ZeuS: A Persistent Criminal Enterprise

Trend Micro, Incorporated

Threat Research Team

A Trend Micro Research Paper | March 2010

CONTENTS

INTRODUCTION

The ZeuS botnet is a short term for networks of compromised computers that use ZeuS/ZBOT Trojans in botnet-related operations.

After the Kneber botnet incident, the ZeuS botnet was suddenly thrown into the limelight of notorious cybercriminal campaigns that the general public is currently talking about.

Figure 1. *News on the most recent ZeuS-related attack*

ZeuS, however, has been in the wild for years and even though it has gone through changes and improvements, it still remains one of the most effective and efficient crimeware that criminals are using.

This research paper attempts to shed light on what ZeuS really is. It presents some basic facts that the general public needs to know and possibly who or what possible criminal organizations are behind the ZeuS botnet.

ZeuS is a crimeware kit designed to steal users' online banking credentials, among other things.

WHAT IS ZEUS?

ZeuS is primarily a crimeware kit designed to steal users' online banking login credentials, among other things. It is the handiwork of Eastern European organized criminals that has now entered the underground cybercriminal market as a commodity.

ZeuS is known by many names—ZBOT due to its botnet capabilities, WSNPoem, PRG, and others—but its use has been particularly criminal. In short, ZeuS is two things:

- From a technical perspective, it is a crimeware tool primarily used to steal money.
- From another perspective, it signals a new wave in online criminal business enterprise wherein many different organizations cooperate with one another to perpetrate outright online theft and fraud.

The principal perpetrators behind the ZeuS botnet are in Eastern Europe, particularly in the Ukraine and Russia. However, the recent availability of the *ZeuS Builder* toolkit in the open market has muddied the waters on attributing crimes to any one individual or group. That said, there is definitively a difference between "professional" criminals and "amateurs." The professional, organized crime syndicates also have other business connections, which they leverage to perpetrate their crimes and move their money.

TREND MICRO

SOME TECHNICAL FACTS

The ZeuS botnet has three basic components:

- ZeuS Trojan
- ZeuS configuration file
- ZeuS drop zone where stolen credentials are sent

The technical aspect of ZeuS is not really not that complicated, at least from a functional perspective. It does use a complex encryption technique but explaining its functionality is pretty simple. It has the three components:

1. ZeuS Trojan
2. ZeuS configuration file (*config*)
3. ZeuS drop zone where stolen credentials are sent

The ZeuS botnet uses several delivery methods in the first stage—the Trojan.

Once the ZeuS Trojan is executed, it downloads its configuration file from a predetermined location then waits for the victim to log in to a particular target that its *config* file has defined, which usually comprises a selection of banks, their login URLs, and the like.

Unlike traditional keyloggers, ZeuS Trojans are "men-in-the-browser" agents that grab variables from a browser session such as an online banking session. This makes ZeuS especially dangerous because it also has the ability to inject additional form fields into a legitimate Web session. Injecting these additional fields can fraudulently urge victims to surrender more information than they would normally be required to in a session, for instance, with their banks.

Some ZeuS variants also contain a nasty feature called "JabberZeuS," which immediately relays victims' login credentials to cybercriminals in real-time via an instant messenger (IM). This allows cybercriminals to bypass multifactor authentication schemes to log in to victims' accounts and to wire money to third parties, virtually piggybacking on the victims' sessions.

This is where the ZeuS botnet's real power lies, the core nature of which is wholesale theft.

ZeuS Components

ZeuS Builder is responsible for creating the binary file used to make the botnet as well as the configuration file that stores all of the botnet's settings.

ZeuS Builder is one of the key parts of the ZeuS toolkit. It is responsible for creating the binary file used to make the botnet as well as the configuration file that stores all of the botnet's settings.

When a criminal first runs *ZeuS Builder,* they are presented with a simple screen that shows information about the ZeuS version they purchased. Interestingly, however, ZeuS also checks if the local system is currently already infected by the ZeuS malware, which gives the user an opportunity to remove it.

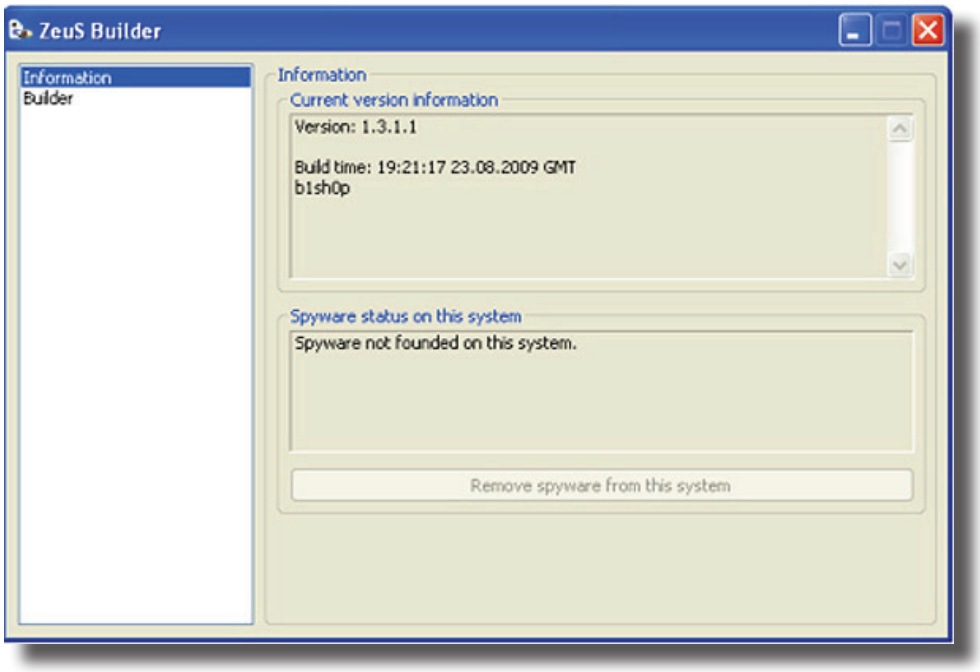

Figure 2. *Standard* ZeuS Builder

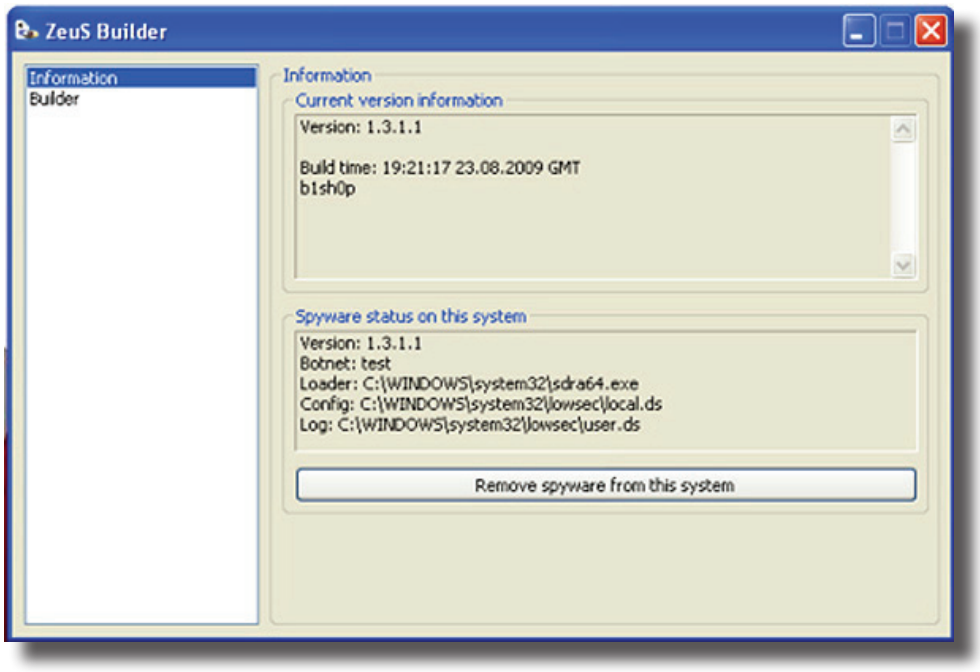

Figure 3. ZeuS Builder *on an infected system (note the "Remove Spyware" option)*

The ZeuS config file contains settings such as the botnet's name, how often it will send stolen information back, the server the malware should connect to, and others.

All ZeuS botnets are built based on a highly versatile configuration file. This file contains settings such as the botnet's name, how often it will send stolen information back, and the server the malware should connect to. More importantly, however, it contains a list of banks for ZeuS to target. ZeuS has the ability not only to gather all the banking login credentials and passwords users enter but also to directly inject extra form components into users' banking website view as mentioned earlier.

ZeuS Builder then takes this configuration file and encrypts it. All ZeuS bots regularly dial home and download the encrypted configuration file to see if they have already received new orders, which, of course, makes security researchers' jobs more difficult. Receiving a copy of an encrypted configuration file does not tell researchers anything unless we can also extract the encryption key from the corresponding ZeuS binary.

Figure 4. *Portion of the ZeuS configuration file that shows some of its target banks*

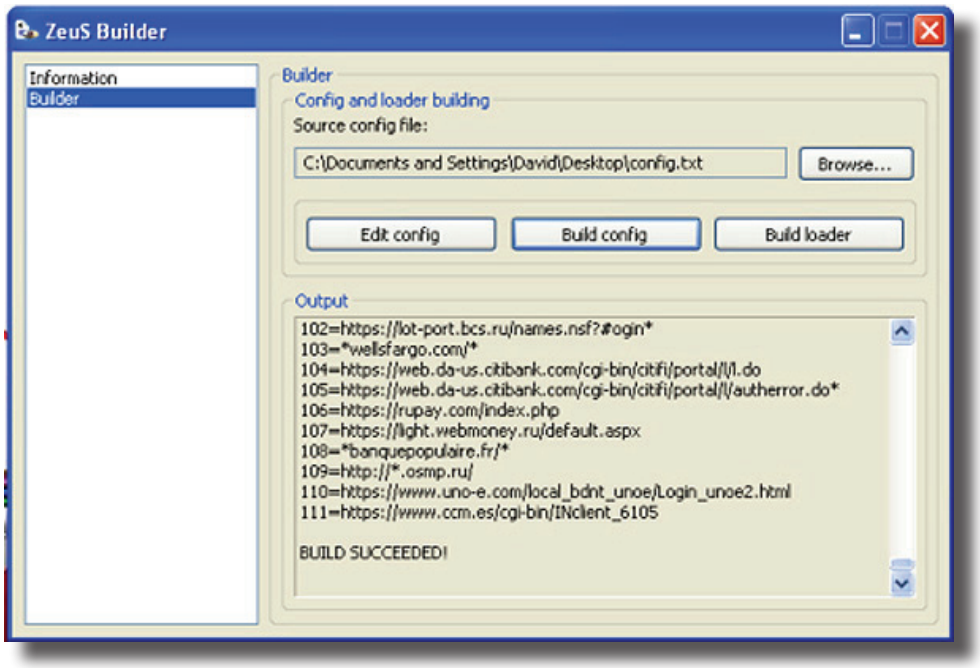

Figure 5. ZeuS Builder *that has successfully encrypted the configuration file*

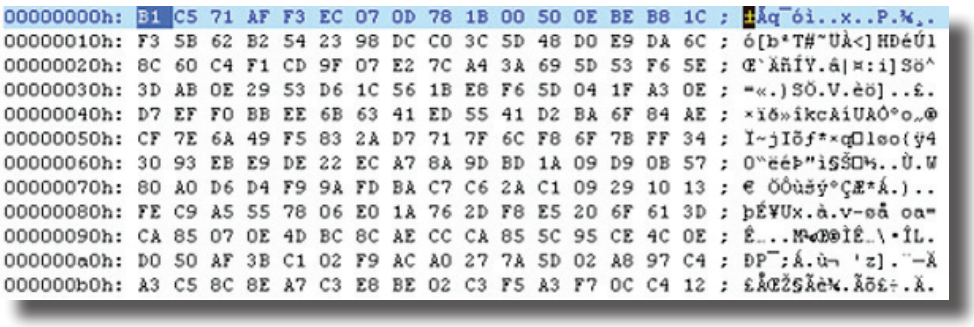

Figure 6. *Same ZeuS configuration file but encrypted*

Criminals who use ZeuS now take both the encrypted configuration file and the ZeuS binary, which they created with *ZeuS Builder,* and place them on a Web server. ZeuS allows either each component to be placed on a separate Web server or all of its components on a single Web server. Once a user's system is infected by the binary, it will apply the latest version of its configuration settings and begin stealing the user's personally identifiable information (PII). After only a few mouse clicks, cybercriminals can get access to a fully functional banking Trojan or botnet.

The ZeuS Server, like ZeuS Builder, is also remarkably simple to configure.

The *ZeuS Server* is also remarkably simple to configure. A cybercriminal simply drops the Web server files onto his/her machine, looks for the install page, and fills in some very basic settings.

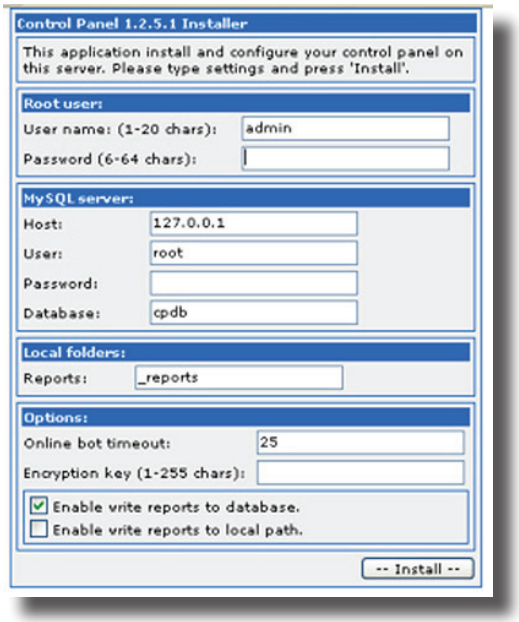

Figure 7. ZeuS Server *installation page*

Once set up, this server will receive all of the data ZeuS bots steal. It also has many other features such as keeping tabs on how many infected users there are (based on OS, geographical location, and others) and running scripts on infected machines, just to name a few.

TREND MICRO

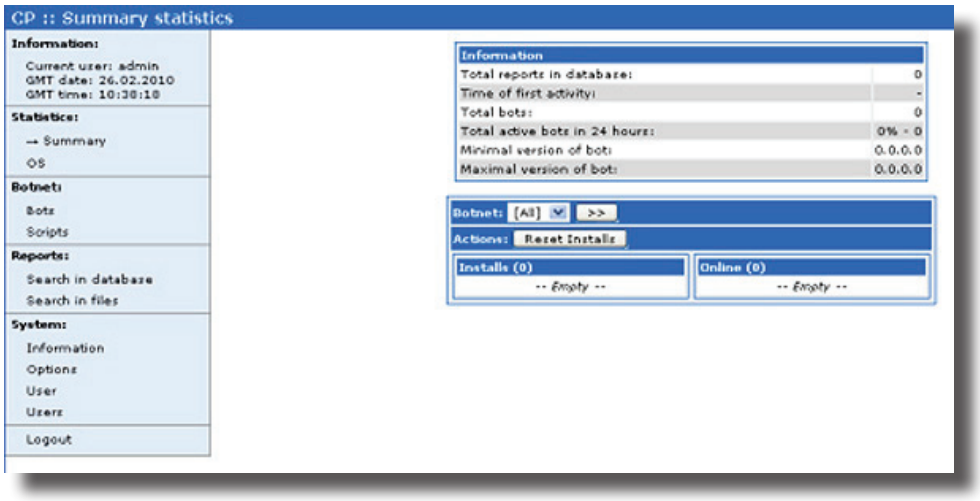

Figure 8. ZeuS Server *main page*

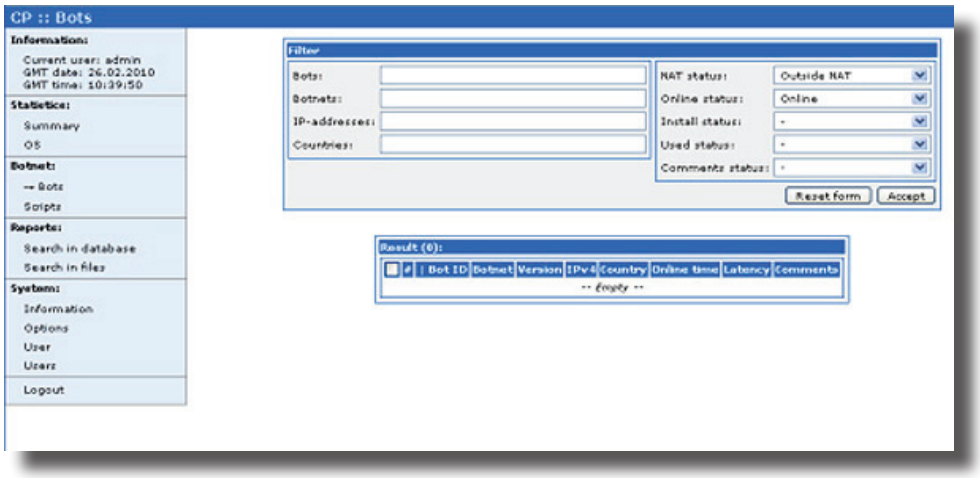

Figure 9. *Some of the additional features of the* ZeuS Server

ZeuS Builder and the ZeuS Server have made the malware toolkit the de facto standard for cybercrime, as they allow even someone with minimal technical knowledge to configure and set up a fully functional and highly professional botnet in less than five minutes.

ZeuS Builder and the *ZeuS Server* are exactly why this particular malware toolkit has become the de facto standard for cybercrime. They allow even someone with minimal technical knowledge to configure and set up a fully functional and highly professional botnet in less than five minutes. The ease by which ZeuS can be used is its major selling point. It is also why we do not envisage it will go away anytime soon.

SOME ZEUS STATISTICS

The ZeuS Trojan has been around for several years now. However, it has only been rampantly used in the past year. In the past four months we have seen an average of around 300 unique samples per day. In fact, there were more than 13,000 unique ZeuS samples in January 2010 alone.

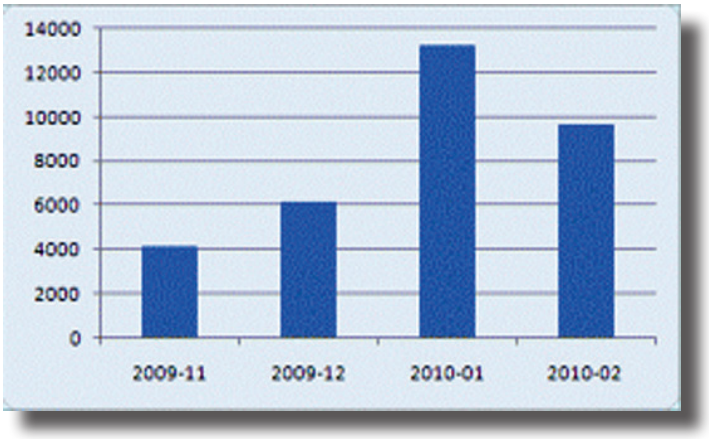

Figure 10. *ZeuS samples from November 2009 to February 2010*

The following are some pertinent ZeuS-related data:

- 18,985 ZeuS binaries in the past month
- 4,582 ZeuS binaries in the past week
- 977 ZeuS binaries in one day

The following are some other pertinent data from *VirusTotal:*

- **Number of new ZeuS binaries in the past month:** 18,985
- **Number of new ZeuS binaries seen in the past week:** 4,582
- **Number of new ZeuS binaries seen in one day:** 977

ZEUS INFECTION CHAIN

The following figure shows how a typical ZeuS infection takes place.

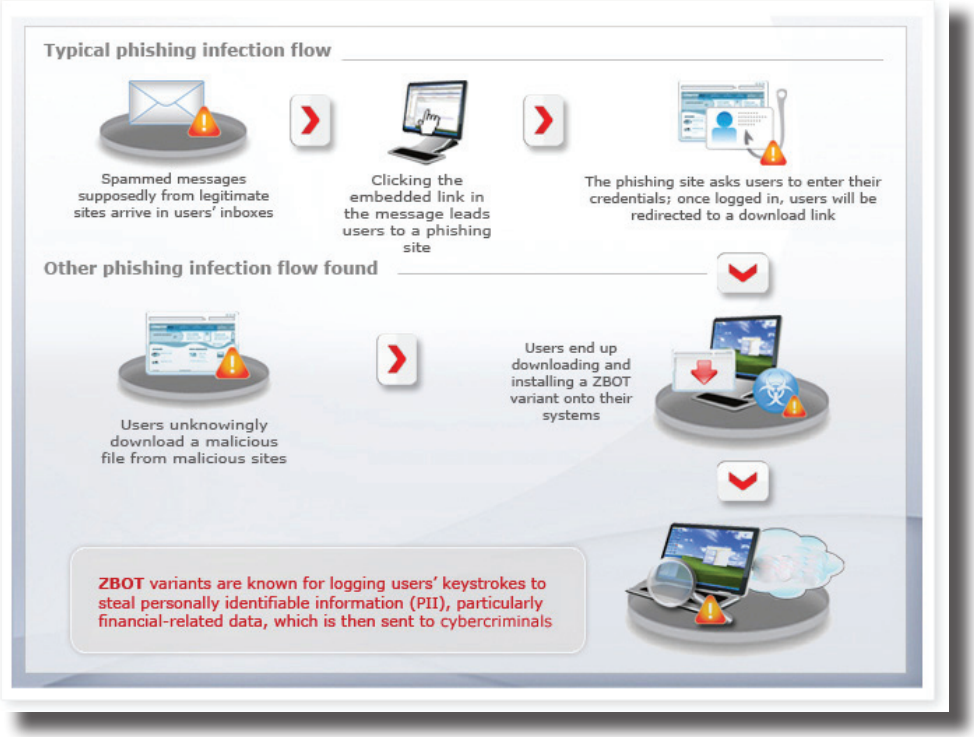

Figure 11. *Typical ZeuS infection diagram*

ZEUS-BREDOLAB CONNECTIONS

According to our research, BREDOLAB and ZeuS are individual tools that are freely available in the cybercriminal underground. Their uses complement each other, which is why we very often see them together.

ZeuS specializes in stealing information from infected systems while BREDOLAB is a software that enables cybercriminal organizations to deliver any kind of software to its victims.

ZeuS specializes in stealing information from infected systems. BREDOLAB, on the other hand, is a software that enables cybercriminal organizations to deliver any kind of software to its victims. Once a user's machine is infected by BREDOLAB, it will receive regular malware updates the same way it receives software updates from the user's security vendor.

This delivery method has proven to be very convenient for cybercriminals. As such, they usually create a BREDOLAB botnet that updates each ZeuS-infected machine with the latest information stealer. In other words, these infections go hand in hand.

Furthermore, BREDOLAB infections use a second payload that accompanies ZeuS—FAKEAV. Since spreading FAKEAV increases cybercriminals' chances of getting big payouts, they often include this scamming software in their BREDOLAB update packages.

The key fact to keep in mind is that even though their makers may not be connected, the botnet controllers use all of these blackhat tools in conjunction with one another to maximize profits. FAKEAV acts as a con man posing as a policeman, ZeuS acts as a spy that will allow the con man to use the stolen data for identity theft, and BREDOLAB acts as the driver that brought them to and took them away from your home.

A recent sample ZeuS-BREDOLAB campaign was the massive spam run in 2009 that featured email messages that spoofed UPS or FedEx. The email messages purported to come from legitimate couriers and notified potential victims of new packages coming their way and convincing them to open the attached invoice. Opening the fake invoice, of course, executes a BREDOLAB variant that infects victims' systems. This then proceeds to the installation of both ZeuS and FAKEAV variants at once and is a typical example of a multipronged attack that a botnet creator will try to pull off.

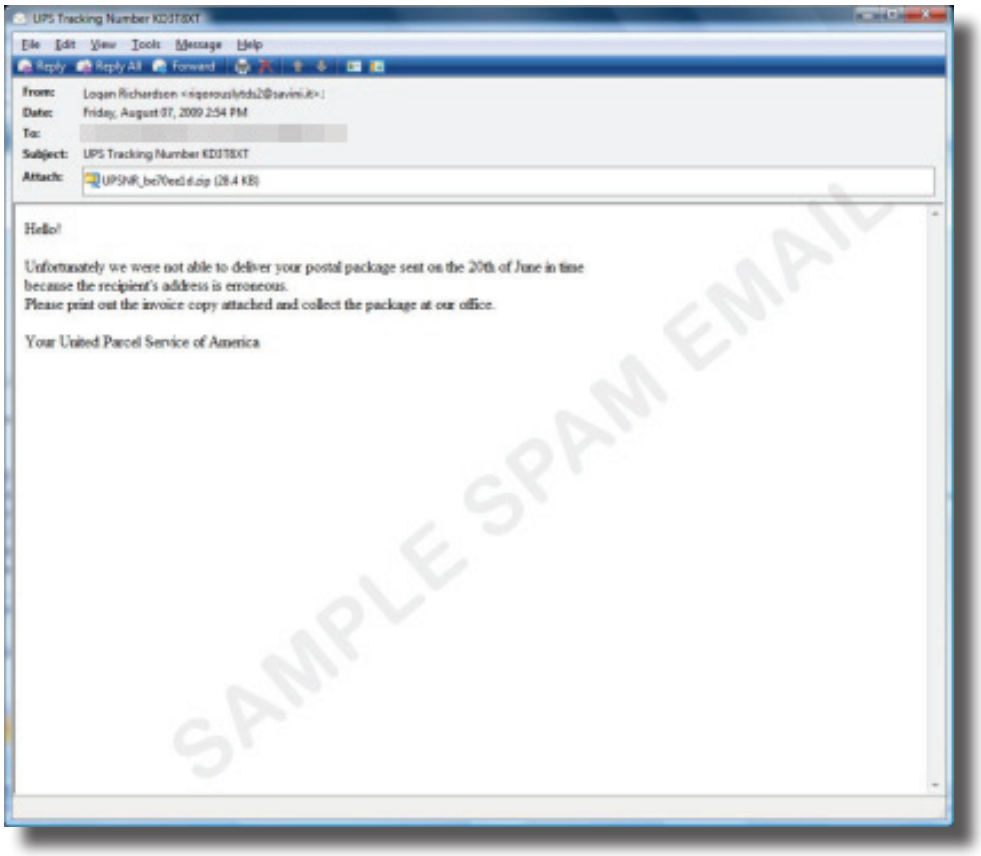

Figure 12. *Sample spam from a ZeuS-BREDOLAB-related UPS campaign*

TREND MICRO

LATEST DEVELOPMENTS

The Avalanche fast-flux botnet sent spammed messages linked to various ZeuS variants en masse.

For the greater part of last year, ZeuS variants were also distributed via the Avalanche botnet, which sent spammed messages en masse. The spam runs imitated several popular Web 2.0 brands like *Facebook* and *MySpace*. The cybercriminals behind the operations even tried to copy email messages and websites of U.S. government institutions like the Federal Deposit Insurance Corporation (FDIC), the Centers for Disease Control and Prevention (CDC), the Social Security Administration (SSA), and the Internal Revenue Service (IRS).

Of course, the links embedded within the spammed messages point to websites that push the ZeuS binary.

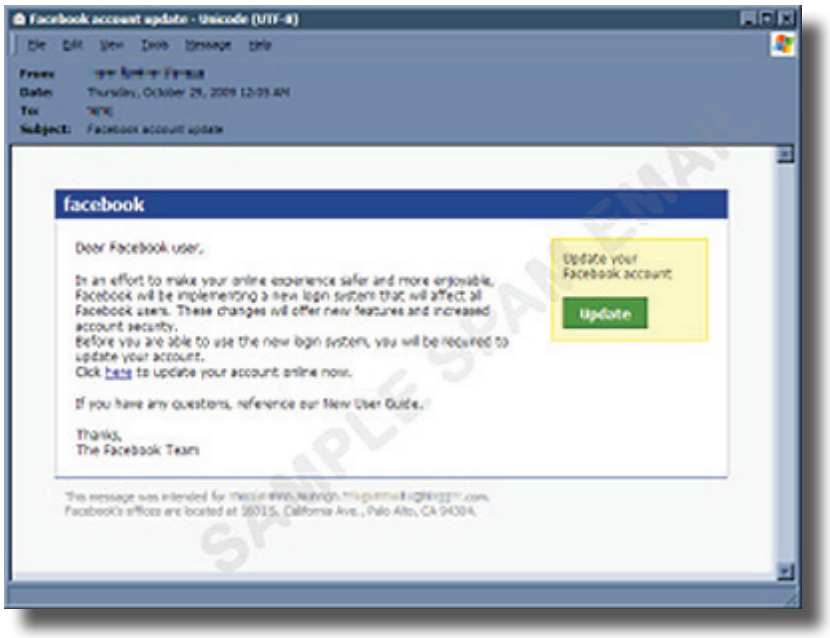

Figure 13. *ZeuS-related* Facebook *spam*

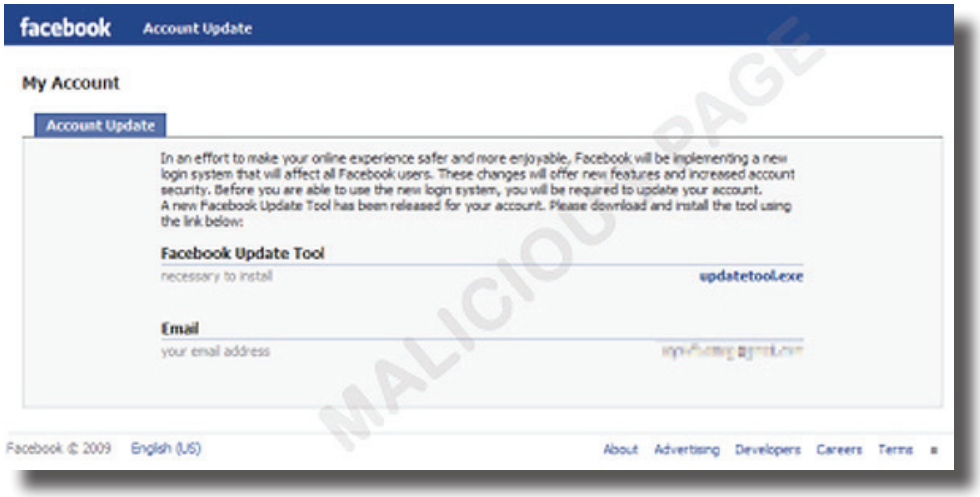

Figure 14. *Bogus* Facebook *Web page pushing ZeuS via the Avalanche botnet*

A significant feature that was recently added to the current ZeuS versions is the "Jabber" functionality. *Jabber* is an open source instant messaging protocol, popularly used by *Google Talk.* This *Jabber*-equipped ZeuS version dubbed "JabberZeuS."

JabberZeuS is a particular ZeuS variant wherein the credentials stolen during a banking session are relayed in real-time to the ZeuS botmaster via instant messages so he/she can immediately log in to the same account undetected using the same credentials (including any multifactor authentication credential) as the victim. This allows cybercriminals to defeat multifactor authentication schemes by replaying them in real-time and to obtain access to online bank accounts so they can wire money to pre-arranged money mule accounts.

JabberZeuS is a ZeuS variant wherein the credentials stolen during a banking session are relayed in real-time to the ZeuS botmaster via instant messages so he/she can immediately log in to the same account undetected using the same credentials as the victim.

Meanwhile, *SpyEye v1.0.2,* a new bot that will, some industry experts say, overtake ZeuS in the future emerged. It has even come to the point where it has been labeled a "ZeuS killer" since SpyEye knows how to hijack ZeuS logs from infected nodes.

WHO IS BEHIND ZEUS?

The ZeuS Cybercriminal Underground: Eastern European Organized Crime

The ZeuS crimeware kit is only a part of the equation. There is an entire organized cybercriminal organization that thrives from this methodology.

In fact, the top bulletproof-hosted ZeuS domains reside in Russia and the Ukraine, as indicated in the figure from the *ZeuS Tracker* website below.

Top ten worst ZeuS C&Cs (by files online)

# of files online	ZeuS C&C	level	SBL	countr
21		4	SBL82408	UA
19		4	SBL82410	UA
17		4	SBL82408	UA
16		4	SBL82408	UA
15		1	SBL81900	RU
15		1	SBL81900	RU
10		4	Not listed	UA
10		4	Not listed	UA
9		1	SBL85946	CN
8		1	Not listed	CN

Figure 15. *Top bulletproof-hosted ZeuS domains*

Note that the data in the figure above only accounts for standalone ZeuS hosts and does not include compromised consumer residential broadband clients that are part of the Avalanche fast-flux network that hosts ZeuS Trojans.

Some security experts also believe that the sites located in the China are actually compromised hosts controlled by cybercriminals based in Russia, the Ukraine, or both.

ZeuS has become the most popular crimeware kit in the criminal underground for wholesale monetary theft.

ZeuS has become the most popular crimeware kit in the criminal underground for wholesale monetary theft. In fact, the sophistication cybercriminal operations use can be seen in their ability to also recruit money mules to move their stolen money around through bogus work-from-home scams. The cybercriminals know that given the current economic situation in the United States—with millions of people out of work—they will have a high success rate in recruiting unwitting accomplices.

Unwitting work-from-home recruits are instructed to provide bank account information, which the cybercriminals use to access compromised online bank accounts and to wire money amounting to less than US$10,000 to money mules, indicating that they are fully aware of banking alert limits. The money mules then wire the money back to Eastern Europe via Western Union or MoneyGram.

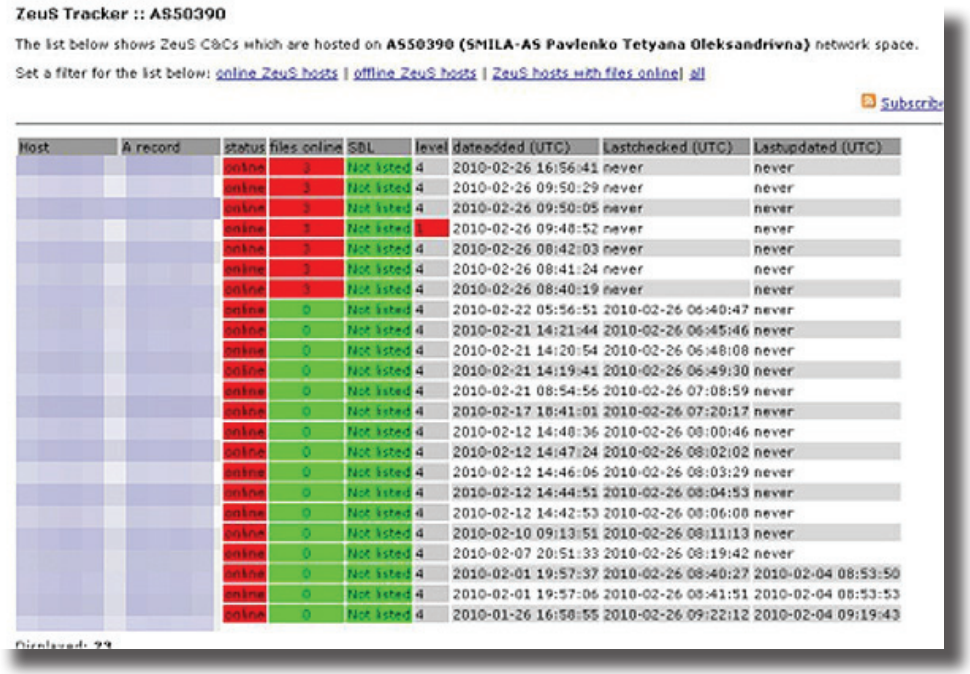

Figure 16. *Some other autonomous system numbers (ASNs) seen in relation to ZeuS campaigns*

Other ZeuS Underground Tidbits

Crypting and QA Business

Crypting service providers offer ZeuS perpetrators binary crypting services using private and customized cryptors.

Crypting service providers can be seen in the Russian underground that offer ZeuS binary crypting services using private and customized cryptors. The same people also offer services that can check the binaries and can evaluate the domain names ZeuS uses as command and control (C&C) servers. CryptService.net, for instance, offers ZeuS perpetrators to check the domain names and binaries on a daily basis.

To use it, one only has to register for the service, upload the binaries, and inform the provider what domain names he/she uses. In case the domain names and binaries are already blacklisted, the service provider immediately sends him/her a notification. This service not only checks via its own multi-antivirus scanning service but also via *ZeuS Tracker,* among other blacklisting services.

The following list the current ZeuS-related service prices:

- 10 WMZ per country for injecting configuration files filtered by country
- 5+ WMZ for ZeuS balance grabbers
- 5+ WMZ for manual crypting services
- 10 WMZ for ZeuS plus pinch crypting services
- 12 WMZ for ZeuS log parsers

Partnerka Distribution

Some pay-per-install (PPI) partnerka also offer ZeuS binary installers. Nowadays, PPI partnerka that are taking ZeuS binaries for installation are not really happy due to the good antivirus detection rate. The last PPI partnerka that we saw drop ZeuS services include:

- Jincash.ru
- Admitad.com

Current ZeuS Prices

- **ZeuS injects configuration files filtered by country:** 10 WMZ per country
- **ZeuS balance grabbers:** 5 WMZ or higher
- **ZeuS manual crypting service:** 5 WMZ or higher
- **ZeuS plus pinch crypting service:** 10 WMZ
- **ZeuS log parser:** 12 WMZ

ZeuS Log Reselling

We have also seen service providers buy, resell, and parse ZeuS log files to obtain access to users' credentials for social networks, mail services, and the like. Some of the logs are even shared with other members the underground community. Log reselling services can cost up to US$0.5 for every 1MB–1GB worth of ZeuS file logs that contain stolen data.

FINANCIAL LOSSES

In a series of investigative reports, Brian Krebs, formerly of the *Washington Post,* documented several incidents involving money stolen from the online accounts of small and medium-sized businesses (SMBs) in the United States. These incidents involved ZeuS as the malware that enabled the cybercriminals to hijack victims' bank accounts.

Figure 17. *News of an SMB going bankrupt due to an e-banking loss*

Hundreds of thousands of dollars are stolen from businesses by cybercriminals who control affected businesses' machines. These result in real monetary losses and they all start with a ZeuS infection.

Figure 18. *News of an entire country losing millions to cybercriminals*

CONCLUSION

As mentioned earlier in this paper, ZeuS has been entrenched in the cybercriminal business for a long time now and has continuously evolved and improved. Given the vast number of toolkit versions readily available in the underground, the features ZeuS possesses to thwart both antivirus and other security solutions, as well as efforts by the security industry, ZeuS will continue to be used by cybercriminals to steal personal information and even people's identities.

ZeuS, moving forward, has, is, and will still be one of the most notorious security threats to Internet users and will continue to effect hazards, especially with regard to users' online financial dealings.

Trend Micro will continue to fight back. In the past six months alone, we have prevented around 9 million ZeuS infections. However, the battle against ZeuS is not yet over.

Learn more about how to protect your enterprise from bot infections with Trend Micro Threat Management Services or sign up for a free Security Threat Assessment with Threat Management Services.

Just visit www.trendmicro.com/tms or call us at 877-21-TREND.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com