

I have focused on identifying and mitigating fraud across Microsoft's online advertising platforms. Through this role, I have gained significant knowledge and experience regarding online advertising business models and technologies, and the structure of illegal schemes to defraud Microsoft and others with regards to online advertising. Before joining Microsoft, I worked for Excell Data Corporation as a Program Manager performing security firewall deployment, configuration, and administration. I am a graduate of the United States Military Academy, West Point, and served for 27 years as a United States Army Communications Electronics Officer (11 years active, 16 reserve), attaining the rank of Lieutenant Colonel.

I. INTRODUCTION TO ZEROACCESS

3. As part of my role at Microsoft, I have investigated the malicious software ("malware") known as the "ZeroAccess" malware. ZeroAccess—also known as the "Sirefef" or "max++" malware—is computer malware that surreptitiously infects users' computers and, without the user's knowledge, assimilates their computers into a network of computers known as a "botnet." Through my investigation, I have recently found that, on any given day, as many as 800,000 ZeroAccess-infected computers are active in the botnet. Other security researchers have estimated that in August, 2013, there were approximately 1.9 million infected computers worldwide. *See, e.g., Pearce et al., "The ZeroAccess Auto-Clicking and Search Hijacking Click Fraud Modules (Draft),"* (hereinafter "*Pearce et al.*") attached hereto as **Exhibit 1**, p. 1. My investigation leads me to believe that over time, over two million computers have been infected worldwide. Most infected computers are located within the United States and Western Europe. The location can be determined by "geolocating" IP addresses of detected infected computers. On October 23, 2013, we detected more than 19,000 infected computers in Texas. The concentration of Internet connections from infected computers for a two week period in October 2013 is shown in the "heat maps" in **Figures 1 and 2** below:

Fig. 1
Texas Heat Map

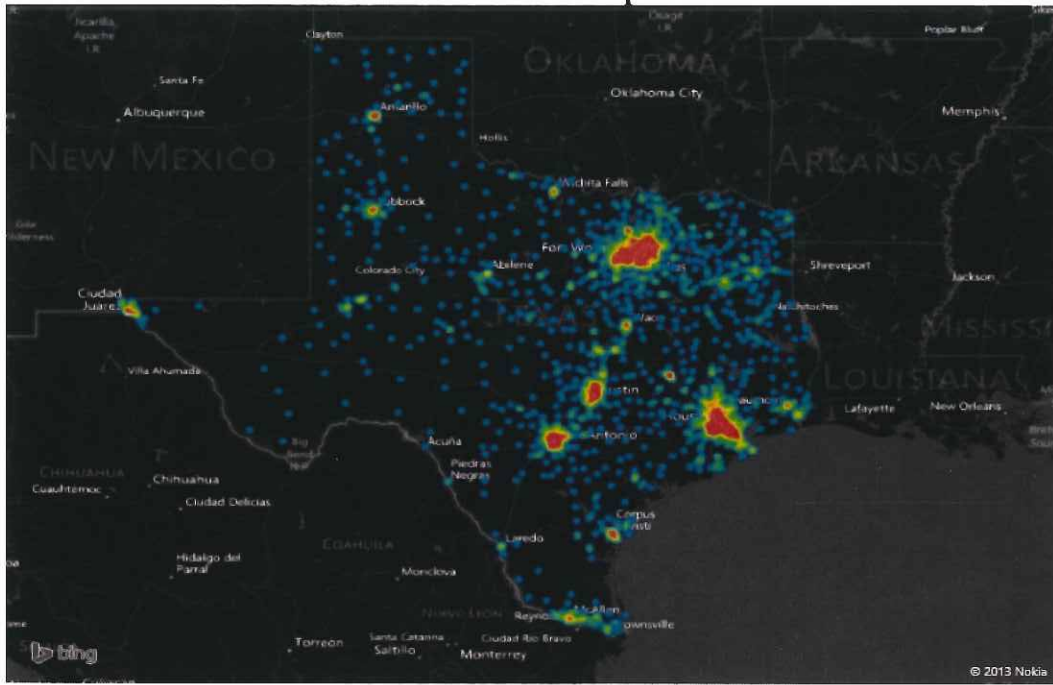
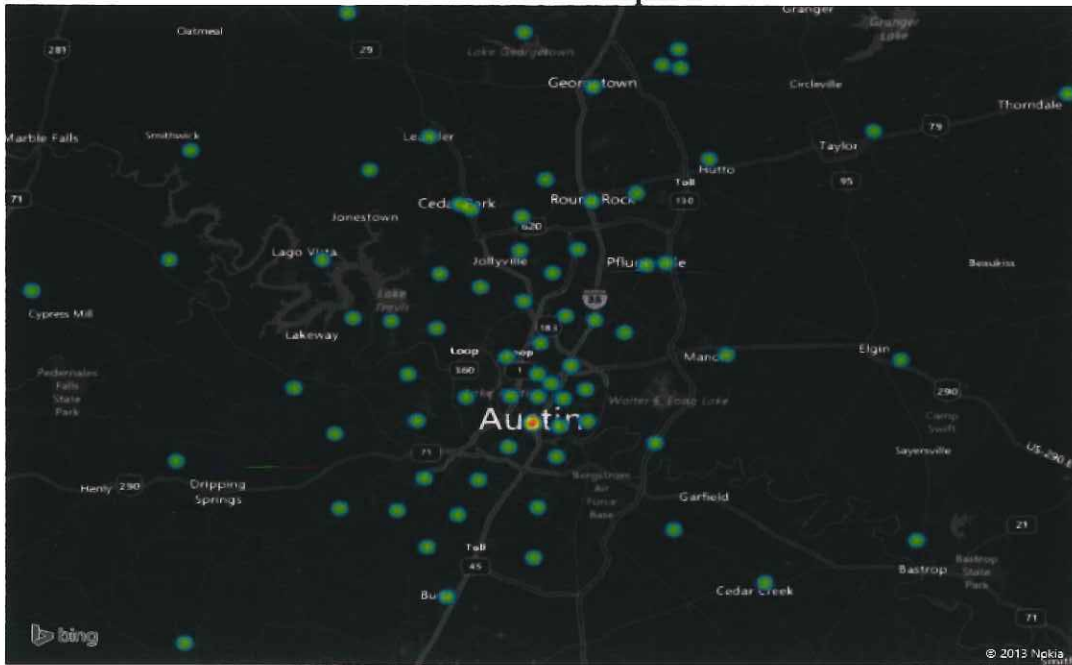


Fig. 2
Austin Heat Map



4. ZeroAccess directly harms the owners of the infected computers and places them at risk of further malware infections. Computers infected with ZeroAccess may be PCs or laptop computers located in private homes, public libraries, hospitals, schools, business, or anywhere else computers are connected to the Internet. ZeroAccess corrupts the operating systems on those computers and disables their security defenses.

5. Microsoft's investigation has shown that cybercriminals operating the ZeroAccess botnet use the infected computers to engage in various forms of illegal activity relating to online advertising fraud, including "browser hijacking." and "click-fraud."¹ Through browser hijacking, the cybercriminals operating ZeroAccess can connect the infected computers to unsafe websites at will. By having this degree of control over infected computers, and by being able to connect the computers to various websites, the ZeroAccess cybercriminals are able to sell traffic that ends up being leveraged by other groups of cybercriminals and online fraudsters. Security researchers have estimated that ZeroAccess costs online advertisers over \$2.7 million per month. See Pearce *et al*, Ex. 1, p. 2.

6. In addition, computers infected with ZeroAccess may be connected to websites that attempt to install an exceedingly dangerous type of malware known as "Zeus" on the computer. Zeus is a family of financial fraud botnet malware that spies on the owner of the computer and steals their financial account information, including account numbers, account balances, and passwords for online banking. The criminals behind Zeus then use this information to surreptitiously empty the victim's bank account. In December, 2012, Microsoft and other plaintiffs from the financial industry won a default judgment against the operators of Zeus in the matter *Microsoft et al. v. John Does 1-39*, Civil Action No. 1:12-cv-01335-SJ-RLM (E.D. N.Y.), taking down significant portions of that botnet. In spite of these concerted efforts

¹ ZeroAccess also includes a module for "bitcoin mining." Bitcoin is an unregulated electronic cryptographic currency used frequently by cybercriminals. Bitcoin mining involves computing extremely large equations in order to "find" new bitcoins. Defendants harness the combined processing power of the multitude of computers that comprise the ZeroAccess botnet in order to supplement the income derived from click fraud and browser hijacking.

and successes, branches and/or versions of the Zeus botnet live on, and the operators of Zeus are evidently using ZeroAccess-generated traffic to infect more computers and rebuild their criminal operation.

7. In addition to the direct harm caused to computer users, ZeroAccess also directly damages companies that place legitimate advertising on the Internet. ZeroAccess-infected computers generate fraudulent “clicks” on online advertisements, defrauding those companies because they pay for each click. ZeroAccess generates a veritable deluge of fraudulently generated clicks on the online advertising system.

8. ZeroAccess also directly damages Microsoft because it burdens Microsoft’s online advertising platform, defrauds its customers, and exploits Microsoft’s famous trademarks in various ways to deceive users whose computers are infected and who are being led through the maze of websites related to the ZeroAccess fraud.

9. While the location of the ZeroAccess cybercriminals is unknown, other security researchers have found evidence suggesting they are in Russia. *See, e.g.*, Infosec, “ZeroAccess Malware Part 4: Tracing the Crimeware Origins by Reversing Injected Code,” attached hereto at **Exhibit 2** (reporting links between ZeroAccess infrastructure and the Russian Business Network, “a well known cybercrime ring”); F-Secure, “ZeroAccess, The Most Profitable Malware In The Wild,” attached hereto as **Exhibit 3** (reporting that ZeroAccess gang advertises for distributors in Russian underground forums); English translations of Russian posts advertising ZeroAccess, attached hereto as **Exhibit 4**. In this declaration, I explain online advertising and fraud, how ZeroAccess works, how it causes harm, and how it can be disrupted.

II. ONLINE ADVERTISING AND FRAUD

A. Online Advertising Platforms Are Lucrative Targets For Fraud

10. Online advertising is a multibillion dollar industry. Recent reports by PwC estimated that Internet advertising revenue totaled \$20.1 billion for the first six months of 2013, with revenues for the first six months of 2013 increasing 18% over the first six months of 2012.

See “IAB internet advertising revenue report,” attached hereto as **Exhibit 5**. In short, since the inception of online advertising in the mid-1990s, it has become a major business activity, involving almost every sector of our economy and affecting anyone who browses the Internet.

11. The online advertising ecosystem is a lucrative target for fraud due to its rapid growth, size, and complexity. Cybercriminals have devised multiple schemes to manipulate the online advertising business model, siphoning off millions of dollars annually. For example, cybercriminals have devised multiple techniques to generate fake “clicks” on or views of advertisements, events that quite often generate revenue for the website hosting the advertisement that was clicked on or viewed. I explain these schemes in more detail below.

12. Most major online advertising platforms try to filter out fraudulently-generated traffic based on its underlying characteristics. To evade these mechanisms, fraudsters need to generate clicks on advertisements in very low volumes from a large number of geographically dispersed computers. The only way this can be done economically is by gaining control over end-user computers owned by innocent persons and businesses. The cybercriminals do this by infecting the computers with malicious software, commonly referred to as “malware.” Thus, in the black-market economy of cybercrime, the money that can be stolen through online advertising fraud has become both a major source of funds and a major impetus for schemes to develop new ways to infect and control end-user computers.

1. Microsoft Provides One Of The Predominant Online Advertising Platforms On The Internet

13. Microsoft owns and operates the Bing[®] search engine and an online advertising platform called Microsoft Bing[®] Ads (formerly known as adCenter). As part of its Bing Ads business, Microsoft contracts with various companies who wish to place advertisements on the Internet (“Advertisers”). Through the Bing Ads platform, Advertisers manage various aspects of their online advertising campaigns including budgeting, ad-placement, and analysis of results. Microsoft places the Advertisers’ advertisements on, among other places, a network of websites published by other entities or individuals (“Publishers”) that also participate in Microsoft’s

advertising network program. Various large companies such as Google, Yahoo! and others also provide large-scale advertising platforms similar to Bing Ads. I will refer to these generically as “Advertising Platforms.”

14. An individual viewing a Publisher’s website can click on an advertisement of interest. This action connects the individual to the Advertiser’s website where additional information about the product or service being advertised will be displayed. The goal of the Advertiser at this point is to encourage the individual to take additional actions such as requesting more information about or purchasing the Advertiser’s products or services. These additional actions taken on an Advertiser’s website are referred to as “conversions,” and may be tracked and monitored by Advertisers.

2. Advertisers Are Charged On A “Per Click” Or “Per View” Basis

15. After a consumer clicks on an advertisement, the Advertising Platform debits the account of the Advertiser that paid to place the advertisement, and credits the account of the Publisher of the website where the click occurred. In one common approach known as “pay-per-click” (“PPC”), Advertisers pay for each click on their advertisement, although on many well-monitored Advertising Platforms, the Advertising Platform itself maintains filters meant to identify fraudulently-generated clicks based on various technical information associated with the clicks, and advertisers are generally not charged for clicks of dubious quality or origin. Another common approach is known as “pay-per-view.” In a pay-per-view system, the Advertiser pays each time an individual user views the advertisement. In a pay-per-view system, “views” are typically bought and sold in units of 1000 views on a cost per “mille” (“CPM”) basis.

Advertising Platforms deploy sophisticated networks of computers to distribute advertisements, monitor clicks and views, and manage accounts.

16. Pay-per-click and pay-per-view systems allow Publishers to profit from the time, effort, and money invested in developing interesting and useful websites without requiring them to directly charge users for access to their websites. It benefits Advertisers by allowing them to

place advertisements on websites likely to attract individuals interested in their products or services, and, in the case of pay-per-click, by connecting them with the individuals who have, by clicking on an advertisement, shown an interest in their products or services.

3. **Tactics Have Evolved To Defraud Pay-Per-Click And Pay-Per-View Advertising Systems**

17. Pay-per-click and pay-per-view systems are subject to fraud. An unscrupulous Publisher could, for example, use automated scripts, end-user computers infected with malware, or hired-individuals to generate a large number of clicks on and/or views of the advertisements placed on its website by advertising platforms such as Microsoft's Bing Ads. Because such methods imitate the actions of a legitimate user of a web browser clicking on an advertisement, but do so for the sole purpose of generating a charge per click with no underlying interest in the product or service being advertised, the clicks are considered fraudulent. This activity is termed "click-fraud." A Publisher or others engaged in click-fraud can reap ill-gotten profits because, for each click recorded, the Publisher's account is credited at the expense of the Advertiser whose advertisement was clicked.

18. For example, in one simple click-fraud scheme, a Publisher hires individuals to simply visit the Publisher's website and repeatedly click on the advertisements placed there. In the absence of fraud-detection measures, each time such a hired-individual clicks on an advertisement on the Publisher's site, the account of the Advertiser whose advertisement is clicked can potentially be debited, and the account of the Publisher of the website where the click occurred is credited. Such a click should be deemed fraudulent because the person behind the click has no legitimate interest in the products or services advertised and is clicking on the advertisement for the sole purpose of defrauding the Advertiser.

19. In other more sophisticated schemes, Publishers can generate a large number of invalid clicks by channeling innocent end-users browsing online to websites the Publisher controls and tricking them into clicking on online advertisements. A variety of techniques can be used to channel users to a particular website. For example, a Publisher can purchase Internet

traffic from individuals or entities that have installed malware on end-users' computers connected to the Internet. The malware can then be used to route the end-users to websites controlled by the paying Publisher. Once on the website controlled by the Publisher, the end-user can be tricked into clicking on advertisements. For example, links to advertisements can be hidden beneath links to legitimate-looking topics. By clicking on the legitimate-looking link, the end-user causes a click on the invisible advertisement to be recorded. Of course, in a pay-per-view system, forcing a click is not necessary; it is sufficient that the user view the advertisement.

20. In other instances, such as the case at hand, end-user computers can be infected with malicious software ("malware") and recruited into networks of infected computers known as "botnets" that can be remotely controlled for illegal purposes. Such botnets can be used to generate clicks on advertisements on websites without the knowledge or participation of the end-user. Botnets that are specialized for this purpose are referred to as "click-bots." Typically, infected computers will be programmed to visit a set of websites selected by the cybercriminals controlling them, and simulate clicks on advertisements placed on those websites.

B. "Traffic" Fuels The Online Advertising Ecosystem

1. Traffic Is Bought And Sold On The Internet With Little Accountability

21. The flow of visitors to a website is referred to as "traffic." When a user's browser connects that user's computer to a website, the connection counts as a "visit." Traffic is the most valuable commodity in the online advertising world. Traffic is bought and sold on the Internet with little accountability, allowing schemes to generate fraudulent traffic to flourish. It is not uncommon for a Publisher to pay other entities or individuals to find users and channel them to its website. Quite often this is done as a way of boosting the statistical ranking of the website, which is based in part simply on the number of visits to it; as a website goes up in the rankings, its publisher often will be able to charge advertisers more to place advertisements on it. Quite often it is done in hopes of driving up ad revenues by generating clicks on, or views of, advertisements on the website. Attached hereto at **Exhibit 6** is a true and correct copy of a

November 12, 2013 article describing an interview with a former publishing executive who admitted that he had knowingly purchased fraudulent traffic and resold it on to advertisers in the past year. This former executive is quoted as stating the following:

Q: How and why were you buying non-human traffic?

A: We were spending anywhere from \$10,000 to \$35,000 a day on traffic. My conversations with [these ad networks] were similar: They would let me decide how much I was willing to pay for traffic, and when I told them \$0.002 or below, they made it clear they had little control over the quality of traffic they would send at that price. Quality didn't really matter to us, though. As a website running an arbitrage model, all that mattered was profit, and for every \$0.002 visit we were buying, we were making between \$0.0025 and \$0.004 selling display ads through networks and exchanges. The biggest determinate of which traffic partner we were spending the most money with was pageviews per visit. Since we were paying a fixed cost per visit, more pageviews equaled more ad impressions. Almost none of these companies were based in the U.S. While our contacts were in the US and had American names and accents, most of the time we found ourselves sending payment to a non-US bank.

Q: How did you know the traffic was bots?

A: These vendors offer a range of services and traffic types – everything from \$2.00 CPC² traffic sourced from Google, Yahoo, and Bing, to \$0.002 CPC from god knows where. When we told them we were looking for the cheapest traffic we could possibly buy there would be sort of a wink and a nod, and they'd make us aware that for that price the traffic would be of "unknown quality". How much you pay determines how much bot traffic you're getting, so when you're paying \$0.002 a click, you're getting mostly bots. You can tell it's bot traffic just by looking at the analytics. We'd see a traffic spike in our real-time analytics dashboard and then we would see all of our traffic for the day serve in a couple of hours, Or it would all come from users using the same really old version of Internet Explorer. Almost all our users had Flash versions from 2003, according to Google Analytics. That just doesn't happen with real users.

22. These statements are consistent with what I have learned about the online advertising industry through my own investigation and research. The entities or individuals selling the traffic can use all of the fraudulent means already described to generate it. The Publisher that purchases fraudulently-generated traffic, regardless of whether he or she knows of

² "CPC" stands for "cost per click." This is the amount that the advertiser will pay for each "click" on an advertisement.

the fraudulent origin of the traffic, can ultimately profit from it. At the end of the line is an Advertiser who is charged for the invalid clicks that are generated through these schemes.

23. As part of my investigation, I reviewed information from online forums in which traffic is bought and sold as a way of determining the prevalence of such schemes. I found that there is a robust market for very inexpensive traffic of questionable origins with many participants and few, if any, real controls over whether or not the traffic bought or sold is generated fraudulently. **Exhibits 7-10** of this declaration show examples of offers to sell traffic taken from a traffic bartering website called "Digital Point." While it is not possible to fully assess the nature of the traffic offered without purchasing it and doing a deeper analysis, I have attempted to draw some reasonable conclusions about the traffic based on what is being offered.

24. In the first example traffic offer, shown in **Figure 3** below, the price per visitor ranges from \$0.002 to \$0.00002 per visitor depending, presumably, on the source of the visitor. A true can correct copy of this advertisement is attached hereto as **Exhibit 7**.

Figure 3

Jul 8th 2011, 6:52 pm

AdSenseSafe
Hand of AdSense

» » [TARGETED] Visitors • AdSense Safe • Increase Clicks & Revenue • Control Panel ◀ ◀

» » **Special Promotion of DigitalPoint Forum Members** ◀ ◀

- InnoShow is Proud to Offer [Advertising](#) to Members of DigitalPoint Forum.
- **We Are Offering a 20% Extra Bonus ONLY to DigitalPoint Members.**
- Please Make a Reply to This Thread With Your UserName After You Purchase to:
- Verify That You're a Member of DP & Receive 20% Extra Credit For Your 1st Transaction.

» **INNOSHOW ADVERTISING NETWORK** ◀

- [Try InnoShow Advertising Services Now!](#)
- [Sign Up Takes Less Than 10 Seconds!](#)
- <http://www.innoshow.com>

» **What Makes Us Different** ◀

Our traffic is highly targeted based on the keywords, description, and site you give us.
The targeted visitors we deliver will be interested and browse/click on your website contents.
We offer various types of visitors and have an advanced control panel.
You may also specify for geo county specific visitors to be offered to you.
Our visitors originate from a very large network of different unique sites we operate.

» **How Much Does It Cost** ◀

- Prices start at \$0.002 per visitor for higher tier view visitors.
- For lower tier bulk visitors prices start at \$0.00002 per visitor.
- We have no minimum purchase amount, so you are free to test us out before making a big purchase.

» **Types of Visitors Offered:** ◀

- View Visitors - General view of your site, somewhat targeted
- Unique Visitors - Interested in your site's content, may have potential to click content, targeted.
- Focused Visitors - Very interested in your site's content, very targeted, best for site revenue increase.
- Search Engine Visitors - Increase your site's search engine rank for specific keyword, also increases your visitors & site revenue.
- User Action Visitors - Need guaranteed signups for your website? Or some other action for your visitor to do?
- Bulk Hits Visitors - Great for increasing site ranking and increase traffic flow to website.

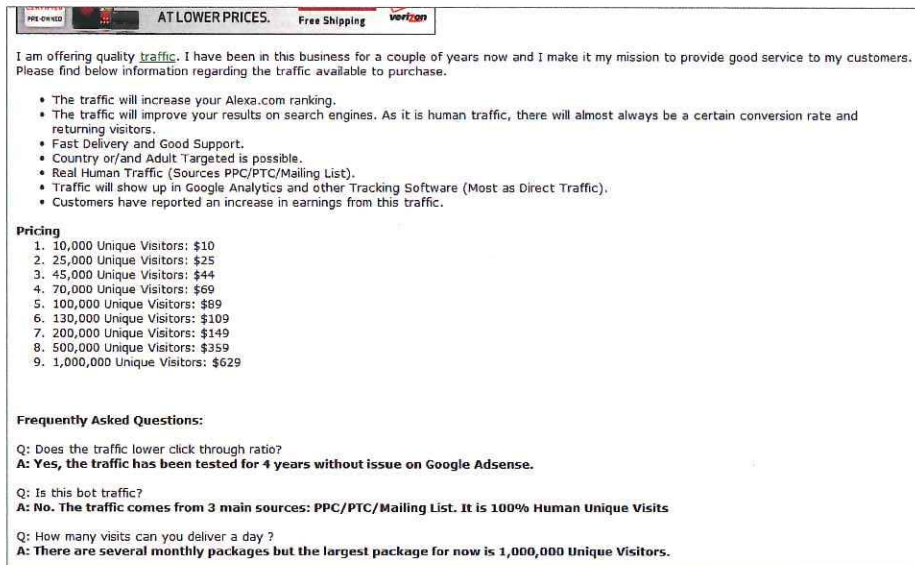
» **Variety of Features for Your Campaign/Visitors:** ◀

- Controllable Via Control Panel - Stop and start your visitor campaigns at will for any URL.
- GEO Country Specific Available - Select from different countries around the world to receive your visitors from.
- Internal Random URL Service - Have Your ordered visitors delivered to unlimited amount of random URLs with a campaign.
- Visitors Per Hour / Day - Specify the amount of visitors you want to receive for the day or every hour.
- Randomize Traffic - Make your traffic / visitors come more naturally and vary throughout the day or every hour.
- Multiple URL Campaign - add as many URLs as you need to a single campaign, visitors will be distributed between them.
- Advanced Cloaking System Available - Cloak to make your traffic untraceable through our Advanced 4 Stage Cloak System.

25. One of the noteworthy aspects of this offer in **Figure 3** is that the traffic vendor offers its customers a “control panel,” through which the traffic purchasers can control the attributes and rate of traffic to a particular website. For example, through the control panel, the purchaser can start, stop, schedule, or randomize the timing of the flow of visitors to a particular website; distribute the purchased traffic to any number of websites controlled by the purchaser, or employ an “Advanced Cloaking System,” meant to “make your traffic untraceable through our Advanced 4 Stage Cloak System.” This is presumably intended to foil traffic quality investigators employed by the major Advertising Platforms. In my experience, these sorts of obfuscation techniques are usually taken by website publishers in hopes of avoiding detection by the fraud detection systems employed by the major Advertising Platforms. This emphasis on making the traffic look more natural (e.g., spread out over the day or at random times) and to conceal the source of the traffic strongly suggests the fraudulent origins of the traffic.

26. In the next example offer, excerpted in **Figure 4**, below, the traffic vendor brags that his traffic will “increase [the] Alexa.com ranking” of the purchaser’s website, which, as I explained above, is one way that the purchaser can increase the price he or she charges to place advertising on his or their website. Note that the seller assures prospective buyers that the traffic is not “bot traffic,” but is “100% Human Unique Visits.” As will be explained further below, the fact that a human is sitting at the computer is no guarantee that the browser on the computer has not been hijacked by the botnet code running on the victim’s computer. A true and correct copy of this offer is attached hereto as **Exhibit 8**.

Figure 4



AT LOWER PRICES. Free Shipping Verizon

I am offering quality traffic. I have been in this business for a couple of years now and I make it my mission to provide good service to my customers. Please find below information regarding the traffic available to purchase.

- The traffic will increase your Alexa.com ranking.
- The traffic will improve your results on search engines. As it is human traffic, there will almost always be a certain conversion rate and returning visitors.
- Fast Delivery and Good Support.
- Country or/and Adult Targeted is possible.
- Real Human Traffic (Sources PPC/PTC/Mailing List).
- Traffic will show up in Google Analytics and other Tracking Software (Most as Direct Traffic).
- Customers have reported an increase in earnings from this traffic.

Pricing

1. 10,000 Unique Visitors: \$10
2. 25,000 Unique Visitors: \$25
3. 45,000 Unique Visitors: \$44
4. 70,000 Unique Visitors: \$59
5. 100,000 Unique Visitors: \$69
6. 130,000 Unique Visitors: \$109
7. 200,000 Unique Visitors: \$149
8. 500,000 Unique Visitors: \$359
9. 1,000,000 Unique Visitors: \$629

Frequently Asked Questions:

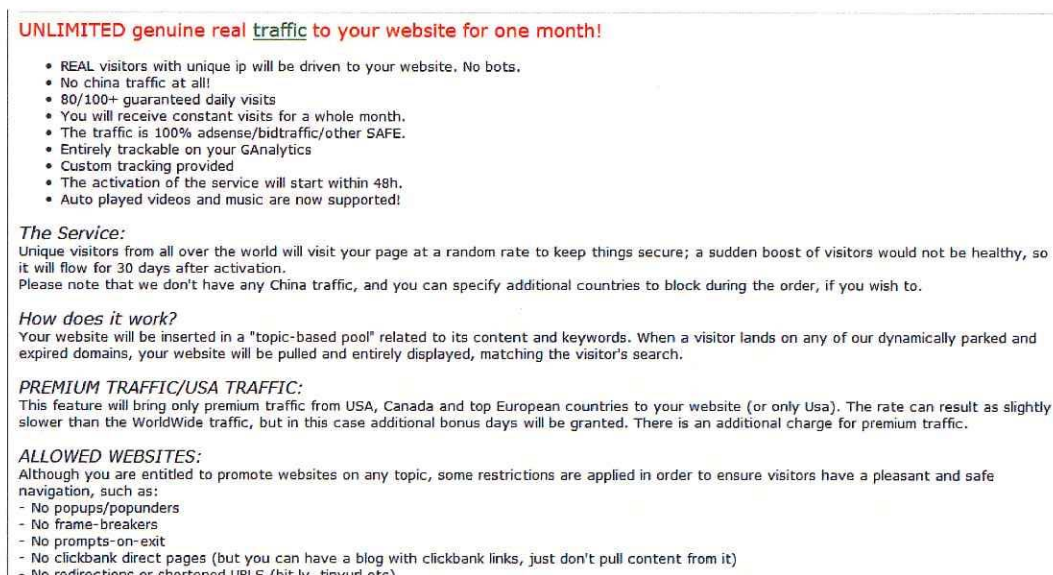
Q: Does the traffic lower click through ratio?
A: **Yes, the traffic has been tested for 4 years without issue on Google AdSense.**

Q: Is this bot traffic?
A: **No. The traffic comes from 3 main sources: PPC/PTC/Mailing List. It is 100% Human Unique Visits**

Q: How many visits can you deliver a day ?
A: **There are several monthly packages but the largest package for now is 1,000,000 Unique Visitors.**

27. In the next example, shown in **Figure 5**, below, the traffic vendor again brags that the traffic is made up of “REAL visitors with unique ip . . . No bots.” The vendor further brags that the traffic is safe for use with “adsense/bidtraffic/other,” by which the vendor hopes to imply that the traffic will not be detected as fraudulently generated by major online advertising platforms. A true and correct copy of this offer is attached hereto as **Exhibit 9**.

Figure 5



UNLIMITED genuine real traffic to your website for one month!

- REAL visitors with unique ip will be driven to your website. No bots.
- No china traffic at all!
- 80/100+ guaranteed daily visits
- You will receive constant visits for a whole month.
- The traffic is 100% adsense/bidtraffic/other SAFE.
- Entirely trackable on your GAnalytics
- Custom tracking provided
- The activation of the service will start within 48h.
- Auto played videos and music are now supported!

The Service:
Unique visitors from all over the world will visit your page at a random rate to keep things secure; a sudden boost of visitors would not be healthy, so it will flow for 30 days after activation.
Please note that we don't have any China traffic, and you can specify additional countries to block during the order, if you wish to.

How does it work?
Your website will be inserted in a "topic-based pool" related to its content and keywords. When a visitor lands on any of our dynamically parked and expired domains, your website will be pulled and entirely displayed, matching the visitor's search.

PREMIUM TRAFFIC/USA TRAFFIC:
This feature will bring only premium traffic from USA, Canada and top European countries to your website (or only Usa). The rate can result as slightly slower than the WorldWide traffic, but in this case additional bonus days will be granted. There is an additional charge for premium traffic.

ALLOWED WEBSITES:
Although you are entitled to promote websites on any topic, some restrictions are applied in order to ensure visitors have a pleasant and safe navigation, such as:
- No popups/popunders
- No frame-breakers
- No prompts-on-exit
- No clickbank direct pages (but you can have a blog with clickbank links, just don't pull content from it)
- No redirections or shortened URLs (bit.ly, tinurl,etc)

28. One of the noteworthy aspects of the offer in **Figure 5** is the explanation of how the traffic is generated: “When a visitor lands on any of our dynamically parked and expired domains, your website will be pulled and entirely displayed, matching the visitor’s search.” In other words, this traffic vendor has collected a portfolio of Internet domains for which the previous registration had lapsed. The vendor waits for any visitor to those expired domains and then redirects them to the traffic purchaser. The visitors may be people actually trying to connect to the expired domain, not realizing it is no longer an active website, or the visitors may be people whose computers are infected with malware, like ZeroAccess, which connects them to the expired domains, and then on to the traffic purchaser, as a way of obfuscating the traffic’s origin.

29. A second noteworthy aspect of the offer in **Figure 5** is the statement that “Unique visitors from all over the world will visit your page at random rate to keep thing secure; a sudden boost of visitors would not be healthy, so it will flow for 30 days after activation.” In my experience, sudden surges in traffic to a particular website may alert an advertising platform that the traffic may be fraudulent, a fact of which this vendor is obviously aware.

30. In the following example, shown in **Figure 6**, below, the vendor offers traffic from China, but at a slow rate of 1000 unique visitors per day, evidently so as not to trigger any investigation by the advertising platforms: “We are providing estimated 1000 [unique visitors] daily and not all of sudden with increasing traffic up to a few hundred thousand hoping to stay low-profile.” A true and correct copy of this offer is attached hereto as **Exhibit 10**.

Figure 6

Traffic from us :D

Hi everyone, if you are looking for some unique visitor to your site, perhaps this would be one of the best deals you can find here 😊
I am providing such traffic randomly (with my friend's help from his own website in china). So majority, you will be getting partial traffic from china (due to the various location in China)
Shall anyone interested, just place your domain name here... perhaps you guys will be getting roughly 1000 unique visitors daily but there isn't any guarantee about it yet (since this is a free service from us here 😊)

Your Ad Here
Cheap SEO Services
AllSEOSTar - Cheap SEO Services : Organic/Targeted Traffic, DoFollow Backlinks, Social Likes/Followers, etc.

Yes, this is free service at the moment to get some feedback from all of you here. Shall you are happy with the traffic, perhaps you can advise us on the next pricing plan that you are good or willing to so called "purchase" the traffic too...
Previously we have tested with few of sample sites containing ads from adsense, adbnite, exitjunctio... etc and no issue / warning for such activity and the ads still loading though 😊 (*well, my friend owns some cyber cafe network in China and with some appropriate proxy within his boxes, traffic is seen generating as per expected)

We are providing estimated 1000 uv daily and not all of sudden with increasing traffic up to few hundred thousand hoping to stay low-profile. If you need such amount of traffic daily, this would be good for you but for the current heavily visited site, i guess 1000 uv daily should not within your interest.

Just leave your domain here and watch with googleanalytic or statcounter. Leave us some feedback if the traffic is genuine and reaching your site .
thankyou

p.s. i will be commenting here once we are ready for the traffic setup (the list will be swap every few hours or daily to cope with existings list of domains available at the moment)on the selected domains

2. Individual Computer Owners Are Directly Harmed By Fraud Related To Online Advertising

31. The schemes behind this sort of traffic harm individual users as well. As detailed further below, paragraphs 55-67, their computers may be enlisted in illegal schemes, their browser searches may be hijacked, and the performance of their computers may be degraded. Further, once a user's computer is infected with malware that gives a cybercriminal control over the computer for one purpose, such as online advertising fraud, the computer becomes an asset that the cybercriminal can sell or rent to other cybercriminals for additional illegal activities, many aimed directly at spying on or stealing from the unsuspecting owner of the infected computer. Thus, online advertising fraud and the money that it pumps into cybercriminal operations have a far wider impact than the advertising industry itself, and it places at risk all those who use the Internet.

III. THE ZEROACCESS BOTNET

A. Microsoft Has Conducted An Extensive Investigation Into ZeroAccess

32. Since 2010, I and other investigators at Microsoft and elsewhere have been investigating various methods that cybercriminals use to defraud the online advertising systems

offered by Microsoft and other companies, such as Yahoo! and Google. Our investigation has focused most recently on the ZeroAccess malware that infects computers of innocent Windows operating system users around the world, and enlists those computers in illegal activity that defrauds online advertising systems.

33. As part of its investigation into ZeroAccess, the Microsoft investigative team that I work with purposefully infected a number of investigator-controlled computers with different variants of the ZeroAccess malware. We then monitored and analyzed the illegal activities engaged in by those computers under the direction of the cybercriminals operating the ZeroAccess botnet. We observed these infected computers communicate with other infected computers connected to the Internet from locations around the world. We observed the infected computers connect to and receive instructions from command and control servers located in various European countries. We carefully analyzed the changes that ZeroAccess malware makes to Microsoft operating system and application software during the infection process and have reverse-engineered the malware to determine how it works. We have analyzed click-traffic on Microsoft's ad-network and have studied evidence directly linking certain clicks on advertisements back to computers infected with the ZeroAccess malware. I have also reviewed literature published by other well-regarded computer security investigators concerning ZeroAccess, and their findings have confirmed my own conclusions regarding this botnet. Through these and related investigative steps, I have developed detailed information about the size, scope, and illegal activities of the ZeroAccess botnet. Based on my investigation, it is my view that the cybercriminals behind ZeroAccess are operating as one or more groups, developing the malware, deploying various tactics to spread the malware to literally millions of computers around the Internet, managing the infected computers for profit, and generally monitoring and defending their network of infected computers.

B. ZeroAccess Is One Of The Largest And Hardest-To-Eradicate Botnets Operating On The Internet Today

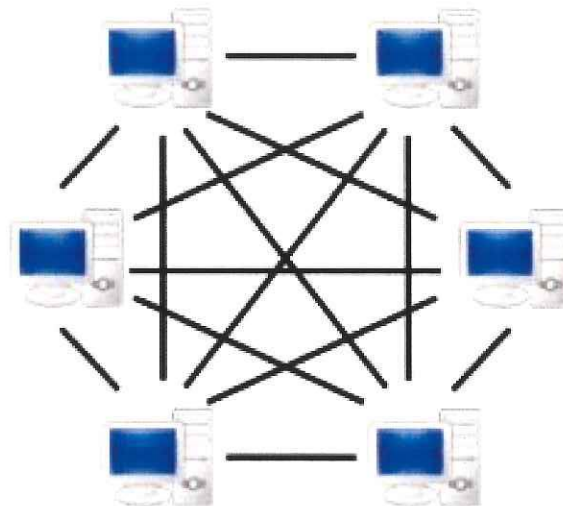
34. ZeroAccess is one of the largest botnets I have studied, recently estimated to comprise approximately 1.9 million infected computers. Botnets are computer networks consisting of tens of thousands, and sometimes even millions, of compromised personal computers infected with malicious software (“malware”) that transforms the computers into tools for criminal activity ranging from stealing personal information to defrauding businesses. For further information, *see, e.g., Pearce et al., Exhibit 1*, p. 1. Botnets harm nearly all users of the Internet, afflicting end users, corporations, and governments alike.

35. Botnets can generally take on one of several structures that allow a single criminal or small gang of criminals to command and control the vast array of compromised computers (known as “bots”). Some botnet networks are very hierarchical in nature, with a small number of “command-and-control” servers connected to the Internet, with which all of the infected computers must communicate regularly to function. Such botnets can be effectively disrupted through measures taken against the command and control servers, which often can be readily identified.

36. ZeroAccess, however, uses what is known as a “peer-to-peer” network topology. In a peer-to-peer network, the participating infected computers, called “nodes,” or “peers,” engage in constant communication with each other, and can quickly and reliably update each other with new versions of the malware and new instructions. In other words, in a peer-to-peer network, any one of the infected computers can function as a command-and-control server. Consequently, there is no single point of command and control that provides an easy target for those seeking to disrupt the network. Because a peer-to-peer botnet is the most difficult type of botnet topology to disrupt, peer-to-peer topologies are especially attractive to cybercriminals designing and propagating botnets. Peer-to-peer topologies are also advantageous for cybercriminals because their architecture allows for more robust communications between the compromised computers, making the botnet as a whole more resilient against efforts to disrupt

the botnet. **Figure 7**, below, depicts a typical peer-to-peer network topology in which each computer communicates with all of the other computers in the network.

Fig 7
Peer-to-Peer Network



37. Further, due to its network architecture, ZeroAccess is one of the most robust and durable botnets on the Internet today. In fact, it recently withstood and recovered from an attempt made by a major security software company to neutralize it. Indeed, following this recent attempt to stop it, the cybercriminals behind ZeroAccess added additional layers of redundancy to the network, making it even harder to disrupt, much less eradicate.

38. Regardless of a botnet's structure, malicious and criminal actors often use botnets because of their ability to support a wide range of illegal conduct, their resilience against attempts to disable them, and their ability to conceal the identities of the malefactors controlling them.

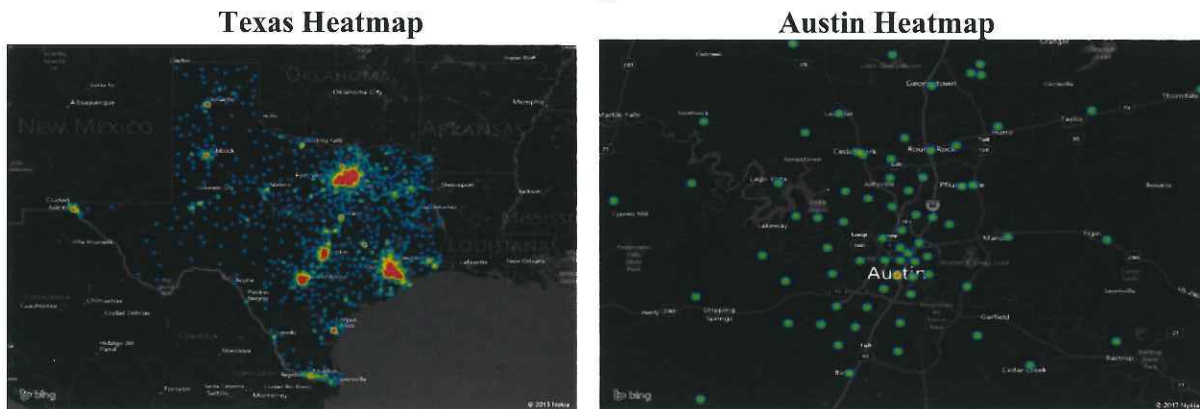
39. Botnets provide a very efficient means of controlling large numbers of computers and targeting any action internally against the contents of those computers or externally against other computers on the Internet. The botnet operators can use the network of infected personal computers for various nefarious and criminal activities including spam, denial of service attacks

on other computers connected to the Internet, theft of financial and banking data, eavesdropping, stalking, and other schemes. Access to the compromised personal computers can also be sold, leased, or swapped by one criminal group to another.

C. **ZeroAccess-Infected Computers Are Spread Worldwide With Numerous Infections In Texas**

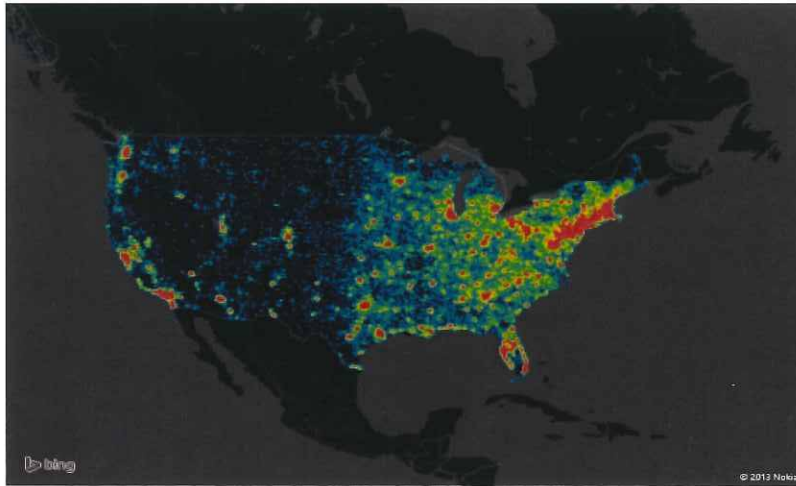
40. The ZeroAccess botnet has its major concentrations of infected computers in the United States and Western Europe. As part of its investigation, Microsoft determined the geographic location of a large sample of these computers from October 12-26, 2013. **Figure 8**, below, shows the location of ZeroAccess infected computers in the state of Texas. Each blue marker on the map represents at least one user computer that the controllers of the ZeroAccess botnets specifically directed malicious code toward, to infect that computer and make it part of the botnets, and to carry out malicious activities through that computer. Yellow or red coloration indicates an increasing concentration of infected computers. As can be seen, the operators of the ZeroAccess botnet have directed such code to computers located in Texas including computers in the Austin area.

Fig. 8



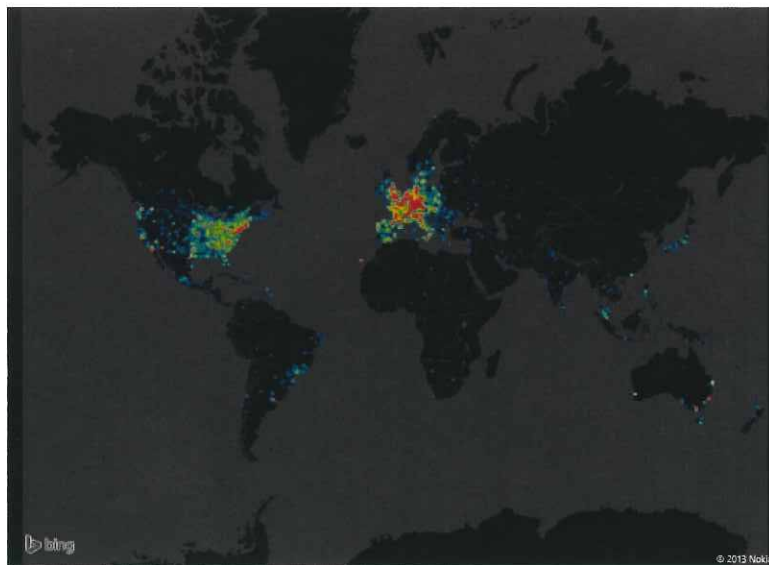
41. **Figure 9**, below, shows the location of ZeroAccess-infected computers in the United States.

Fig. 9



42. **Figure 10**, below, shows the location of ZeroAccess-infected computers worldwide. The relatively low number of infections in Eastern Europe is potentially significant. In my experience, cybercriminals often avoid attacking computers located in the region where they base their operations so as to avoid provoking their local law enforcement authorities to take action against them.

Fig. 10



D. ZeroAccess Causes Serious Damage To The Computers It Infects And Enlists Them In Illegal Activity

1. Initial Infections Occur Primarily Through “Drive-By” Downloads

43. I have studied the mechanisms through which ZeroAccess infects computers, and I have concluded that the majority of ZeroAccess infections result from what are known as “drive-by-downloads.” In a drive-by-download, a cybercriminal creates a website and stages on that website specialized software known as an “exploit pack” designed to infect end user computers. These websites are known as “exploit websites.” When a user’s computer connects to such a 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 execute code or hook malware into the operating system. If the exploit pack finds a vulnerability, it downloads and installs the ZeroAccess malware or other malware onto that computer. For further information on how ZeroAccess is installed through exploit packs and deceptive techniques, *see* Wyke, “ZeroAccess,” attached hereto as **Exhibit 11**, at page 5. I have reviewed this article, and its conclusions are consistent with my own.

44. To bring users to the exploit website, the cybercriminal will typically plant redirector code on other websites on the Internet. These may be popular websites that the cybercriminal has hacked specifically for this purpose, or websites specially designed to lure the unsuspecting and then redirect them to the exploit website. When an unsuspecting user browses to one of these websites, the redirector code on the website automatically and surreptitiously causes the user’s computer to be connected to the exploit website.

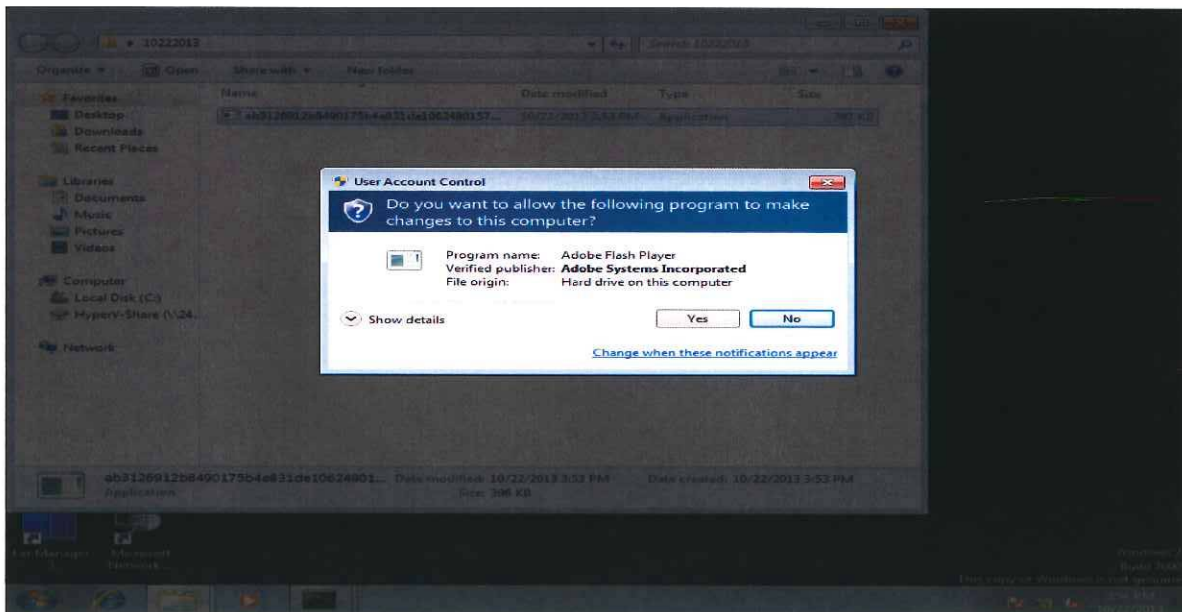
45. ZeroAccess may also infect user computers using “Trojan software,” a practice where the botnet operators disguise the malware as legitimate software that the computer owner might want to download and install on their computer. The malware, for example, may be disguised as an online video game. The ZeroAccess botnet operators will place the disguised malware on a website that hosts the purported online game with a filename designed to trick users into downloading and installing the malware.

46. Once infected, the user's computer becomes part of the botnet, able to communicate with and receive instructions from the botnet's operators as described in detail below, giving the botnet operators control over the user's computer.

2. **ZeroAccess Damages The Windows Operating System And Internet Explorer During Installation**

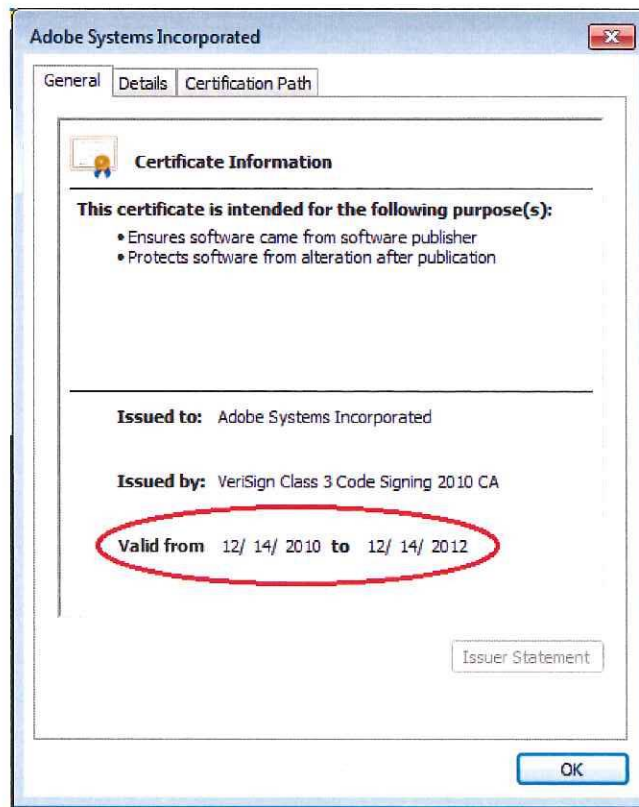
47. ZeroAccess malware needs administrator access privileges to install itself. In most cases, to acquire that level of access, it will seek to fool the user into allowing it to run with that level of access. It does this by pretending to be a legitimate upgrade for software on the user's computer, and by fooling the user into launching the false, counterfeit "upgrade" as an administrator. For further information on infection process, see the discussion in Wyke, "ZeroAccess" attached hereto as **Exhibit 11**. I have reviewed this article, and its conclusions are consistent with my own. Shown in **Figure 11**, below, is an example of an attempt by ZeroAccess, masquerading as an upgrade to Adobe Flash, to induce the user to run it under administrative privileges.

Figure 11



48. If the user inspects the certificate information, the user will be presented with a certificate from Adobe, as shown in **Figure 12**, below. The certificate was validly signed by Adobe, but is no longer valid as it is out-of-date. The high infection rate reported for ZeroAccess indicates that most victims do not inspect the certificate, and if they do, don't notice that it is out-of-date. The fact that the cybercriminals need to resort to these deceptive practices to get around normal Windows defenses shows that the spread of the ZeroAccess botnet is not related to a security flaw in Microsoft's system.

Fig. 12



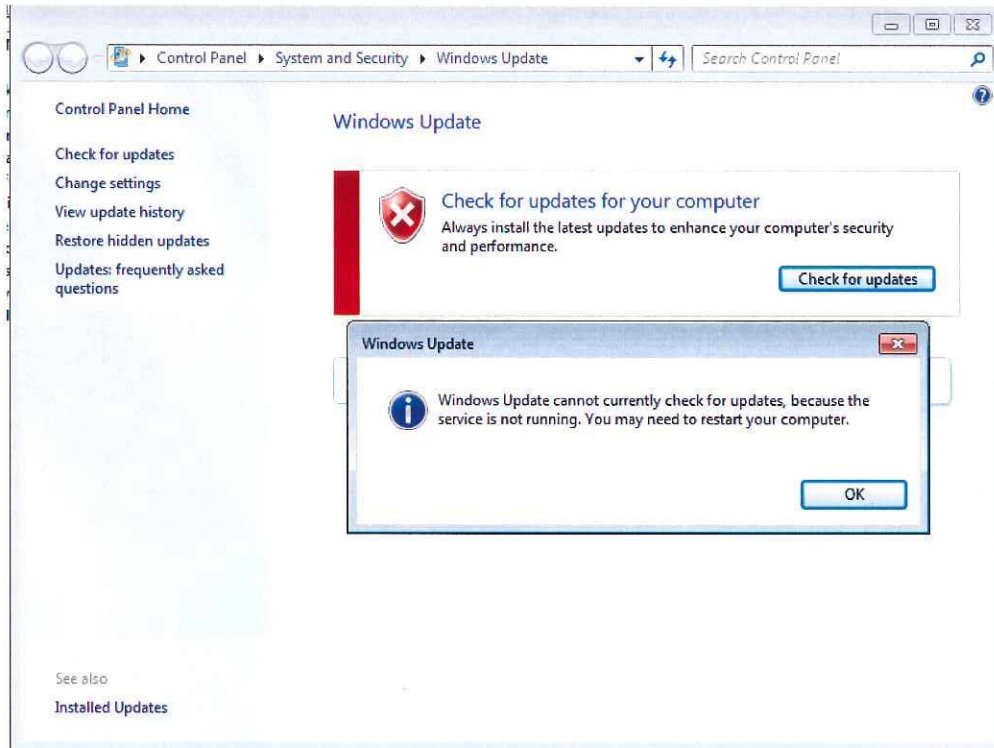
49. Once able to install, ZeroAccess makes damaging changes to the Windows operating system and to Internet Explorer. It creates hidden directories, overwrites software drivers needed by the operating system, injects itself into low-level processes, and makes changes to the system registry, which is a primary repository of crucial information the computer needs to run correctly. It also injects code in the Internet Explorer process, effectively

converting Internet Explorer into a malware program which, though still bearing the name Internet Explorer, instead becomes a counterfeit instrument of fraud. For further information on the ZeroAccess installation process on Windows and the damage it causes, see Giuliani, “ZeroAccess—an advanced kernel mode rootkit,” attached hereto as **Exhibit 12**. I have reviewed this article, and the conclusions reached are consistent with my own.

3. ZeroAccess Malware Has Built-In Self-Defense Features

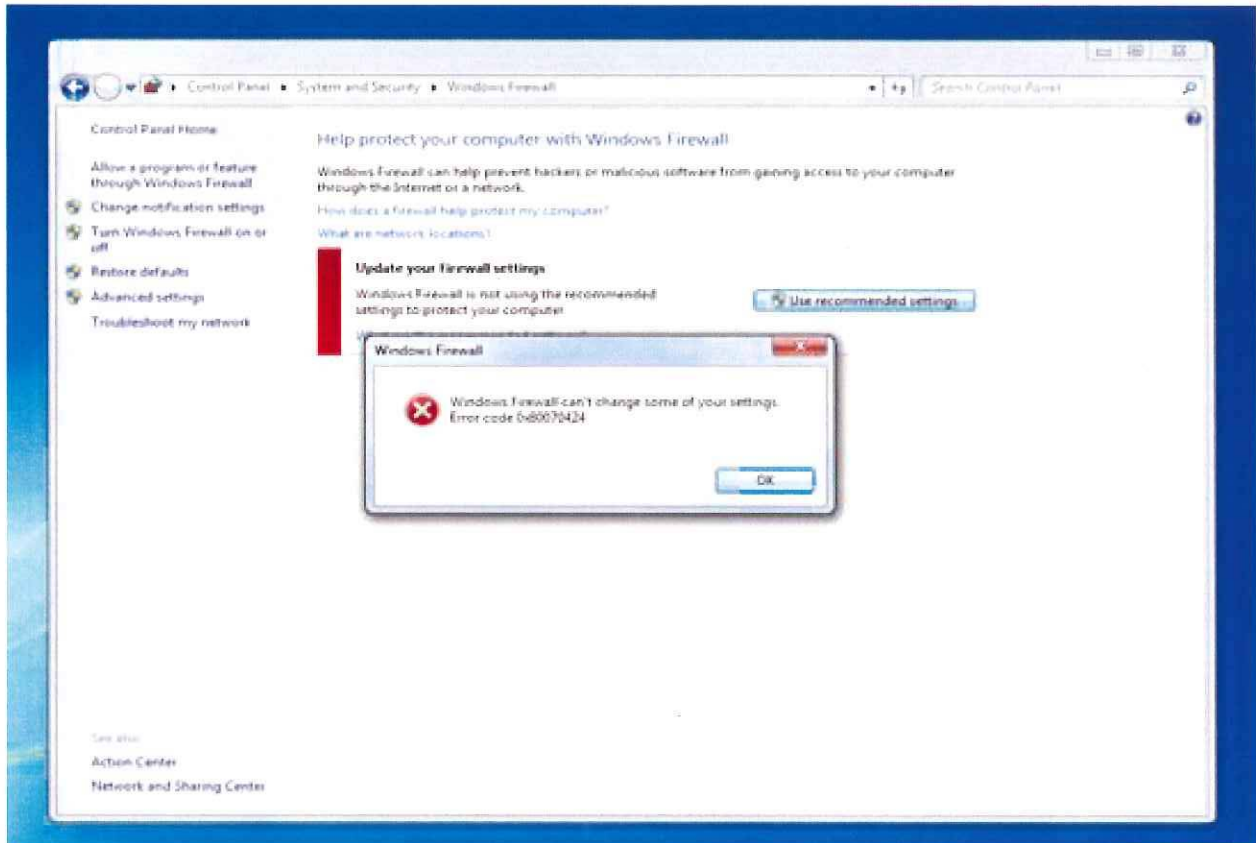
50. The ZeroAccess malware employs multiple defensive features. First, all of its key components are encrypted, which make it difficult to counter. Second, the ZeroAccess malware will disable security features on the infected computer, lowering security credentials and disabling Windows security. The ZeroAccess malware, by disabling these services, keeps infected computers from, among other things, automatically installing security updates from Microsoft. It disables the following Windows services: Base Filtering Engine Service, IP Helper service, Windows firewall service, Windows Defender service, Windows Security Center Service), and Proxy Auto Discovery Service. For example, **Figure 13**, below, shows the error message received when trying to update Windows antivirus software on a ZeroAccess-infected computer.

Fig. 13



51. As a second example, **Figure 14**, below, shows the message received when attempting to enable Windows firewall on a ZeroAccess-infected computer.

Fig. 14



52. **Figure 15**, below, shows the message received as a result of ZeroAccess disabling a common utility used to clean unwanted software off of a computer.

Fig. 15



4. Enlistment In Peer-To-Peer Network

53. In the next step of the infection, a ZeroAccess-infected computer joins the peer-to-peer network made up of other ZeroAccess infected computers around the world. When first installed, ZeroAccess contains a configuration file listing the Internet addresses of up to 256 known ZeroAccess infected computers. These are peers of the newly infected computer. The newly-infected computer starts attempting to make contact with each of these at the rate of one per second. Each time it makes contact with one of these peers, it asks that peer to send it a list of that peer's most recent contacts in the peer-to-peer network. Depending on how a peer is connected to the Internet, it may be able to respond or not; approximately one of twelve is able to respond, and these are termed "super-nodes." The newly infected computer saves the new peer addresses sent to it by the super-node in a second list, and it begins contacting those as well at the rate of one per second. The process repeats *ad infinitum* among the peers, all of which are

constantly making inquiries of, and responding to inquiries from, other peers. In this manner, the ZeroAccess-infected computers are able to all maintain very up-to-date lists of all active computers in the botnet. For further discussion on how a newly infected machine interacts with the peer-to-peer network, see Wyke, “ZeroAccess” attached hereto as **Exhibit 11**, at p. 18. I have reviewed this article, and its conclusions in this section are consistent with my own.

54. By itself, this mechanism is somewhat vulnerable to a type of countermeasure employed against peer-to-peer botnets in the past known as “network poisoning.” In the recent past, a major vendor of Internet security software attempted such a measure against ZeroAccess. In response, the cybercriminals behind ZeroAccess upgraded the malware. Now, each ZeroAccess infected computer contains a third list comprised of all of the peer nodes that it has communicated with at any time in the past. This list can contain up to 16 million addresses. Each infected computer now continually cycles through this list as well as its other two lists, repeatedly exchanging information with all of the nodes it has communicated with in the past. By employing this triple-list mechanism, the cybercriminals behind ZeroAccess have created a durable peer-to-peer botnet.

IV. ILLEGAL ACTIVITIES OF ZERO ACCESS

A. The Infected Computers In The Peer-To-Peer Network Rely On A Separate Set Of Servers For Coordination Of Their Illegal Activities.

55. The infected computers in the peer-to-peer network rely on a separate set of servers for coordination of their illegal activities. These servers are a vulnerable point in the ZeroAccess control infrastructure. When ZeroAccess first infects a computer, it does not contain the files or modules required to commit actual click fraud or browser hijacking. Instead, it must acquire these from a peer it contacts. Each time a ZeroAccess-infected computer contacts any other peer, it also asks what other ZeroAccess modules or files that peer has. It checks the response against its own files or modules, and requests anything more recent than what it has. In this way, updated click fraud and browser hijacking modules and configuration files are propagated quickly through the peer-to-peer network.

56. Some of the files a ZeroAccess-infected computer will acquire in this fashion contain a list of domain names. A domain name can be thought of as the name of a website. Currently, each list contains twelve domain names, but there are two distinct lists in circulation, meaning there are a total of 24 such domain names. In this case, the domain names are just strings of characters that the ZeroAccess-infected computer will decode to generate a number. That number is an IP address.³ Each ZeroAccess-infected computer, working from its list of twelve domain names, currently decodes them to a corresponding list of twelve IP addresses. At present, the domain names in both lists decode to the same set of twelve IP addresses. In addition to these twelve encoded IP addresses, a ZeroAccess-infected computer may also download a file containing six un-encoded IP addresses. Any of the IP addresses provided through these mechanisms are the Internet addresses of server computers on the Internet. These computers are not part of the peer-to-peer network of infected computers. Instead, they give the infected computers explicit instructions on how to commit the click fraud or browser hijacking. This list of IP addresses changes gradually over time. As discussed, there are currently 18. I will refer to these as the “Fraud Control IP Addresses” and to the computers connected at those addresses as the “Fraud Control Servers.” These IP addresses and domain names are listed in Appendix A to Microsoft’s complaint in this matter. Appendix A also includes an additional 25 domain names that ZeroAccess has used in the past as part of its IP address-encoding mechanism but that currently appear to be inactive. At present, ZeroAccess-infected computers also do a DNS-lookup⁴ on the domain names. They do not appear currently to make any use of the information received as a result of these lookups, but it is possible that, if the cybercriminals behind ZeroAccess controlled these domains, this process could be used as a way for them to

³ An “IP address” is a number assigned to devices connected to the Internet, which is used to route communications to and from them. In effect it represents the network location of a given device and gives some indication of the device’s physical location as well.

⁴ “DNS” stands for “Domain Name System,” which is the directory service for the Internet. In the same fashion that a person could look up a name in a phone book and get a corresponding phone number, a computer can look up a domain name in the DNS system and get a corresponding IP address.

send additional information to the infected computers, and therefore this could serve as a fallback mechanism. *See also* Pearce *et al.* attached hereto as **Exhibit 1**, p. 14, Table 5, The current eighteen ZeroAccess IP Addresses appear to be maintained by ISPs located in Latvia, Luxembourg, Switzerland, the Netherlands, and Germany. The role played by the computers at these IP addresses is discussed below.

57. ZeroAccess can and has been reported to engage in multiple types of fraud including spam, bit-coin mining, browser hijacking, and click fraud. *See* Pearce *et al.*, **Ex. 1**, p. 2. Currently, the cybercriminals behind the ZeroAccess botnet appear to be focusing the resources of the botnet on the latter two activities, which are primarily means of generating traffic. They monetize the hijacked traffic and fraudulent clicks they generate from infected end-user computers by selling that traffic to other cybercriminals or to traffic brokers. Additionally, operating as “traffic brokers” themselves, may also sell traffic directly to website owners to increase the visits to specific websites. They might also turn over the hijacked traffic to other traffic brokers for a fee. I describe each of these in detail below.

B. ZeroAccess Conducts Browser Hijacking

58. Browser hijacking operates as follows: First, through a web browser such as Internet Explorer, the user uses a search engine, for example Bing, Yahoo! or Google, to search for a particular topic. The search engine returns a list of results, and the user reviews the links and determines which to click on. So far, all appears normal. However, as soon as the user clicks on one of the links, the ZeroAccess malware running on the user’s computer redirects their browser to a computer server at one of the Fraud Control IP Addresses and transmits to that server the search terms that the user used in their search. With that information, the command and control server redirects the user’s computer it to one of numerous possible websites chosen by the botnet operators, all the while misrepresenting to the user that they are using the Bing-branded search engine containing Microsoft’s Bing trademark and the Internet Explorer-branded browser. For example, **Figures 15 and 16**, below, shows the differing results for a user who

searches for the term “spongebob” on a clean computer (**Fig. 15**), versus on a ZeroAccess-infected computer (**Fig. 16**). On the clean computer, the browser connects to the website “spongebob.nick.com,” and then downloads further information from Nickelodeon sites and advertisements provided from Google’s ad network. On the ZeroAccess infected computer, however, the browser is hijacked and is sent first to two unnamed computers IP address on the Internet, and from there is connected to a website called “alt.slpad.com.” The error message that pops up at that point, shown enlarged in **Figure 17**, notifying the user that the computer has been infected, is typical of a scareware scam. If the user calls that number, the people responding will likely attempt to trick the user into paying to have their computer “cleaned.”

Fig. 15

“spongebob” Search – Clean Computer

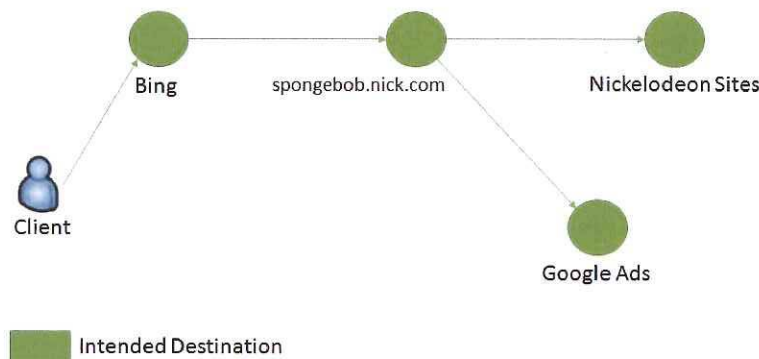


Fig. 16

“spongebob” Search – Infected Computer

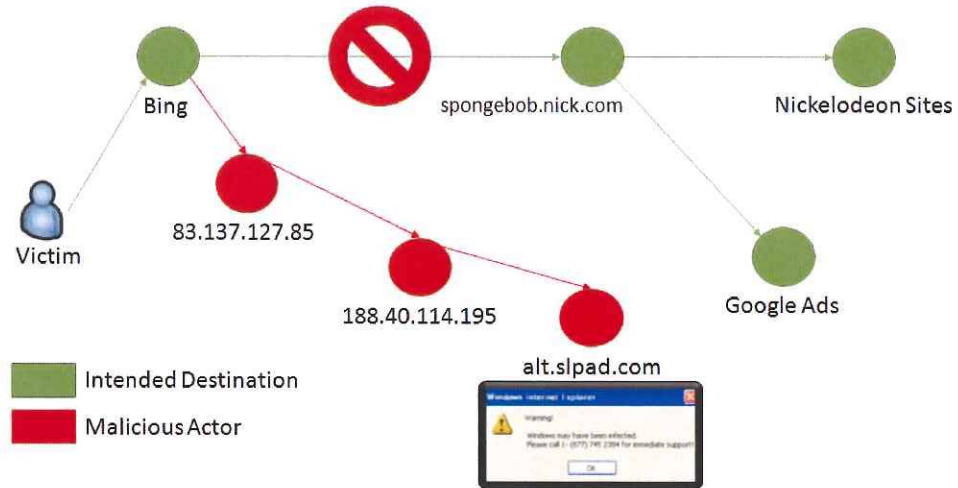


Fig. 17

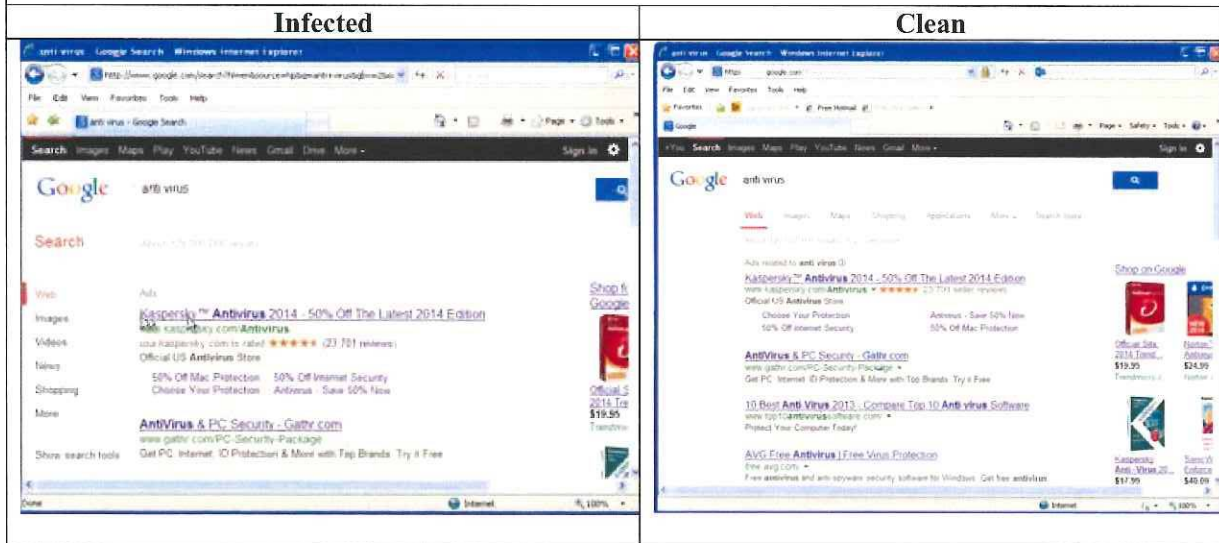


59. For example, if the user searched using the terms “antivirus software,” the command and control server might redirect the user’s computer to a website on which counterfeit versions of antivirus software, or even malware masquerading as antivirus software, is available for download. As part of the research into ZeroAccess, investigators ran various searches and monitored what occurred. I have excerpted a few screen shots from those searches which I

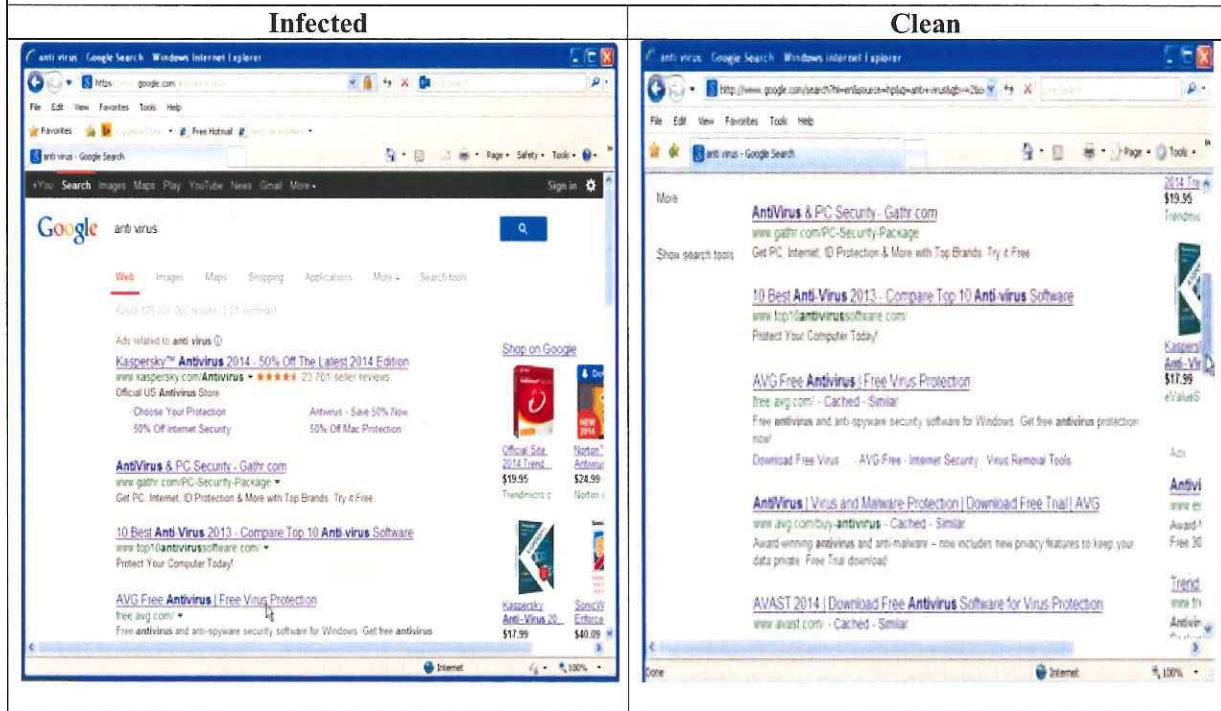
include and explain below in order to give a clear idea of what the user sees if their computer is infected with ZeroAccess.

60. The series of images below in **Figure 18**, shows a comparison between what occurs during a search on an uninfected computer on the right, versus the same search on a ZeroAccess-infected computer on the left.

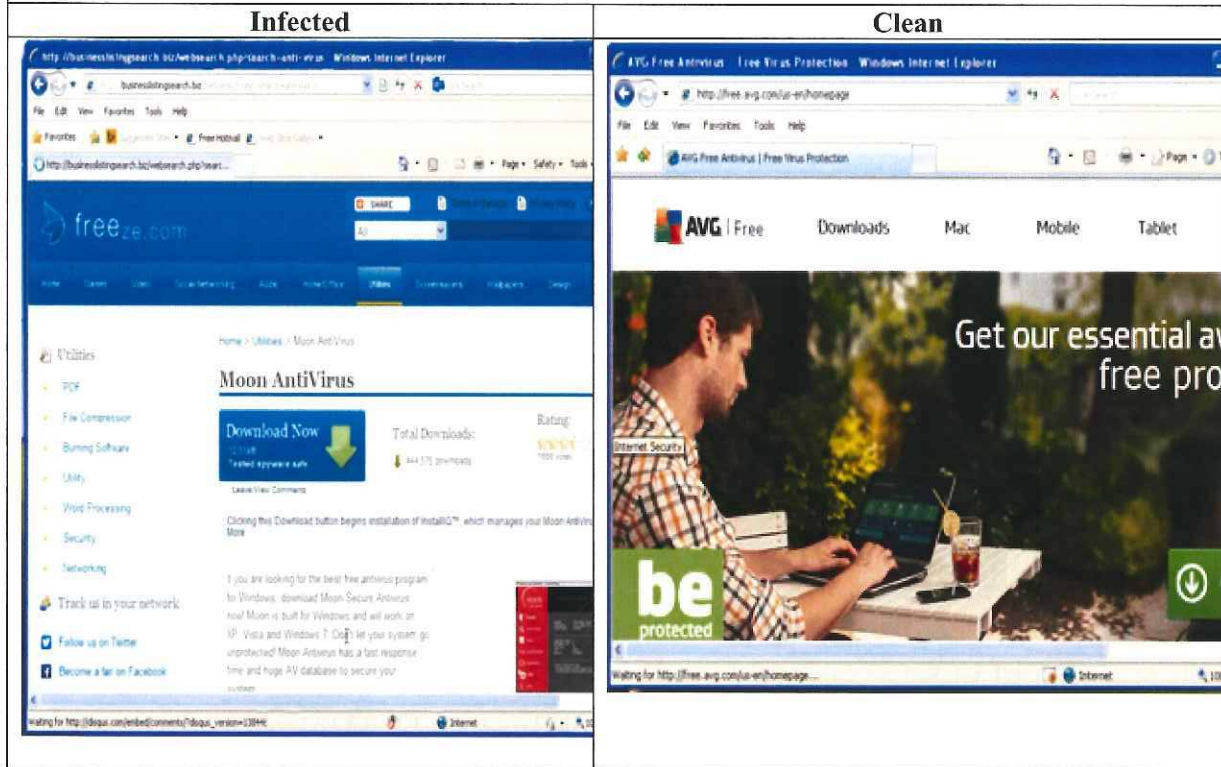
Step 1 (below): The user enters the same search term in Google on both the ZeroAccess-infected (left) and the clean computer (right). At this stage, the browser on both computers returns the same set of links in the results.



Step 2 (below): On both computers, the user clicks on the same link, "AVGFree Antivirus." This link corresponds to a website named "free.avg.com."



Step 3 (below): On the infected computer, the browser is hijacked and taken to the website called “businesslistingssearch.biz.” The entity behind that website has evidently purchased the traffic generated by ZeroAccess, potentially through one or more traffic-brokers. On the clean computer, the browser goes to the website indicated by the link the user clicked on, AVG Free Antivirus (free.avg.com).



61. In the sequence of events described above, the ZeroAccess-infected computer connects to the website for Moon AntiVirus. Microsoft investigators downloaded the installation package from this website and had it scanned by various antivirus products. Several of these products determined that the package contained “adware.” The term “adware” refers to a type of application, which, when running on a user’s computer, connects to one or more sources of online advertisements, and continually shows a steady stream of those advertisements to the person operating the computer. Upon installing the package, we determined that, in addition to Moon AntiVirus, the package also installed an application calling itself “WeatherBug.” **Figure 19**, below, shows the “WeatherBug” application after it has been installed, displaying advertisements. In effect, what has occurred is that the group behind this particular download of

Moon AntiVirus purchased traffic that was generated by a ZeroAccess infected computer. While Moon AntiVirus can be downloaded for free, the purveyors of Moon AntiVirus probably hope to make money on a pay-per-view or pay-per-click basis through displaying advertisements on the computer via the “WeatherBug” application.

Fig. 19



62. Search Engine hijacking can connect users to unsafe webpages and prompts users to install counterfeit software, malicious code and spyware. In **Figure 20**, below, the user’s browser is hijacked and connected with a domain that installs a type of malware known as “scareware” on the computer. The scareware pretends to scan the computer and falsely reports a threat related to child pornography. As the scam unfolds, the perpetrators attempt to get the user to pay them money to “fix” their computer and remove the bogus threat. Of course, the real threat, ZeroAccess, remains on the user’s computer. In effect, the cybercriminals propagating the scareware have purchased traffic generated by the cybercriminals operating ZeroAccess and

Suddenly, a classic type of malware known as “scareware” launches on the user’s computer. This malware pretends to have launched a security scan of the user’s computer (in fact, no security scan is being conducted), and to have found a threat related to child pornography. The goal of this malware is to induce the user to click on the button in the lower left to “Get full time protection now.” Typically, this type of scam ends with an attempt to coax the user into making a credit card payment in order to get the “full-time protection.” In the meantime, the computer is effectively unusable—there is no way for the user to get rid of the fake security scan dialog without removing the malware that has infected the computer



63. ZeroAccess may also connect infected computers to websites that offer free versions of popular software. When the user attempts to download the software, some other payload, potentially malware, is installed instead. **Figure 21**, below, is a webpage to which a hijacked browser is taken. The webpage prompts the user to download software masquerading as a popular Microsoft game called “Halo.” In fact, if the user clicks the install button, while the Microsoft Halo end user license agreement is displayed and non-functioning Halo files are downloaded, the real payload is unwanted software including “Search Protect” (reported as a browser hijack that changes the user’s homepage and search provider), “PlusHD” (reported as virus-like adware) and “SpeedUpMyPc” (reported as virus-like adware) are installed in the background.

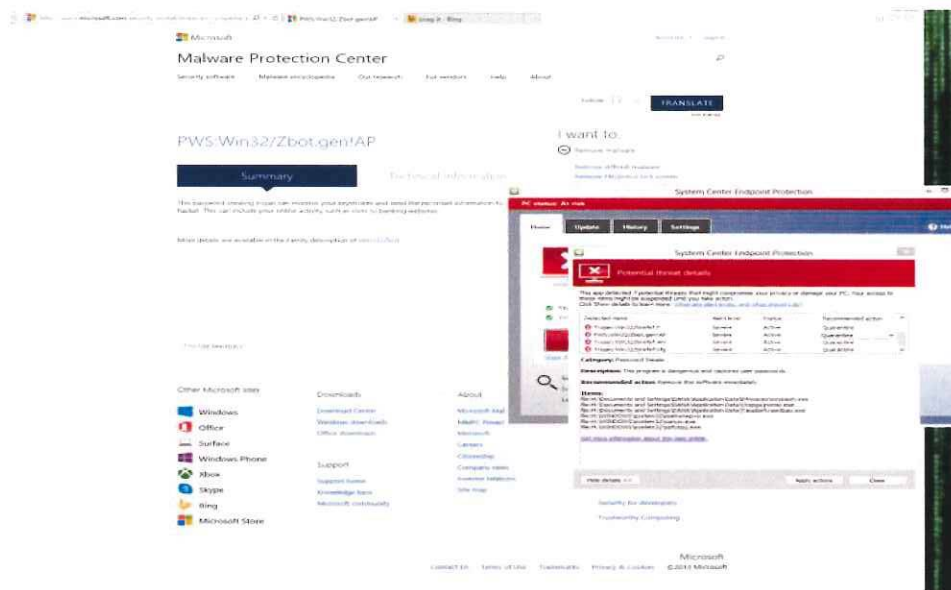
Fig. 21



64. Sometimes, the user has no notice that they have been connected to a dangerous website. Often, there is no effective visual indication to the user that the browser is connecting to multiple websites and downloading information from them. Thus, it is possible for a ZeroAccess-infected computer to be connected to a website hosting an exploit pack for a second malware infection. In fact, in one test conducted as part of this investigation, we determined that the browser had connected to a website that then downloaded the Zeus malware to the computer as shown in **Figure 22**. Zeus is a financial fraud botnet that spies on the owner of the computer and steals their financial account information, including account numbers, account balances, and passwords for online banking. The criminals behind Zeus then use this information to surreptitiously empty the victim's bank account. In December 2012, Microsoft and other plaintiffs from the financial industry won a default judgment against the operators of Zeus in the matter *Microsoft et al. v. John Does 1-39*, Civil Action No. 1:12-cv-01335-SJ-RLM (E.D. N.Y.),

taking down significant portions of that botnet. In spite of these concerted efforts and successes, branches of the Zeus botnet live on, and the operators of Zeus are evidently using ZeroAccess-generated traffic to infect more computers and rebuild their criminal operation.

Fig. 22



C. **ZeroAccess Click Fraud**

65. One of the primary illegal activities engaged in by ZeroAccess-infected computers is click fraud, which occurs in the background without visible indication to the computer operator. When ZeroAccess-infected computers are turned on, the ZeroAccess malware running on those computers will connect with one or more of the 18 IP addresses listed in Appendix A to Microsoft’s Complaint. The computers at those IP addresses provide the ZeroAccess-infected computer with a list of URLs, each pointing to a website to connect to. When a ZeroAccess-infected computer connects to a website that contains an advertisement, the browser on the infected computer downloads the advertisement. At that point, the ZeroAccess malware simulates a click on the advertisement. It then moves on to the next website in its list and repeats the process.

66. The way the operators of ZeroAccess monetize this activity is complex.

Referring to paragraphs 21-30, above, in which I discuss how traffic is bought and sold on the Internet, the operators of the ZeroAccess botnet are in the position of being able to sell traffic to traffic arbitragers or website publishers interested in using it to generate advertising revenue on the Internet. Because the ZeroAccess operators can program their army of infected computers to go to any website on the Internet and click on advertisements, they are in a strong position to sell the traffic and clicks thus generated at a premium price.

67. The extent of the click fraud perpetrated by ZeroAccess-infected computers was demonstrated in research published on May 20, 2013 by the Microsoft Malware Protection Center, which has been part of the team investigating ZeroAccess, attached hereto as **Exhibit 13**. (Blizard and Livic, MMPC, “The Wonder of Sirefef Plunder”). In that study, Microsoft investigators looked at the effect on clicks on the Microsoft ad-network of adding anti-ZeroAccess files to Microsoft’s antivirus software, which occurred on February 13, 2013, which resulted in ZeroAccess being cleaned off of nearly 500,000 computers. Microsoft monitored the activity of 1874 of those computers on its advertising platform, and was thus able to measure the impact on click traffic of cleaning them. In **Figure 22**, below, the orange line represents the number of clicks made by the 1874 monitored computers on advertisements on websites of Publishers participating in Microsoft’s ad platform. It can be seen that ZeroAccess accounted for approximately two thirds of the clicks made by these computers on advertisements on Publisher websites participating in Microsoft’s advertising platform. This is consistent with additional research on a single infected system, which, over a twelve day period, generated 509 ad requests and clicked on 43 of those ads, which would have resulted in revenues of \$9.07, had the fraud not been detected.⁵

⁵ We estimate that, on average, a single infected computer would generate approximately 1164 ad requests per day. Based on our observation of infected computers, approximately 4% of the traffic generated was directed at Microsoft’s advertising platform. The remaining 96% was directed at other advertising platforms.

Fig. 22

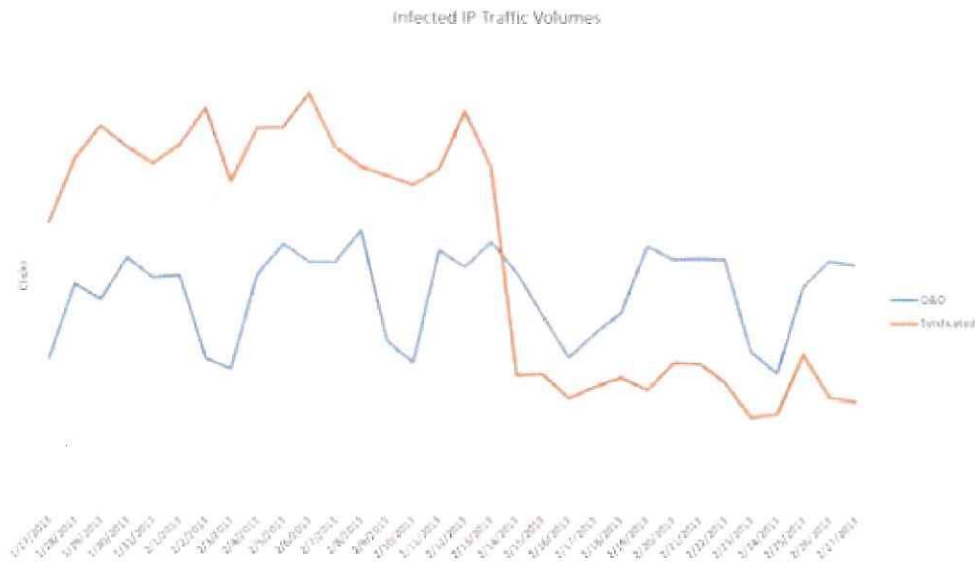


Figure 1: Sirefef infected IP traffic volumes.

V. ZEROACCESS DIRECTLY DAMAGES MICROSOFT AND ITS CUSTOMERS

A. ZeroAccess Damages Infected Computers Thereby Damaging Computer Owners And Microsoft

1. ZeroAccess Corrupts The Windows Operating System And Places The Computer At Risk Of Secondary Infections

68. Based on my investigation, ZeroAccess makes damaging changes to the Windows operating system. It creates hidden directories, overwrites software drivers needed by the operating system, injects itself into low-level processes, and makes changes to the system registry, which is a primary repository of crucial information the computer needs to run correctly.

69. The ZeroAccess malware will also disable security features on the infected computer, lowering security credentials and disabling Windows security, leaving the computer susceptible to secondary infections. It disables Base FilteringEngine Service, IP Helper service, Windows firewall service, Windows Defender service, Windows Security Center Service, and

Proxy Auto Discovery Service. The ZeroAccess malware, by disabling these services, keeps infected computers from, among other things, retrieving security updates from Microsoft. These events take place without the knowledge or authorization of the end-user, as ZeroAccess runs as a background process (that is, it runs in the background, has no user-interface, and gives the computer's owner no indication that it is present or running). As shown above, the fact that ZeroAccess disables a computer's defenses is particularly dangerous in that ZeroAccess also connects the user's computers to multiple websites from which the computer may be attacked by secondary malware infections.

2. **ZeroAccess Corrupts Internet Explorer And Degrades The Use Of Bing**

70. ZeroAccess injects code in the Internet Explorer process, effectively converting Internet Explorer into a malware program which, though still bearing the name Internet Explorer, instead becomes an instrument of online fraud. It hijacks Internet searches carried out on a user's computer. The ZeroAccess malware monitors when the user visits any major search engine, including the Bing.com search engine, and intercepts the search terms that the user types into Bing. After Bing returns links for search results, the ZeroAccess malware detects when the user clicks on any of those links. Instead of taking the user to the webpage of the link, the ZeroAccess malware intercepts the click and redirects the user to a completely different website chosen by the cybercriminals behind ZeroAccess. All of this activity occurs without the user's consent. Further, ZeroAccess also repeatedly launches hidden browser instances, causes them to navigate to websites of the cybercriminals' choice and causes the user's computer to "click" on advertisements placed on those websites. All of this activity is hidden to the user. They do not know that these clicks are taking place and have not consented to it.

3. **ZeroAccess Consumes Computing Resources And Degrades The Performance Of End-User Computers**

71. Because of the operations described above, a ZeroAccess-infected end-user computer's processing power, memory, communications bandwidth, and other resources will be

used for the high volume of processing, data transfer and connections to the Internet that the ZeroAccess-infected end-user computer engages in. Users have reported computer performance degradation that has been attributed to ZeroAccess malware. I have personally observed that ZeroAccess-infected computers perform standard operations at a detectibly slower pace, which I attribute to the background activity being conducted by the ZeroAccess malware on the computer. One security researcher has estimated that the ZeroAccess-related Internet activity on a typical infected computer adds up to about 32 Gigabytes per month, which is the equivalent of downloading 45 full-length movies. See McNamee, Kindsight, “Malware Analysis Report, New C&C Protocol for ZeroAccess/Sirefef” attached hereto as **Ex. 14**. The high volume of Internet traffic generated by an infected computer estimated by this researcher is consistent with the constant level of Internet activity I have observed in ZeroAccess infected computers.

4. Microsoft Customers Waste Time Combating ZeroAccess Infections

72. Owners of ZeroAccess-infected computers are typically unaware that their machines are infected and operating as part of a ZeroAccess botnet, or that their computers are secretly engaged in illegal activity. The ZeroAccess malware is designed to be hidden. Users that become aware that ZeroAccess is wrongfully installed on their system must expend time and experience frustration in an attempt to remove ZeroAccess from their systems. Indeed, given the way that ZeroAccess installs itself, users attempting to clean it from their system unassisted run the risk of causing their browsers or computers not to operate correctly. Attached hereto as **Exhibits 15-18** are reports from customers describing some of the difficulties they have experienced in attempting to remove ZeroAccess from their computers.

B. ZeroAccess Irreparably Harms Microsoft

1. ZeroAccess Damages Microsoft’s Reputation, Brands, And Goodwill

73. ZeroAccess irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows operating system, Internet Explorer, Bing, and a variety of other software and services. Trademark registrations for marks

infringed by the creators of the ZeroAccess botnet are attached to Microsoft's complaint as Appendix C. 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 expenditure 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, Internet Explorer, and Bing marks.

74. The activities of ZeroAccess injure Microsoft and its reputation, brand, and goodwill because users subject to the negative effects of these malicious applications incorrectly believe that Microsoft, Windows, Internet Explorer, Bing, or Bing Ads are the sources of their computer problems. For example, because of ZeroAccess, users get less relevant and often harmful or dangerous search results, as their browser and the Bing search engine is hijacked to less relevant, dangerous or offensive sites. There is a great risk that end-users may attribute this problem to Microsoft and associate these problems with Microsoft's Bing and Bing Ads products, thereby diluting and tarnishing the value of these trademarks and brands.

75. In order to carry out the intrusion into end-user computers, the Defendants cause the ZeroAccess command and control servers to make repeated copies of Microsoft trademarks onto end-user computers, in the form of file names and registry paths containing the trademarks "Windows" and "Microsoft." 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.

76. Based on my experience assessing computer threats and the impact on business, I conclude that customers may, and often do, incorrectly attribute the negative impact of the ZeroAccess botnet and other malware downloaded to their computers as a result of having their browsers hijacked and redirected to malware download sites to Microsoft. 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.

2. ZeroAccess Costs Microsoft Time And Money To Combat

77. Microsoft devotes significant computing and human resources to combating ZeroAccess 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 end-users combat ZeroAccess, it must also expend resources in monitoring its online advertising platform for fraudulent traffic and clicks, filtering them out before they do damage where possible, and reimbursing advertising customers where it is discovered after the fact. These efforts require in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft's advertising customers.

3. ZeroAccess Damages Microsoft-Licensed Software

78. Microsoft and its customers are injured when the ZeroAccess botnet software and other malware is maliciously introduced onto people's computers making them part of the botnet. The installation of the botnet software by deceiving consumers is an intrusion into and corruption of the Microsoft Windows operating system, without Microsoft's authorization. The Windows operating system is licensed by Microsoft to its customers. Attached as **Exhibit 19** is a true and correct copy of the Windows 8 end-user license agreement. Attached as **Exhibit 20** is a true and correct copy the Windows 7 end-user license agreement. Attached as **Exhibit 21** is a true and correct copy of the Windows Vista end-user license agreement. Attached as **Exhibit 22** is a true and correct copy of the Windows XP end-user license agreement.

4. ZeroAccess Damages Microsoft Advertising Platform And Its Customers That Use It

79. ZeroAccess also adversely affects Microsoft's advertiser customers, other advertisers and website owners, who legitimately pay service providers such as Bing Ads to

increase targeted traffic to their website. Advertisement owners (people who create ads for their business) place their ads on specific pages, or associate their ads with keywords in search engines, so that end users searching for relevant items may visit the ad owners' website.

ZeroAccess and similar malware skew this relation grossly. By generating non-user initiated clicks and website visits ZeroAccess increases traffic to the ad owners' website but none of that traffic leads to potential sales. This results in the ad owners paying the ad distributor as the ads were clicked on, but in reality the ad owner paid for traffic that was of no use.

80. Bing advertisers bid for ad placement on Bing search results. But ZeroAccess changes the results on user's computer. The advertiser is not charged by Bing because their link does not get clicked on, but the advertiser is harmed nonetheless: their ads are down-graded as less relevant as they are not clicked on. It makes it harder for their ads to get good placement on future search results. It is a form of reputational harm.

81. There is a great risk that advertisers may attribute this problem to Microsoft and associate these problems with Microsoft's Bing and Bing Ads products, thereby diluting and tarnishing the value of these trademarks and brands.

C. Blocking Communication Between The Infected Computers And The Fraud-Control IP Addresses Is The Best Way To Disrupt ZeroAccess

82. The ZeroAccess botnet is designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. This is particularly obvious from the use of the peer-to-peer topology and the use of multiple peer node lists built into the malware, the primary purposes of which are to allow infected user computers to continue to connect to the ZeroAccess botnets and evade actions to stop the botnets' injury. In addition, as discussed above, the ZeroAccess peer-to-peer network has no central point of command and control that can be readily taken offline. The infected computers in the network can quickly spread new modules and configuration files amongst themselves, allowing the botnet operators to respond to any attack on the network through technical means. The malware on each infected computer disables the normal security features of Windows, and the malware files themselves

are encrypted.

83. However, the activities of the botnet can be disrupted by severing communication between the ZeroAccess-infected computers and the Fraud-Control IP Addresses listed in **Appendix A** to Microsoft's Complaint from which those infected computers get their instructions on how to commit browser hijacking and click fraud.

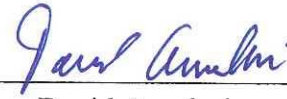
84. Piecemeal requests to filter traffic to Fraud-Control IP Addresses, informal dispute resolution or notice to the Defendants prior to filtering the traffic would be insufficient to curb the injury. Based on my experience observing the operation of numerous botnets, prior legal actions involving botnets, and my observations of the specific architecture of the ZeroAccess botnet, I believe the operators of the ZeroAccess botnet would take swift preemptive action to defend the botnet if they were to learn of Microsoft's impending action against it. For example, they could set up computers at new IP addresses and redirect the infected computers there for instructions.

85. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by botnets, but allowed the botnet operators to receive notice. In these cases, the botnet operators quickly moved the botnet infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the botnet to continue its operations and destroying or concealing evidence of the botnet's operations. Indeed, when a major security service vendor attempted to neutralize ZeroAccess, the cybercriminals running ZeroAccess were quickly able to deploy a fix that largely stymied their effort to take down the botnet.

86. Given the specific architecture of the ZeroAccess botnet and its use of the Fraud-Control IP Addresses to communicate with and control infected user computers, I believe that, if provided advance notice that the Fraud Control Servers were to be turned off, the operators of the ZeroAccess botnet would update infected computers with new (and different) primary IP Addresses representing new Fraud Control Servers, and would destroy evidence of the botnet's operation and evidence of the infected end-user computers that need to be cleaned.

87. I believe that the only way to suspend the injury caused to Microsoft, its consumers and the public, block the ability of the computers located at the Fraud-Control IP addresses to communicate instructions to the ZeroAccess-infected computers, cause the Fraud Control Servers to stop instructing infected end-user computers, and preserve evidence, is to take the steps described in the declaration of Jason Lyons (one of my colleagues) submitted along with Microsoft's TRO application, which I have read and agree with. Through this relief, the monetization capability and operational control of the ZeroAccess click fraud and browser hijacking schemes will be significantly hindered, and the Internet service providers that provide services to the owners of the infected computers can notify them that they are infected and assist them in restoring their computers to normal operation.

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.



David Anselmi

Executed this 24th day of November, 2013.