Klein, CTO of a web security services firm, last year it was just a nasty botnet. This new version has added power by being retrofitted with financial fraud capabilities. It can capture any data in any web session. Now, this writer has been a passionate HATER of cloud based computing, so in my view, having your data or (worse) sensitive client data stored through the Internet and accessed by HTML files, provides an open door for Ramnit, a truly awful threat to anything and everything web-based.

This monster begins by attaching itself to (as they always do) Windows files such as EXE, SCR and good old DLL files (when can we rid ourselves of those?) as well as Word documents. HTML files are also in this group, and it can now discover our handy pocket friend: USB cards. Once it has this new home, an autorun script ensures infection of whatever else our key is plugged into. Now resident in a system, it buries itself into the registry (nothing new there) and uses a hidden browser instance to connect to your friendly Hacker, and run scripts to find financial stuff and send it over to an eager thief. As Dr. Leonard McCoy said in STAR TREK IV: "Oh, joy."

Ramnit leaves behind some classic symptoms of a virus. One user posted a note that his laptop was now clean (I doubt it) but he had one file named "yghaubfg.exe" and a folder "qdpnkxvp" on his system under Downloads. I am always amazed that hackers employ such obvious and fraudulent names for the files, for which we may be thankful. The latter file and directory name seem standard for Ramnit.

Cleaning up after Ramnit

Technicians love to spend hours on diagnostics and discovering how things work. While interesting, I prefer sanity to extended effort, so I endorse using a BartPE boot CD to clean your system. Better yet, maintain a GHOST image of your primary operating system drive and also have a redundant system, a secondary computer, to act as your station in case your primary fails. (A note on my preferred system configuration: my stations have two hard drives: OPSYS and STORAGE. The operating system drive contains just that and nothing else. STORAGE stores literally "everything else" inclusive of a ghost image. I highly commend this protocol).

The removal process is otherwise complex. One expert ran Avast antivirus, and a 2 hour scan revealed 4,300 infected files. Believe me that while re-installation may be the only option at this point, I commend a ghost image as discussed just above as a FAR better solution for rebuilding. This expert was also worried about .DOC and .HTML files being infected, which is another good reason for an independent backup location. Rolling back the registry to a restore point did not work either, all points having been deleted. (But Windows search still had the doggie. Go figure). Trust me, spending 30 minutes for a ghost image restore is a bargain of time utilization and keeps the stress level low.

Remedies for Facebook

All of which means that Facebook is nothing more than a really great delivery system for Ramnit to find other places to burrow into, which makes Facebook so damn dangerous. The worst of it is that people use it in their workplace. If your organization is into cloud computing, you have a really nice LEGAL exposure issue and a potential lawsuit in your future.

As for defense issues, the standard concepts of changing passwords every 30 days on Facebook is a good first, but simple step. A better step in the workplace is to lock out Facebook entirely, if it has no business use. There is an easy way to do this.

OpenDNS is a terrific web-management protocol, and has the paid program (inexpensive) has the ability to manage white and black lists. Implementing the DNS servers is simple. Once you have their DNS servers IP addresses, dig into the router or server, and replace your ISP DNS systems with their systems and *voila!* OpenDNS is your best friend. Dig into the Black list and add Facebook and whatever else you want. Users may scream, which is a good time to have them read not only this article but also anything describing the consequences of a lawsuit and unemployment benefits.

Danny Harris, security guru at Aon group, held a security seminar in 2003 that left the whole IT staff shaking their heads in shame. The bad guys are so good at what they do that our puny efforts seemed doomed to eternal failure. Case in point: virus code buried inside photographs that are impossible to see or detect. Same with the famous Facebook "two blondes" picture. Rule of thumb: someone sends you a picture: dump with freedom. The best rule is trust NOBODY and enjoy only your own photographs. On Facebook, this is a tall order indeed. Open a picture = hello Ramnit.

The root problem is that so we are Internet-web based for absolutely everything in life. Bill-paying is now the online way to live along with financial account access. Major banks have gotten better to a degree. If I try to access my accounts from another computer other than the one I have at home, the security protocols require a send and verify code to email, which is a great idea ... unless someone hijacks my email too (from Facebook) and can get the code and impersonate me (from Ramnit) which is not farfetched idea at all. It really makes me long for my old DOS 3.2 computer in some ways.

Having scared myself to pieces, I created a GHOST image of this computer. Took 10 minutes to create = same to restore if I have to. Trust me, this is a far better, less stressful method to repair a computer.