TREND MICRO

FROM RUSSIA TO HOLLYWOOD:
TURNING THE TABLES ON A SPYEYE CYBERCRIME RING

TrendLabs℠

Loucif Kharouni, Kevin Stevens,
Nart Villeneuve, and
Ivan Macalintal

A 2011 Trend Micro Research Paper

Contents

Introduction

This March, Trend Micro began investigating a specific SpyEye botnet created and controlled by a cybercriminal who goes by the handle, Soldier. This paper will delve deeper into activities related to his SpyEye botnet. It will talk about his success in instigating attacks that impacted various organizations worldwide, particularly in the United States; how his particular botnet works; and how much he has made from the malicious campaigns he has so far instrumented. It will provide insights on how Trend Micro was able to track him down from Russia to Hollywood and reveal what we learned about him and his accomplices in the process.

In 2009, the ZeuS toolkit underwent several enhancements to become one of the most notorious crimeware toolkits circulating in the underground economy. Detected by Trend Micro as ZBOT malware, variants created with the said toolkit proliferated throughout the Web until the emergence of an alleged competitor—SpyEye.

Initially detected by Trend Micro as EYEBOT malware, variants created with the crimeware toolkit, which later came to be known as SpyEye, first appeared in Russian underground forums. After a while, sales of the toolkit's versions steadily spread to other underground forums for an initial price of US$500.

SpyEye then seemed well-equipped to gain a piece of the underground market that ZeuS initially created. In fact, based on the SpyEye developments we saw, we forecast that given some time, the crimeware toolkit can even overthrow ZeuS from its throne.

Research Findings

Who Is Soldier and How Does He Make Money?

For some time now, we have been investigating a certain threat actor or cybercriminal who goes by the handle, Soldier. Soldier, believed to be a Russian man in his early 20s, appears to have been involved with ZeuS and SpyEye binary propagation since 2007.

We have collected a great deal of intelligence on Soldier and his various activities and have shared the data with law enforcement authorities. As far back as 2007, we discovered that Soldier has been using ZeuS, SpyEye, and other cybercrime toolkits (e.g., blackhat search engine optimization [SEO] kits) to spread ZeuS and SpyEye binaries. He appears to mainly target users in the United States. To increase the ZeuS and SpyEye infection count in the United States, he also bought traffic from other cybercriminals. Apart from using malware to steal user credentials, Soldier also turned a profit by using a network of money mules whom he recruited via fictitious companies such as L&O Consulting.

Figure 1. *Site of a fake company* (loconsulting.biz) *Soldier uses to recruit unknowing users as money mules*

Soldier's SpyEye money-laundering process is depicted in the figure below.

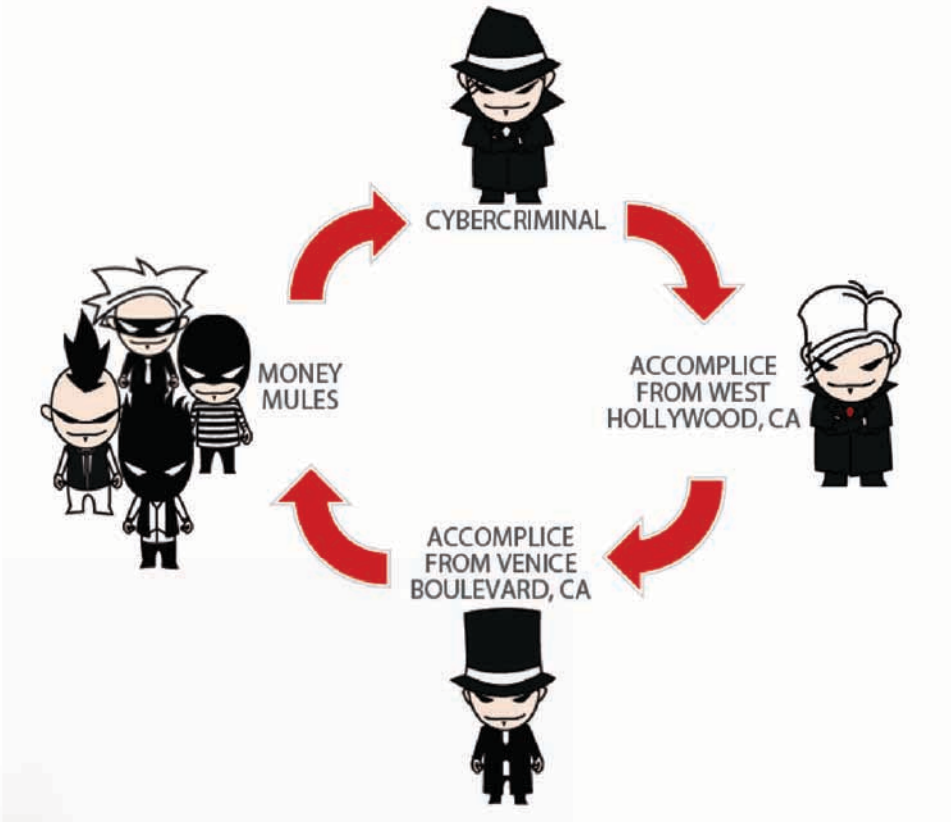


Figure 2. *Soldier's SpyEye botnet's money-laundering process*

The following email samples we obtained led us to question the legitimacy of the site shown in Figure 1 and helped us determine that the real purpose of L&O Consulting's operations was money laundering.

Quoc replies to Rose
11 Jul 2011

They change themselves again. I don't need to repeat their description, but I want to point out some of my opinions.

Jessey
Personnel manager
L & O Consulting LLC
Main e-mail: loconsulting@qmx.co
Corporate e-mail: jessey@loconsulting.biz
Tel:
Fax:
www.loconsulting.biz

Form the job description, I can be 99.99% sure it's a money laundering schema. This is what I think it would happened if I joined.

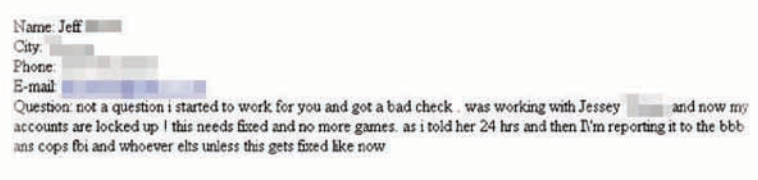
1. Someone from Russia or where else send me a check.
2. I cash it and transfer to another person.

What is the point from there: money has circulate through banking, spread out and rejoined to one, come from one to the other country.

What would be the problem to me.

1. Money coming to my account and out. How do I claim tax for my personal tax return? I can't not take all the coming in as my income. It's a killing tax rate for huge amount of money (up to 45% for Fed and CA). I cannot claim the money send out as my expend due to I'm not registered as a money transfer agency. (Check Cashing). Then that large amount of money one more time consider as my gift tax (up to 50%). There is no answer for that, a big question.
2. When there is a big question mark in my record, FBI would definitely following up on me or even worst

Figure 3. *Sample email from an angry person who has been victimized by the fake site in Figure 1*



Name: Jeff
City:
Phone:
E-mail:
Question: not a question i started to work for you and got a bad check . was working with Jessey and now my accounts are locked up ! this needs fixed and no more games. as i told her 24 hrs and then I\'m reporting it to the bbb ans cops fbi and whoever elts unless this gets fixed like now

Figure 4. *Sample email from a mule complaining about receiving a fake check*

Further investigation revealed that with the help of money mules and certain accomplices in the United States, Soldier made over US$3.2 million in the past six months alone or around US$533,000 a month or US$17,000 a day.

Month	Earnings
November 2010	US$576,836.95
December 2010	US$809,758.96
January 2011	US$843,869.72
February 2011	US$719,379.42
March 2011	US$957,375.32
April 2011	US$763,142.43
May 2011	US$53,134.00

Table 1. *Summary of Soldier's earnings from November 2010–May 2011*

Soldier also conducted business transactions with another Russian cybercriminal that we are currently investigating based on bank data we collected during the course of our research. We also obtained the following simple money-laundering schema cybecriminals use to create fake checks:

```
Soldier (Russia) -> Viatcheslav (USA) -> GABRIELLA ->
Mules -> Soldier
```

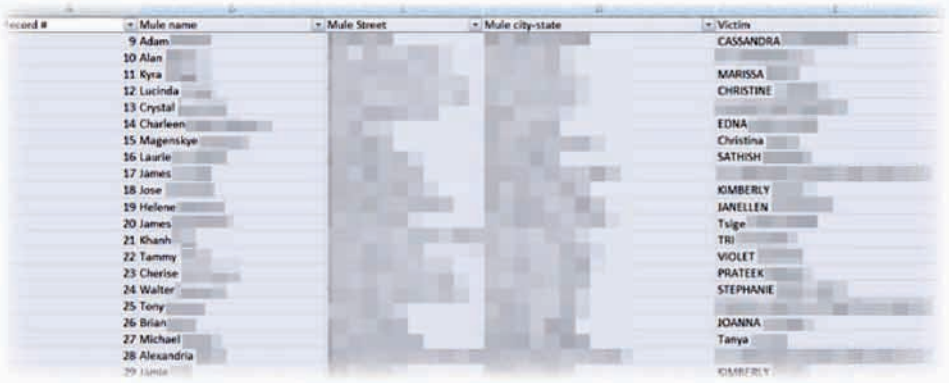


Figure 5. *List of Soldier's SpyEye botnet mules*

In the course of conducting research, we also found that Soldier had two accomplices in the United States with the following details:

```
Viatcheslav                    GABRIELLA
West Hollywood, CA             LOS ANGELES CA
```

What Is Soldier's C&C Server Infrastructure Like?

Soldier uses *SpyEye 1.3.41* whose gate panel is constructed on other servers that are not connected to the *CN1* and *SYN1* panels. We were able to identify some of his SpyEye servers, namely:

- *{BLOCKED}ker006.com/us6/bin/1310.exe*
- *{BLOCKED}ffic911.net*
- *{BLOCKED}1.net/se/load/* (has 25,000 bots)
- *{BLOCKED}1.net/se/logs/*
- *{BLOCKED}911.com*
- *{BLOCKED}ker004.com*
- *{BLOCKED}ffic911.net/traffic/bos/*
- *{BLOCKED}.{BLOCKED}.228.147/~site911/se/load/*
- *{BLOCKED}.{BLOCKED}.228.147/~site911/se/logs/*
- *{BLOCKED}.{BLOCKED}.228.147/~site911/se/kit/*
- *{BLOCKED}st003.net*
- *{BLOCKED}st003.com/~main/us6/bin*
- *{BLOCKED}.{BLOCKED}.243.232*
- *{BLOCKED}stse.com*
- *http://{BLOCKED}.{BLOCKED}.228.147/~main/us1/*
- *http://{BLOCKED}.{BLOCKED}.96.95/us1/*
- *http://{BLOCKED}.{BLOCKED}.99.250/us1/*
- *http://{BLOCKED}ker007.ru/us10/*

- *http://{BLOCKED}p4u.net/us2/*
- *http://{BLOCKED}ker911.com/us2/*
- *http://{BLOCKED}er001.com/us2/*
- *http://{BLOCKED}ker002.com/us2/*
- *http://{BLOCKED}er003.com/us2/*

Profiling Soldier's Victims

We compiled some information regarding Soldier's preferred targets and victims in the following sections.

BOTNET SIZE

Soldier's SpyEye botnet was able to compromise 25,394 systems (based on globally unique identifier [GUID]) or 82,999 unique IP addresses between April 19 and June 29, 2011. While nearly all of his victims were in the United States, a handful was spread out across 90 other countries as well.

GEOGRAPHIC SCOPE

We processed 24,536 IP addresses (one unique IP address per compromised system) and found that 97 percent were in the United States.

TOP COUNTRY TARGETS

Our research findings further support our belief that Soldier's SpyEye botnet mostly targets users in the United States.

Country	Infection Count
United States	23,739
United Kingdom	86
Brazil	74
Mexico	46
Thailand	41
Turkey	37
Saudi Arabia	33
India	31
Romania	27
Canada	26

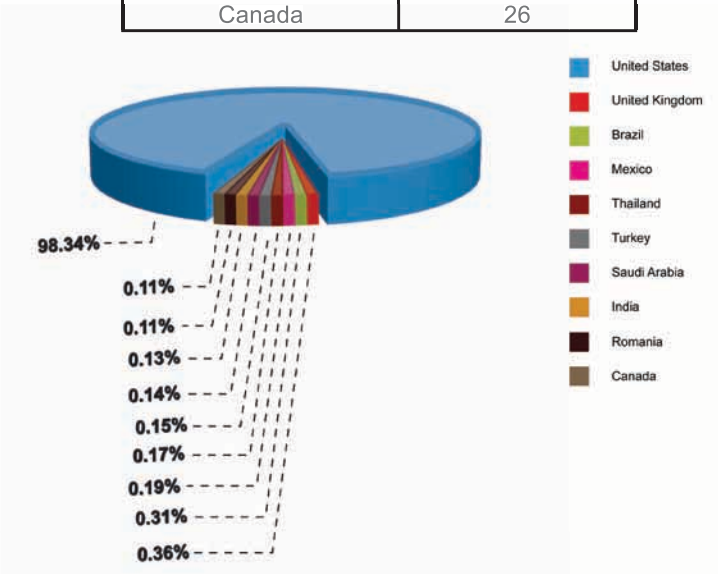


Figure 6. *Most targeted countries*

TOP OS TARGETS

This particular SpyEye botnet was built to specifically target *Windows*-based systems, the majority (57 percent of the total number of compromised systems) of which run *Windows XP*. As shown below, nearly 4,500 *Windows 7*-based systems have been compromised by the botnet as well despite certain security improvements in the said OS.

OS	Infection Count
Windows XP	14,141
Windows Vista	6,707
Windows 7	4,452
Windows Server 2003	63
Windows 2000	29
Others	2

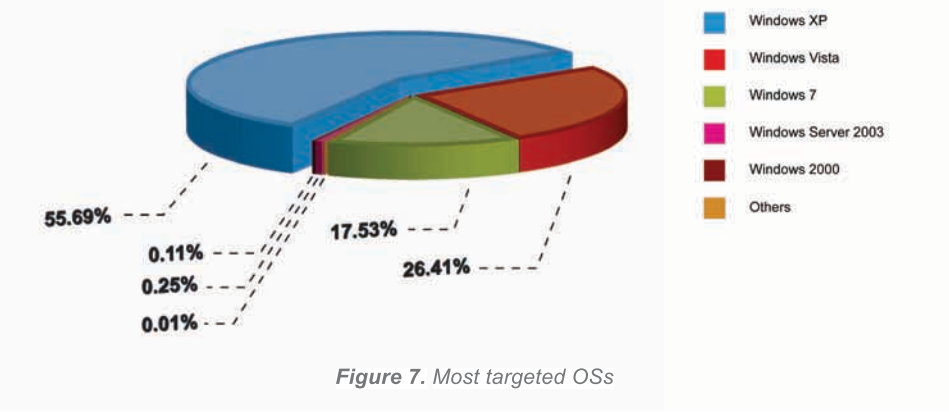


Figure 7. *Most targeted OSs*

Data Stolen by Soldier's SpyEye Botnet

DATA TYPES

Soldier's SpyEye botnet appears to target the customers of specific banks. To steal information related to its targets, a particular code is injected, client side, into online banking pages, aiding in the facilitation of fraud. This botnet extracts user credentials for a variety of accounts in popular banks in the United States.

Please note that this fraud was made possible by compromising users' systems with the injection of code only in pages they were viewing.

Bank	Infection Count
Chase	1,499
Wells Fargo	770
Bank of America	1,283

Table 2. *Most affected online banking users*

Even though SpyEye is better known for stealing bank account credentials, it is also capable of stealing other personal credentials. In fact, we processed the data we gathered about this particular SpyEye botnet for other well-known services and found that it also stole credentials related to sites like *Facebook.* Note, however, that the list below is not exhaustive.

Service	Infection Count
Facebook	21,819
Yahoo!	9,987
Google	8,078
Live	4,507
POP3	2,878
eBay	1,199
Amazon	866
Twitter	649
FTP	473
PayPal	193
Skype	138

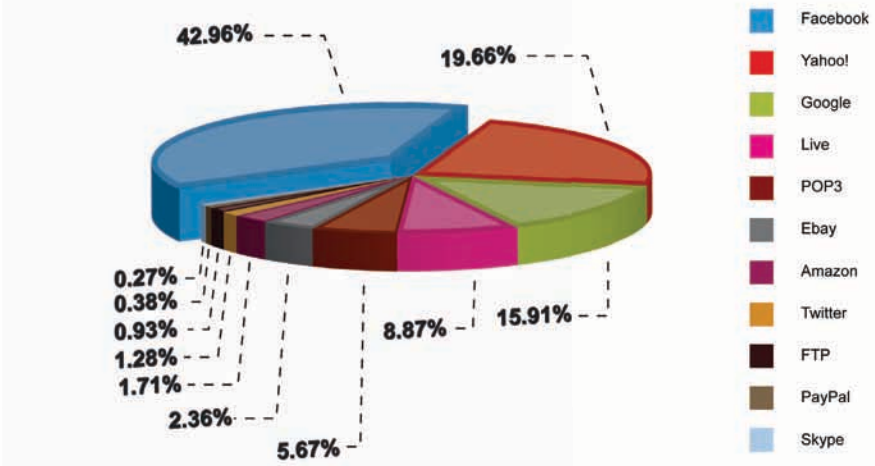


Figure 8. *Most targeted services*

NOTABLE COMPROMISED VICTIMS

Based on the victims' IP addresses recorded by Soldier's SpyEye C&C server, we were able to determine which networks the said addresses were assigned to. Using this information, we were also able to determine some of the victims' identities as well as the industries they belonged to. Some of the victims we identified belonged to the following industries:

- Government (local, federal)
- Military
- Education and research
- Banking
- Transportation (air)
- Manufacturing (automobile)
- Communications and media
- ICT

More on SpyEye

What Is SpyEye and How Does It Work?

Since its inception, SpyEye has been exhibiting routines similar to those of ZeuS, particularly in relation to information, financial, and identity theft. Like ZeuS, SpyEye makes use of a configuration file to further its criminal agenda, which comprises monitoring banking or other target sites with the goal of stealing data, which is then sent to a remote server managed and controlled by a bot master. SpyEye also utilizes rootkit technology to hide malicious files and processes from affected users, allowing its variants to avoid detection and possible removal.

In the first quarter of 2010, there were rumors of a possible bot war between ZeuS and SpyEye. This stemmed from SpyEye's ability to terminate running ZeuS processes in order to gain "sole pOwnership" of infected systems.

Since then, we have been monitoring various SpyEye developments. We have also documented some of the key developments and enhancements that have been made to the crimeware toolkit, leading to the much-talked-about ZeuS-SpyEye merger. SpyEye has since begun taking ZeuS's place as the criminals' favorite crimeware toolkit. More recent modifications to the toolkit raises expectations that it won't be long before huge cybercrime campaigns using SpyEye are identified.

SpyEye in the Cybercrime Underground

It is believed that SpyEye was originally written by a cybercriminal who goes by handles like gribodemon and harderman. At some point, gribodemon began outsourcing some of his code development to other developers. He even started paying other people to write certain sections of the said code before putting all of the pieces together to create SpyEye. As such, gribodemon became more of a project manager than the actual SpyEye coder.

The basic SpyEye toolkit as well as the additional components' prices are listed below.

Component	Price
Basic toolkit	US$2,000
Firefox Web injection plug-in	US$2,000
Anti-rapport plug-in	US$500
SOCKS 5 proxy plug-in	US$1,000
Remote desktop (RDP) functionality plug-in	US$3,000
FTP back-connect plug-in	US$300
Firefox certificate grabber plug-in	US$300
Credit card credential grabber plug-in	US$200
Opera and *Chrome* form grabber plug-in	US$1,000
Complete toolkit with all kinds of plug-in	US$8,000–10,000 **May be discounted based on how close the buyer is to the seller)*

Table 3. *SpyEye toolkit and component price list as of July 2011*

An individual who goes by the handle Xylitol and the so-called Reverse Engineers Dream Crew (RED Crew) recently released a SpyEye loader, which allows a person to use the SpyEye builder without a serial key. When cybercriminals buy SpyEye, they receive the loader that is locked via software protection. After running the builder, they are shown their hardware ID (HWID), which they then send to gribodemon so he can give them a corresponding serial key. This stopped them from sharing the builder they bought with other cybercriminals.

The new loader that RED Crew coded was a means to get around the limitations that gribodemon set. This way, everyone who downloads the loader can use it to build their own SpyEye botnets even without buying a copy of the toolkit.

Tracking SpyEye-Related Activities

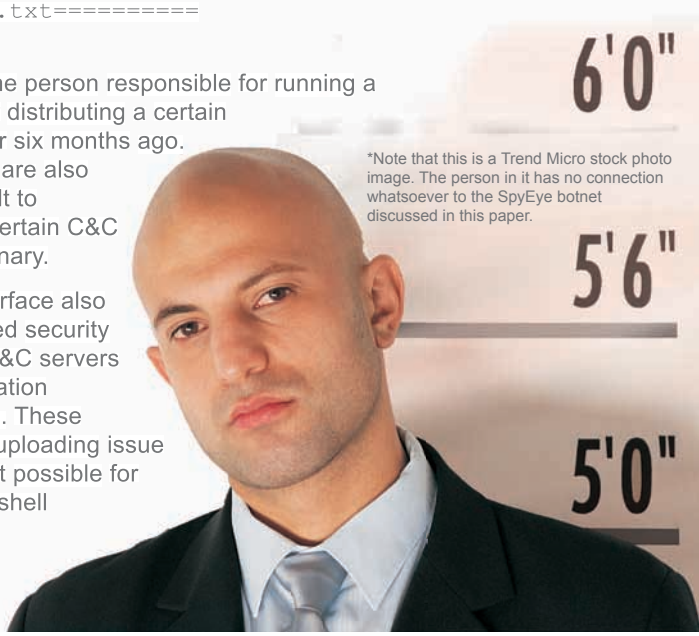
A few online tools and resources to track SpyEye-related activities currently exist, including the *SpyEye Tracker (SET)* site wherein a list of running SpyEye command-and-control (C&C) servers is found. This site aids security experts with their investigations by identifying known SpyEye domains, when these were added, and other useful data.

Examining the binaries themselves along with their configuration files is also helpful. Security analysts can decode encrypted configuration files in order to see the list of C&C domains or IP addresses and drop zones. This may even help them obtain the user name of the bad guy who is responsible for spreading a certain SpyEye binary. (See a decrypted sample SpyEye configuration file below.)

```
==========Spyeye Version: 10341==========
==========collectors.txt==========
85.17.xxx.xxx:99
==========config.dat==========
CC9B3D8C
==========customconnector.dll.cfg==========
http://94.75.xxx.xxx/~main/xxx/gate.php;50
http://78.159.xxx.xxx/xxx/gate.php;50
http://78.159.xxx.xxx/xxx/gate.php;50
http://ipxxx.ru/xxx/gate.php;50
==========socks5.dll.cfg==========
%BOTNAME%;85.17.xxx.xxx;4000;3000;1
==========webinjects.txt==========
```

Determining the user name of the person responsible for running a particular C&C server and/or for distributing a certain SpyEye binary used to be easier six months ago. Now, the bad guys' user names are also encrypted, making it very difficult to determine who actually runs a certain C&C server or distributes a certain binary.

Various bugs in the SpyEye interface also existed in the past, which allowed security researchers to access certain C&C servers and to circumvent the authentication mechanisms bot masters put up. These vulnerabilities, along with a file-uploading issue on SpyEye's *CN1* panel, made it possible for unauthorized users to upload a shell and/or to steal bots from certain SpyEye bot masters.



*Note that this is a Trend Micro stock photo image. The person in it has no connection whatsoever to the SpyEye botnet discussed in this paper.

SpyEye's Future

Xylitol and the RED Crew's recent release of the bot loader will surely push gribodemon to produce a new SpyEye version in order to get his customer base back on track. He is likely to follow in the footsteps of ZeuS author, monstr.

When users cracked ZeuS's code in a similar manner, monstr quickly released *ZeuS v. 1.4,* which has been renamed to *v. 2.0.* Monstr made sure that he included several new features so his customers would upgrade to his latest creation.

We believe gribodemon will react in much the same manner. He will come up with a new SpyEye version with innovative features to regain his customers' confidence and patronage. In effect, SpyEye is set to become even bigger and is showing no signs of dying in the future.

Conclusion

In the single but huge SpyEye cybercrime ring featured in this paper, we attempted to show how many users can be exposed to this threat and how damaging successful compromises can become. Moreover, we showed just how profitable a single SpyEye botnet can be for cybercriminals.

The findings in this paper support what we have been saying about SpyEye since early last year, that the toolkit will be one of the most sought-after crimeware tools to instigate more and more nefarious data-stealing campaigns.

Though the targets specified in this paper are generally located in the United States, including top organizations, institutions, and companies, other cybercriminals who use or plan to use SpyEye for various purposes may target other demographics, companies, and institutions in other countries. The threats that SpyEye poses can and is likely to have a global reach. Trend Micro will carry on tracking any development related to SpyEye so we can continue to protect users wherever and whenever they are.

With this in mind, users are advised to keep their security solutions up to date. Trend Micro product users are already protected from this threat via the Trend Micro™ Smart Protection Network™ infrastructure, which blocks access to related malicious sites and domains as well as detects and deletes SpyEye binaries and other components used in cybercriminal campaigns.

Non-Trend Micro product users can stay protected by using *Web Protection Add-On*, a free tool specifically designed to block user access to potentially malicious sites in real time.

References

- Kevin Stevens. (October 3, 2010). *TrendLabs Malware Blog.* "The SpyEye Interface, Part 1: *CN1."* http://blog.trendmicro.com/the-spyeye-interface-part-1-cn-1/ (Retrieved September 2011).
- Kevin Stevens. (October 15, 2010). *TrendLabs Malware Blog.* "The SpyEye Interface, Part 2: *SYN1."* http://blog.trendmicro.com/the-spyeye-interface-part-2-syn-1/ (Retrieved September 2011).
- Kevin Stevens. (November 25, 2010). *TrendLabs Malware Blog.* "ZeuS-SpyEye Merger in Progress." http://blog.trendmicro.com/zeus-spyeye-merger-in-progress/ (Retrieved September 2011).
- Loucif Kharouni. (January 24, 2011). *TrendLabs Malware Blog.* "*SpyEye/ZeuS Toolkit v1.3.05 Beta,* Part 1." http://blog.trendmicro.com/spyeyezeus-toolkit-v1-3-05-beta/ (Retrieved September 2011).
- Loucif Kharouni. (February 22, 2011). *TrendLabs Malware Blog. "SpyEye/ZeuS Toolkit v1.3.05 Beta,* Part 2." http://blog.trendmicro.com/spyeyezeus-toolkit-v1-3-05-beta-part-2/ (Retrieved September 2011).
- Loucif Kharouni. (June 10, 2011). *TrendLabs Malware Blog. "SpyEye 1.3.4.x* Comes with Noteworthy Modifications (Part 1)." http://blog.trendmicro.com/spyeye-1-3-4-x-comes-with-noteworthy-modifications/ (Retrieved September 2011).
- Loucif Kharouni. (June 13, 2011). *TrendLabs Malware Blog. "SpyEye 1.3.4.x* Comes with Noteworthy Modifications (Part 2)." http://blog.trendmicro.com/spyeye-1-3-4-x-comes-with-noteworthy-modifications-part-2/ (Retrieved September 2011).
- Robert McMillan. (February 9, 2010). *Computerworld.* "New Russian Botnet Tries to Kill Rival." http://www.computerworld.com/s/article/9154618/New_Russian_botnet_tries_to_kill_rival (Retrieved September 2011).
- Roland Dela Paz. (February 16, 2010). *TrendLabs Malware Blog.* "Keeping an Eye on EYEBOT and a Possible Bot War." http://blog.trendmicro.com/keeping-an-eye-on-the-eyebot-and-a-possible-bot-war/ (Retrieved September 2011).
- Trend Micro Threat Research Team. (March 2010). *TrendWatch.* "ZeuS: A Persistent Criminal Enterprise." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/zeusapersistentcriminalenterprise.pdf (Retrieved September 2011).

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware, and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our website at www.trendmicro.com.

TRENDLABS℠

TrendLabs is Trend Micro's global network of research, development, and support centers committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery.