ZeuS Banking Trojan Report

secureworks.com/research/zeus

Wednesday, March 10, 2010

- **Author:** Kevin Stevens and Don Jackson, Security Researchers
  SecureWorks Counter Threat Unit SM (CTU)
- **Date:** March 10, 2010

Introduction

This Threat Analysis from the SecureWorks CTUSM provides a brief overview of the current version of ZeuS and its modules, along with the market pricing. We will then see how ZeuS is actively being used and the irony of how the criminals themselves can sometimes be the victims.

ZeuS is a well-known banking Trojan horse program, also known as crimeware. This trojan steals data from infected computers via web browsers and protected storage. Once infected, the computer sends the stolen data to a bot command and control (C&C) server, where the data is stored.

ZeuS is sold in the criminal underground as a kit for around $3000-4000, and is likely the one malware most utilized by criminals specializing in financial fraud. ZeuS has evolved over time and includes a full arsenal of information stealing capabilities:

- Steals data submitted in HTTP forms
- Steals account credentials stored in the Windows Protected Storage
- Steals client-side X.509 public key infrastructure (PKI) certificates
- Steals FTP and POP account credentials
- Steals/deletes HTTP and Flash cookies
- Modifies the HTML pages of target websites for information stealing purposes
- Redirects victims from target web pages to attacker controlled ones
- Takes screenshots and scrapes HTML from target sites
- Searches for and uploads files from the infected computer
- Modifies the local hosts file (%systemroot%\system32\drivers\etc\hosts)
- Downloads and executes arbitrary programs
- Deletes crucial registry keys, rendering the computer unable to boot into Windows

Zeus Author Protects Code with Hardware-Based Licensing System

The latest version of ZeuS as of this date is 1.3.4.x and is privately sold. The author has gone to great lengths to protect this version using a Hardware-based Licensing System. The author of Zeus has created a hardware-based licensing system for the Zeus Builder kit that you can only run on one computer. Once you run it, you get a code from the specific computer, and then the author gives you a key just for that computer. This is the first time we have seen this level of control for malware.

Zeus Versions

The version number breakdown is as follows (from the ZeuS manual):

What do the numbers [signify] in the version?
a.b.c.d
a(1) - a complete change in the bot. This has never changed from 1.
b(3) - Major changes that cause complete or partial incompatibility with the previous versions. Recently we moved from version 2 to version 3.
c(2) - This is for bug fixes, improvements, and adding features.
d(1) - This for a small revision in the code to make the malware undetectable by AV vendors.

The latest public version the CTU has encountered is 1.2.7.19. This version is actively being traded and has the Firefox form grabber module enabled. The Firefox module allows the ZeuS trojan to grab data out of any forms completed on the Firefox web browser. The webinjects text file, which allows for the injection of fields into the Internet Explorer (IE) web browser, does not work with Firefox and only works with IE. The function of the webinjects text file is to display an extra field for a victim to complete when they log onto a banking site (see Figures 1 and 2). The extra field asks for data in addition to the username and password. This technique is similar to phishing, but the extra field is not part of the original site.

The current list of modules that work with ZeuS are as follows:

- **Zeus Kit for Version 1.3.4.x ($3,000 to $4,000)**
  The Private Version of the Zeus Kit is running between $3,000 and $4,000. The latest private version of ZeuS, as of this date, is 1.3.4.x. This private version seems to be only sold by the author, and he is protecting all of its functionality through the hardware I I.D., locking which we mentioned previously.
- **Backconnect $1500**
  The backconnect module allows an attacker to 'connect back' to the infected computer and make financial transactions from it. This way, banks that try to track where money transfers originate will always trace it back to the computer of the account holder.

- **Firefox form grabber $2000**
  The Firefox form grabber module grabs data out of fields that are submitted using the Firefox web browser. This data can include personally identifiable information (PII) as well as usernames and passwords for bank accounts, trading accounts, online payment accounts, and anything else that would require the use of a username and password.
- **Jabber (IM) chat notifier $500**
  The Jabber module allows an attacker to receive stolen data in "real time". If a bank account is being protected with a token that generates random numbers, then the attacker can access the victim's account in real time after the victim logs in using the token. An example of what would be sent via the Jabber module is:

  > Request Type :Domestic Wire
  > Name :John Smith
  > Address :1234 Main Street
  > City :Atlanta GA 12345
  > Payee Name :Some Bank
  > Memo :Credit to acc:1111111111
  >
  > Beneficiary Account :Checking #0000001234
  > Beneficiary Address 1 :Georgia
  > Payee Bank ID :0123456
  > Bank Name :Some Bank
  > Addr1 :Atlanta Some Bank
  > Amount :1500000.00
  > From Account :My Money Market #123456789
  > Date Posted :01/01/10
  > Time Posted :2:00 PM

VNC (Virtual Network Computing) private module $10,000

The VNC module is similar to the backconnect module, except that it allows you to establish a fully functioning virtual connection. The attacker can take control of the infected computer without the victim being aware of it. Essentially, the VNC provides the hacker with not just a Network Proxy but with a Total Presence Proxy (it is the total package), allowing the hacker to use all of the victim's hardware and software, including its browser, so as to avoid a bank's fraud detection systems. Essentially, it allows the hacker to get around many hardware-based authentication systems. Additionally, if the victim is doing large dollar transactions and is required to insert a smartcard into their computer that the bank will recognize, the hacker will have access to that smartcard via the VNC module.

Windows 7/Vista Support $2000

This module allows the ZeuS trojan to infect these Windows 7 and Vista systems. Without it, the botnet controller is limited to Windows XP systems.

ZeuS 1.4 Adds Polymorphic Encryption and Web Injects for Firefox

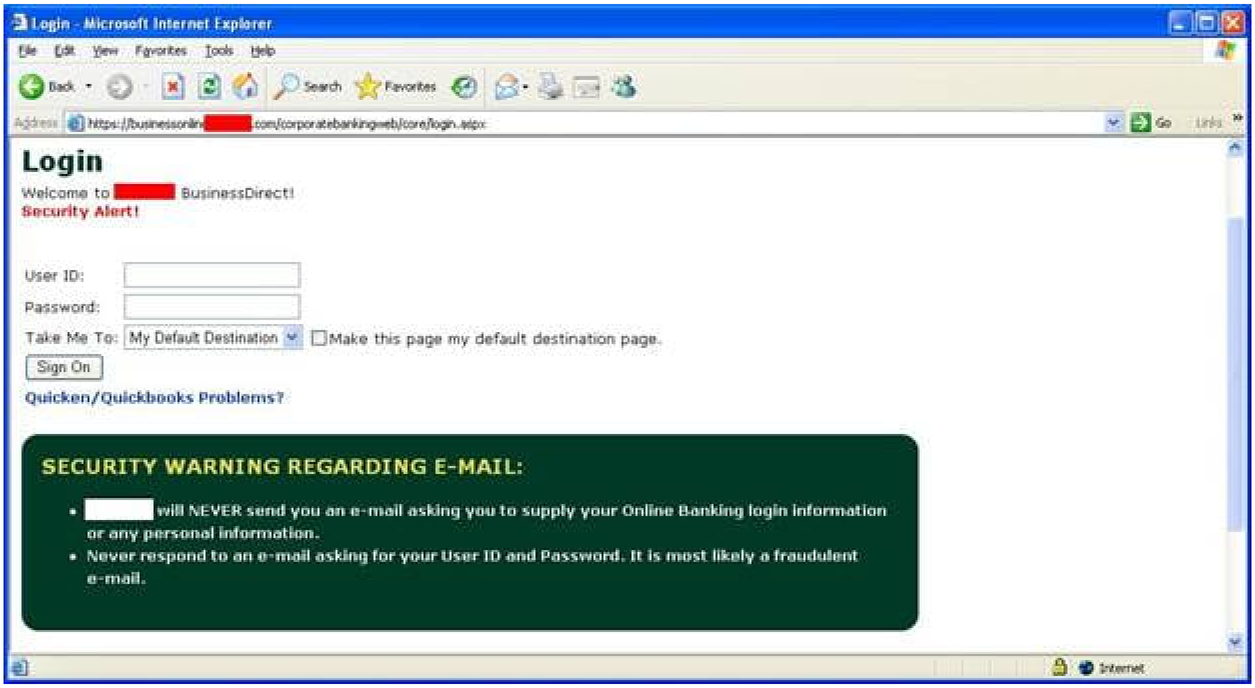
The authors of ZeuS are currently developing 1.4 which is being beta tested. It includes two key components which make the ZeuS Banking Trojan even more stealthy and comprehensive, due to its ability to also do web injects for the Firefox browser. The components are:

1. **Web Injects for Firefox**
2. **Polymorphic Encryption:** The 1.4 version of ZeuS will enable the ZeuS Trojan to re-encrypt itself each time it infects a victim, thus making each infection unique. The 1.4 version also enables the ZeuS file names to be randomly generated, thus each infection will contain different file names. This will make it very difficult for anti-virus engines to identify the ZeuS Banking Trojan on the victims' system.

How Zeus Works

ZeuS performs stolen data exfiltration and remote commands via encrypted HTTP POST requests to a Command and Control web server. The encryption ZeuS uses is RC4, with a key that is embedded in the binary. While the primary function of this malware is to commit financial fraud, its general information stealing behaviors make it a threat to all enterprises. Basic credential theft is not targeted, meaning the ZeuS botnet controller does not run the botnet to just see what it can get. The botnet controller usually has a financial target in mind. The criminals typically search for data of interest to directly derive value or to sell the data to another criminal.

Several of these tasks can be done "on-demand" via the HTTP-based control panel, and directed to selected infected computers. These on-demand tasks may be performed via special scripts that can be executed on select systems. These scripts can be used to take screenshots of infected systems or to do ZeuS binary updates.


Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://businessonlin[redacted].com/corporatebankingweb/core/login.aspx
Go Links
Internet

Login

Welcome to [redacted] BusinessDirect!

Security Alert!

User ID:

Password:

Take Me To: My Default Destination ☐ Make this page my default destination page.

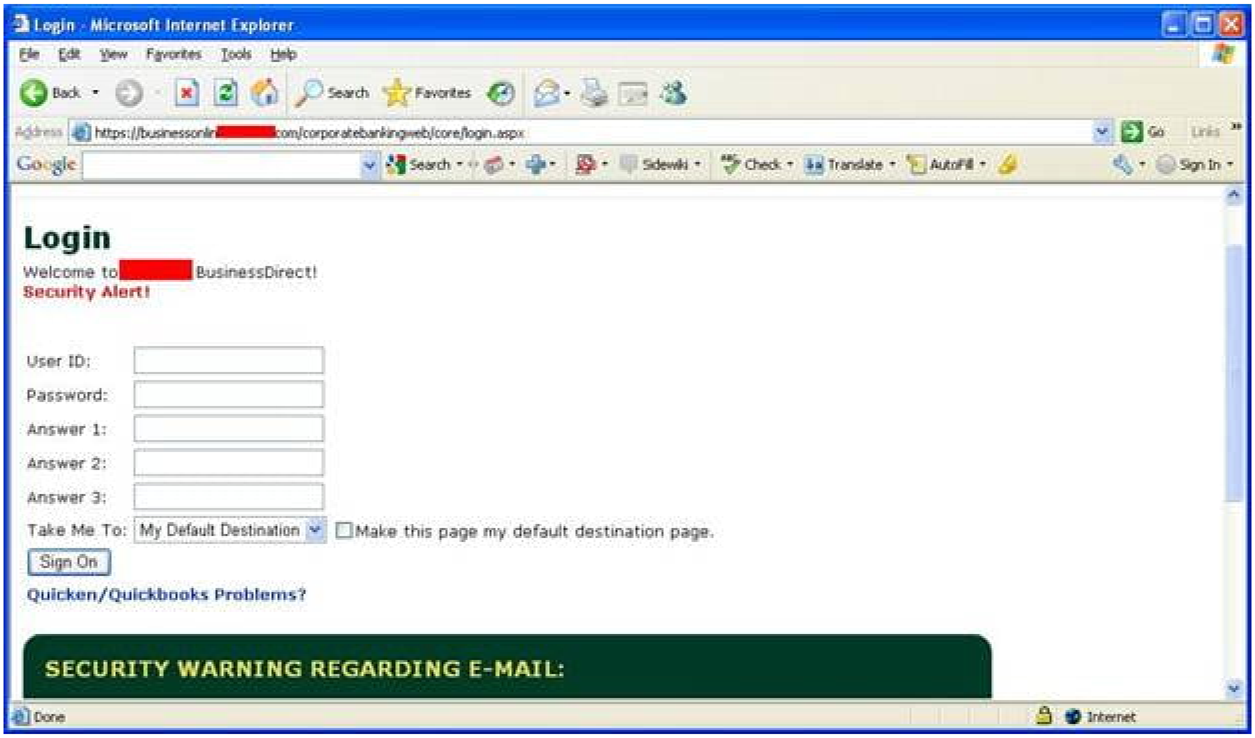
Sign On

Quicken/Quickbooks Problems?

SECURITY WARNING REGARDING E-MAIL:

- [redacted] will NEVER send you an e-mail asking you to supply your Online Banking login information or any personal information.
- Never respond to an e-mail asking for your User ID and Password. It is most likely a fraudulent e-mail.

Figure 1. View of a login page for a financial site.


Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://businessonlin[redacted].com/corporatebankingweb/core/login.aspx
Go Links
Google Search Sidewiki Check Translate AutoFill Sign In
Done
Internet

Login

Welcome to [redacted] BusinessDirect!

Security Alert!

User ID:

Password:

Answer 1:

Answer 2:

Answer 3:

Take Me To: My Default Destination ☐ Make this page my default destination page.

Sign On

Quicken/Quickbooks Problems?

SECURITY WARNING REGARDING E-MAIL:

Figure 2. View of the same page from a computer infected with ZeuS. Note it includes three new fields.

ZeuS includes these capabilities to assist with automated clearing house (ACH) fraud. ACH is an electronic network for financial transactions in the United States. It is used for online bill payments, payroll direct deposits from employers and to transfer money from one account to another. ZeuS is aimed at taking advantage of ACH to transfer money to criminal accounts.

How to detect the ZeuS Banking Trojan on your computer

Computers infected with this version of ZeuS will have the following files and folders installed. The location depends on whether the victim has Administrator rights. The files will most likely have the HIDDEN attribute set to hide them from casual inspection.

With Administrator rights:

> %systemroot%\system32\sdra64.exe (malware)
> %systemroot%\system32\lowsec
> %systemroot%\system32\lowsec\user.ds (encrypted stolen data file)
> %systemroot%\system32\lowsec\user.ds.lll (temporary file for stolen data)
> %systemroot%\system32\lowsec\local.ds (encrypted configuration file)

Without Administrator rights:

> %appdata%\sdra64.exe
> %appdata%\lowsec
> %appdata%\lowsec\user.ds
> %appdata%\lowsec\user.ds.lll
> %appdata%\lowsec\local.ds

ZeuS also makes registry changes to ensure that it starts up with Administrator privileges:

> HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
> From:
> "Userinit" = "C:\WINDOWS\system32\userinit.exe"
> To:
> "Userinit" =
> "C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe"

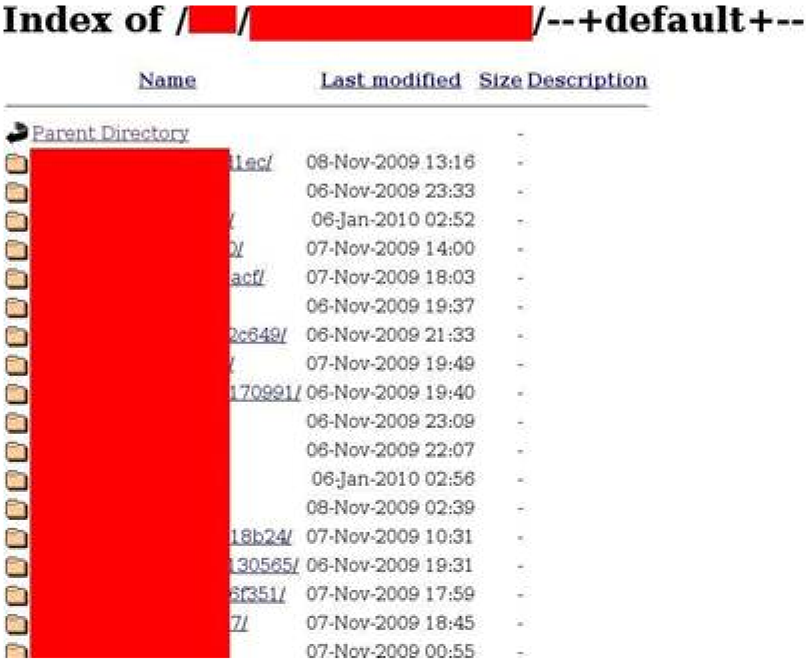
Without Administrator rights:

> HKCU\Software\Microsoft\Windows\CurrentVersion\Run
> Add:
> "Userinit" = "C:\Documents and Settings\&lt;user&gt;\Application Data\sdra64.exe"

The sdra64.exe program uses process injection to hide its presence in the list of running processes. Upon startup, it will inject code into winlogon.exe (if Administrator rights available) or explorer.exe (for non-Administrators) and exit. The injected code infects other processes to perform its data theft capabilities.

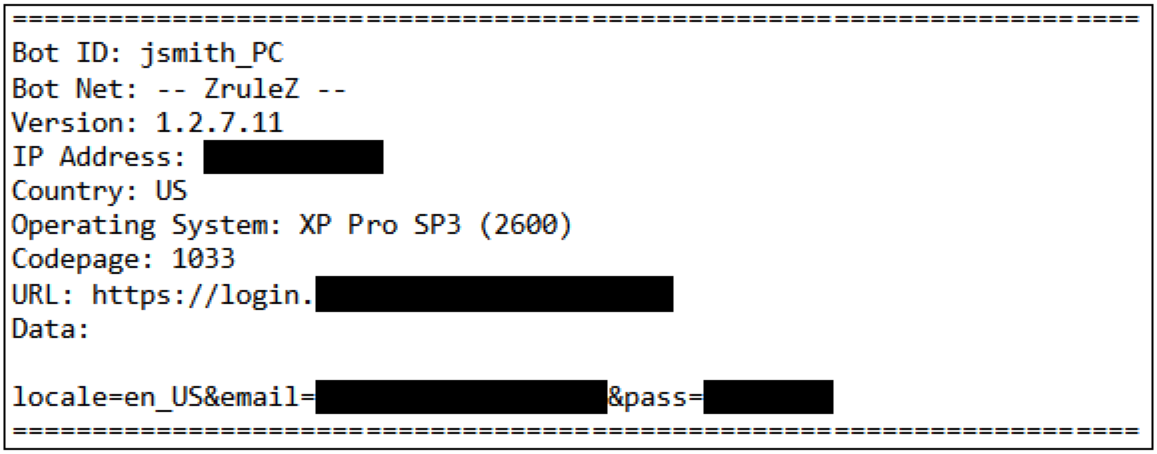
Types of data being targeted by ZeuS

The following figures illustrate what type of data is stolen and collected from infected computers. The list of infected systems shown in Figure 3 can range from the hundreds to thousands. The number of infected systems usually depends on how long the botnet is active and how well the bot controller spreads the malware.



```
Index of /[redacted]/[redacted]/--+default+--

      Name                  Last modified       Size Description
------------------------------------------------------------------
Parent Directory                                 -
[redacted]                 08-Nov-2009 13:16    -
[redacted]                 06-Nov-2009 23:33    -
[redacted]                 06-Jan-2010 02:52    -
[redacted]                 07-Nov-2009 14:00    -
[redacted]                 07-Nov-2009 18:03    -
[redacted]                 06-Nov-2009 19:37    -
[redacted]                 06-Nov-2009 21:33    -
[redacted]                 07-Nov-2009 19:49    -
[redacted]                 06-Nov-2009 19:40    -
[redacted]                 06-Nov-2009 23:09    -
[redacted]                 06-Nov-2009 22:07    -
[redacted]                 06-Jan-2010 02:56    -
[redacted]                 08-Nov-2009 02:39    -
[redacted]                 07-Nov-2009 10:31    -
[redacted]                 06-Nov-2009 19:31    -
[redacted]                 07-Nov-2009 17:59    -
[redacted]                 07-Nov-2009 18:45    -
[redacted]                 07-Nov-2009 00:55    -
```

Figure 3. List of infected systems. Each system is a folder on the C&C server.



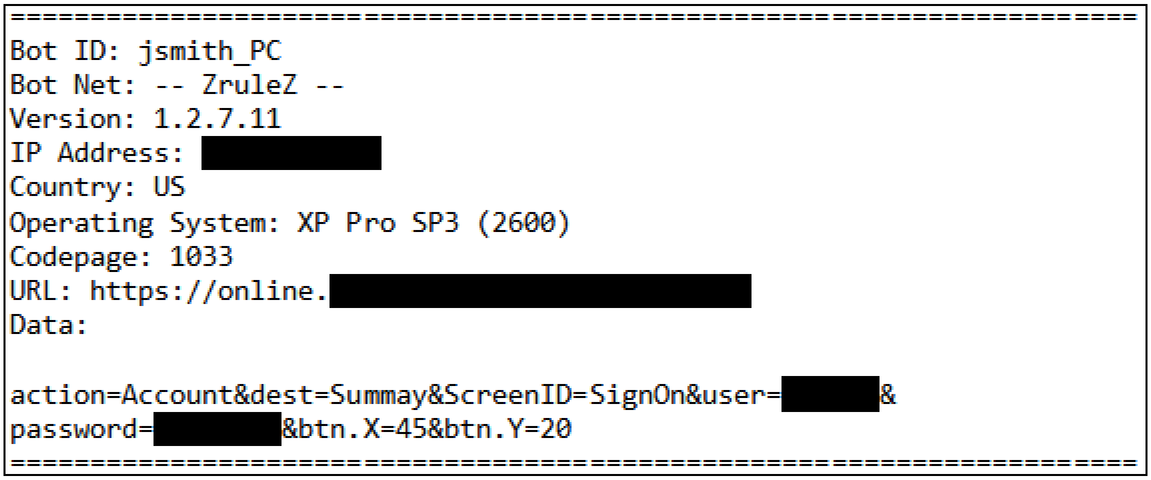
```
========================================================================
Bot ID: jsmith_PC
Bot Net: -- ZruleZ --
Version: 1.2.7.11
IP Address: [redacted]
Country: US
Operating System: XP Pro SP3 (2600)
Codepage: 1033
URL: https://login.[redacted]
Data:

locale=en_US&email=[redacted]&pass=[redacted]
========================================================================
```

Figure 4. Sample of collected information from an infected system for a social networking site.

Figure 4 illustrates a fragment of information collected from an infected system.

- This listing begins with the bot id, which is usually the name of the affected computer.
- Next is the name of the botnet that includes the affected computer. Also listed is the bot version.
- Next appears the IPv4 IP address of the affected computer and the country it belongs to. This information is not always accurate because a host with an internal IP will not display correctly.
- Further down the list appears the OS.

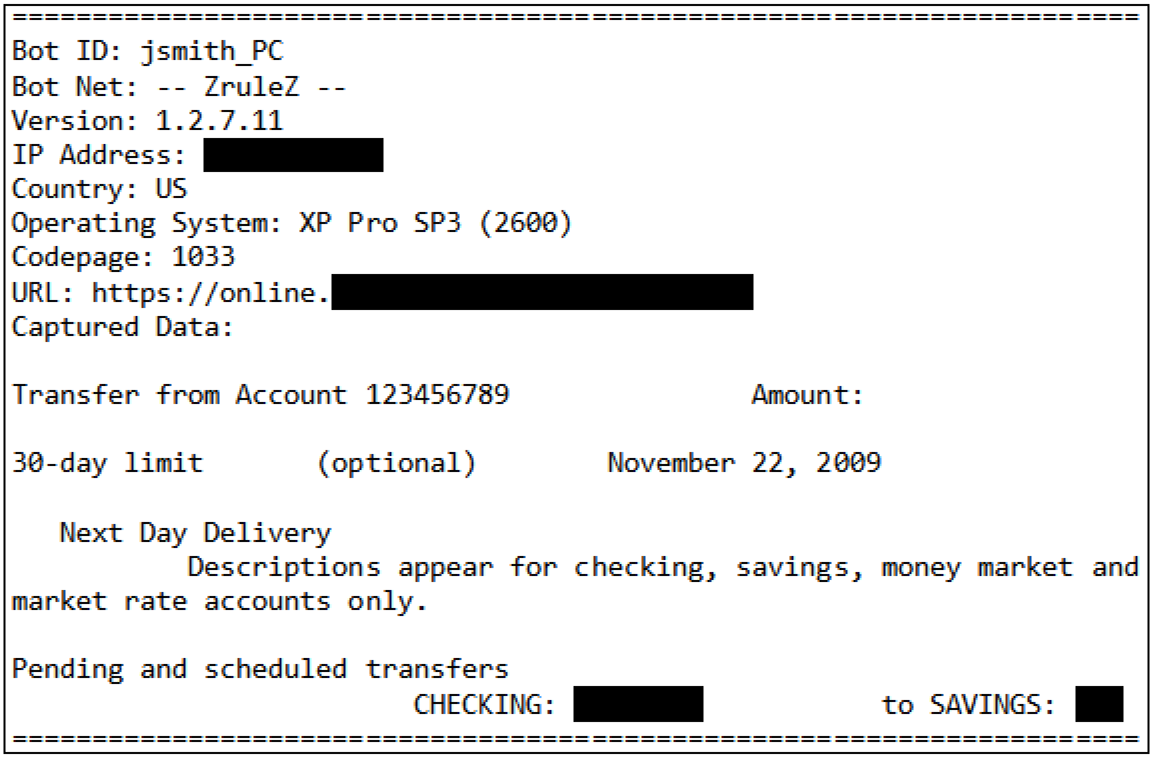
- This log was captured from an Internet Explorer web browser used to visit a popular social networking website.
- ZeuS captured the language used, full page parameters, email address, password, and anything else that was being generated from the login attempt.



```
=======================================================================
Bot ID: jsmith_PC
Bot Net: -- ZruleZ --
Version: 1.2.7.11
IP Address: [redacted]
Country: US
Operating System: XP Pro SP3 (2600)
Codepage: 1033
URL: https://online.[redacted]
Data:

action=Account&dest=Summay&ScreenID=SignOn&user=[redacted]&
password=[redacted]&btn.X=45&btn.Y=20
=======================================================================
```

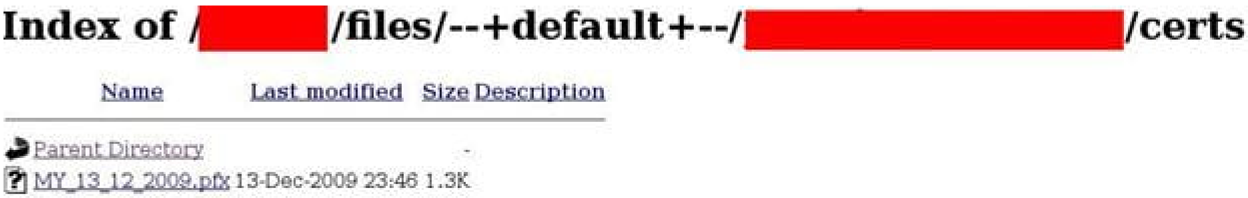
Figure 5. Sample of banking information collected from an infected system.

Figure 5 is similar in function to the previous listing, but this time ZeuS is stealing the login information for a bank account. Figure 6 shows the same user transferring money from checking to savings. These examples demonstrate the risks that infected computers and their users are susceptible to.



```
=======================================================================
Bot ID: jsmith_PC
Bot Net: -- ZruleZ --
Version: 1.2.7.11
IP Address: [redacted]
Country: US
Operating System: XP Pro SP3 (2600)
Codepage: 1033
URL: https://online.[redacted]
Captured Data:

Transfer from Account 123456789               Amount:

30-day limit       (optional)       November 22, 2009

   Next Day Delivery
           Descriptions appear for checking, savings, money market and
market rate accounts only.

Pending and scheduled transfers
                         CHECKING: [redacted]          to SAVINGS: [redacted]
=======================================================================
```

Figure 6. Sample of banking transaction information collected from an infected system.

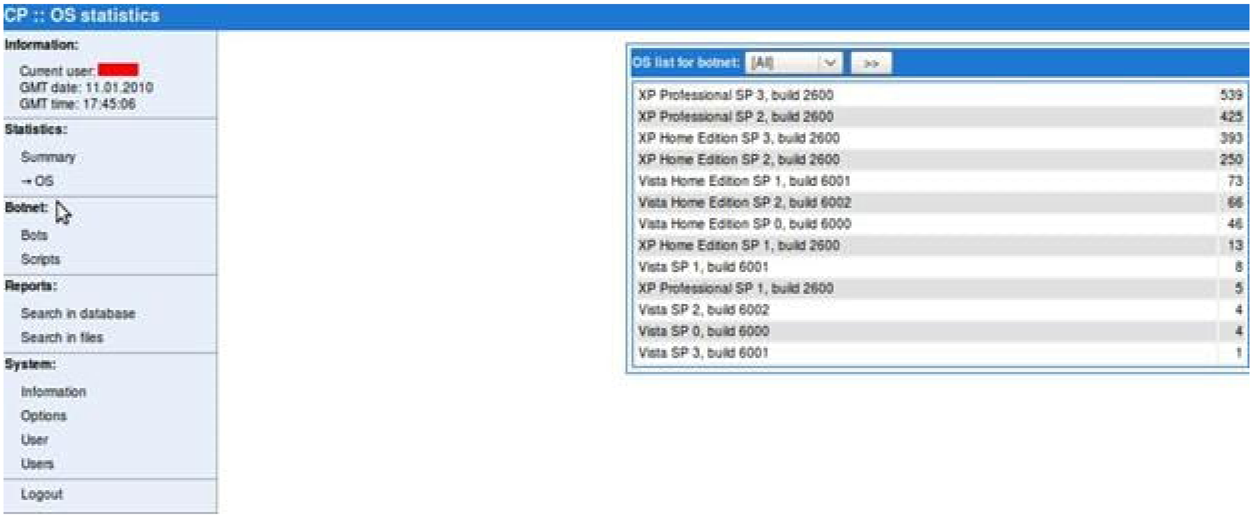


Index of /[redacted]/files/--+default+--/[redacted]/certs

Name	Last modified	Size	Description
Parent Directory		-	
MY_13_12_2009.pfx	13-Dec-2009 23:46	1.3K	

Figure 7. PFX (PKCS #12) Digital Certificate file collected from an infected system.

ZeuS even steals PFX (PKCS #12) Digital Certificates that the victim's web browser uses to authenticate to a site (Figure 7). So the victim is still vulnerable if their banking site uses assigned certificates.



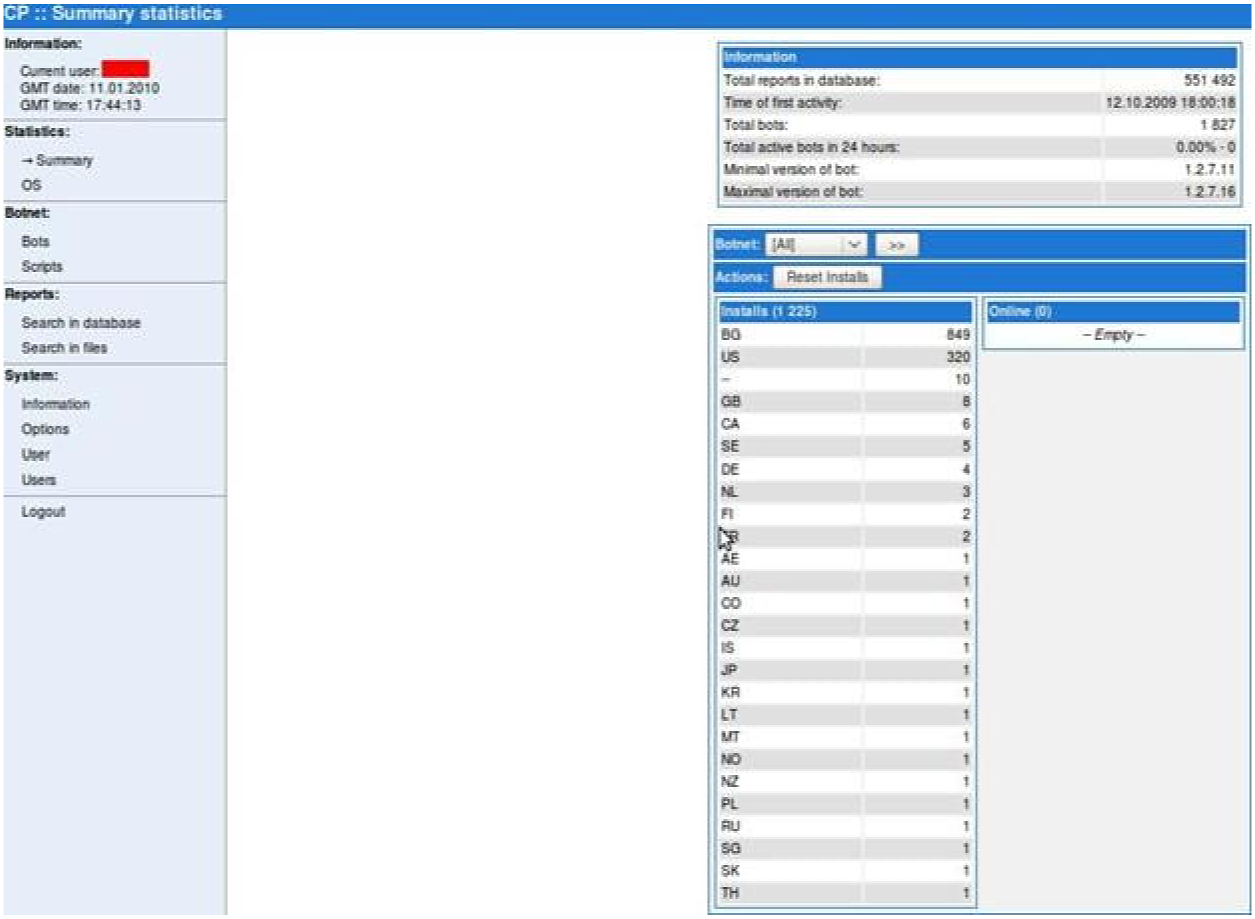
Current user: [redacted]
GMT date: 11.01.2010
GMT time: 17:45:06

OS list for botnet: [All]

XP Professional SP 3, build 2600	539
XP Professional SP 2, build 2600	425
XP Home Edition SP 3, build 2600	393
XP Home Edition SP 2, build 2600	250
Vista Home Edition SP 1, build 6001	73
Vista Home Edition SP 2, build 6002	66
Vista Home Edition SP 0, build 6000	46
XP Home Edition SP 1, build 2600	13
Vista SP 1, build 6001	8
XP Professional SP 1, build 2600	5
Vista SP 2, build 6002	4
Vista SP 0, build 6000	4
Vista SP 3, build 6001	1

Figure 8. ZeuS server control panel, operating system statistics.

Figure 8 shows a ZeuS server using the 1.2.4.2 version control panel. The screen displays totals of the bots and what OS version they are running, the most popular being Windows XP Professional SP3. This ZeuS bot also infected Vista users, which means the bot controller paid extra for the Vista/Windows 7 module.



CP :: Summary statistics

Information:

Current user: [redacted]
GMT date: 11.01.2010
GMT time: 17:44:13

Statistics:

→ Summary
OS

Botnet:

Bots
Scripts

Reports:

Search in database
Search in files

System:

Information
Options
User
Users

Logout

Information	
Total reports in database:	551 492
Time of first activity:	12.10.2009 18:00:18
Total bots:	1 827
Total active bots in 24 hours:	0.00% - 0
Minimal version of bot:	1.2.7.11
Maximal version of bot:	1.2.7.16

Botnet: [All] >>

Actions: Reset Installs

Installs (1 225)	
BG	849
US	320
--	10
GB	8
CA	6
SE	5
DE	4
NL	3
FI	2
FR	2
AE	1
AU	1
CO	1
CZ	1
IS	1
JP	1
KR	1
LT	1
MT	1
NO	1
NZ	1
PL	1
RU	1
SG	1
SK	1
TH	1

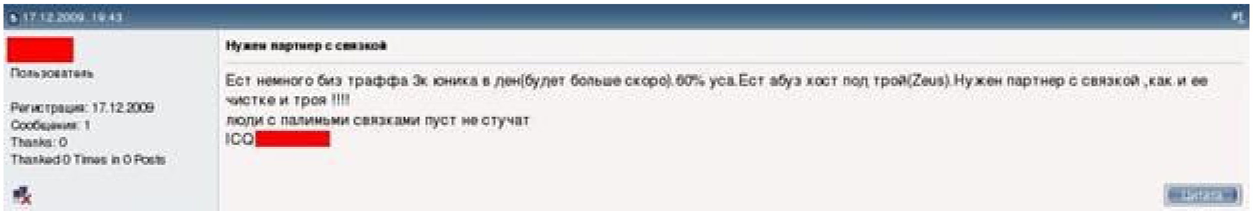
Online (0)
-- Empty --

Figure 9. ZeuS server control panel, statistics summary.

Figure 9 shows the same botnet, listing bots by country. It lists the most prevalent country as BG (Bulgaria), but according to reports from bot operators, this value is not accurate because ZeuS could not determine the country listing from internal IP addresses. Note that this botnet has 1,827 infected computers (bots) in it and has logged 551,492 reports.

Stolen ZeuS data cache

Now we will take a look at how botnet data gets stolen and leaked. Figure 10 shows a botnet controller looking for a partner for his ZeuS botnet.



17.12.2009, 19:43 #1

[redacted]
Пользователь

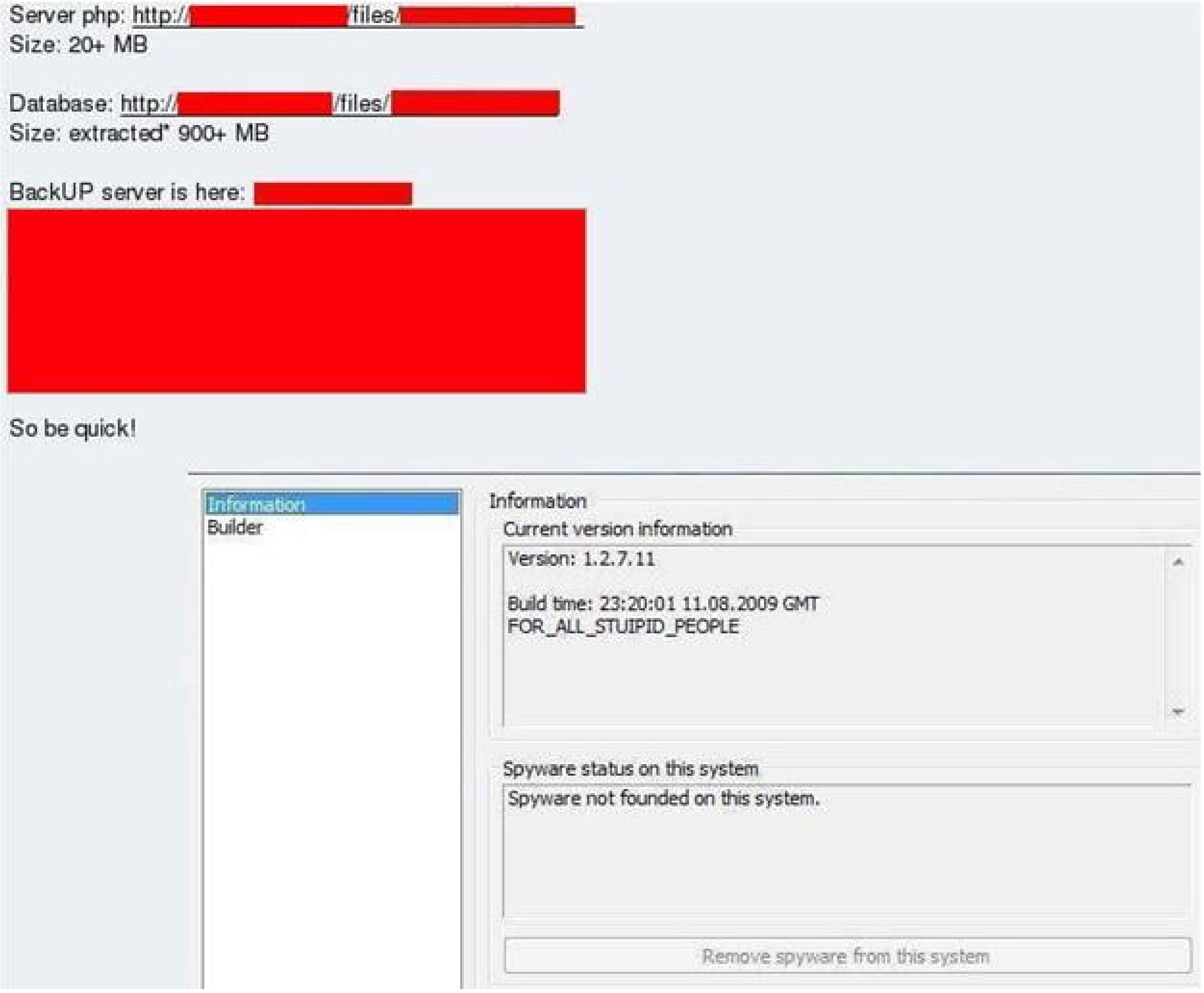
Регистрация: 17.12.2009
Сообщения: 1
Thanks: 0
Thanked 0 Times in 0 Posts

Нужен партнер с связкой

Ест немного биз траффа 3к юника в ден(будет больше скоро).60% уса.Ест абуз хост под трой(Zeus).Нужен партнер с связкой ,как и ее чистке и троя !!!!
люди с палимыми связками пуст не стучат
ICQ[redacted]

Figure 10. Message from botnet controller looking for business partner.

Now his ZeuS server gets hacked and the database is posted online. The download contains the entire database plus the server-side ZeuS PHP files. The attacker is even happy enough to tell you what server he got it from.



Server php: http://[redacted]/files/[redacted]
Size: 20+ MB

Database: http://[redacted]/files/[redacted]
Size: extracted* 900+ MB

BackUP server is here: [redacted]
[redacted]

So be quick!

Information

Current version information

Version: 1.2.7.11

Build time: 23:20:01 11.08.2009 GMT
FOR_ALL_STUIPID_PEOPLE

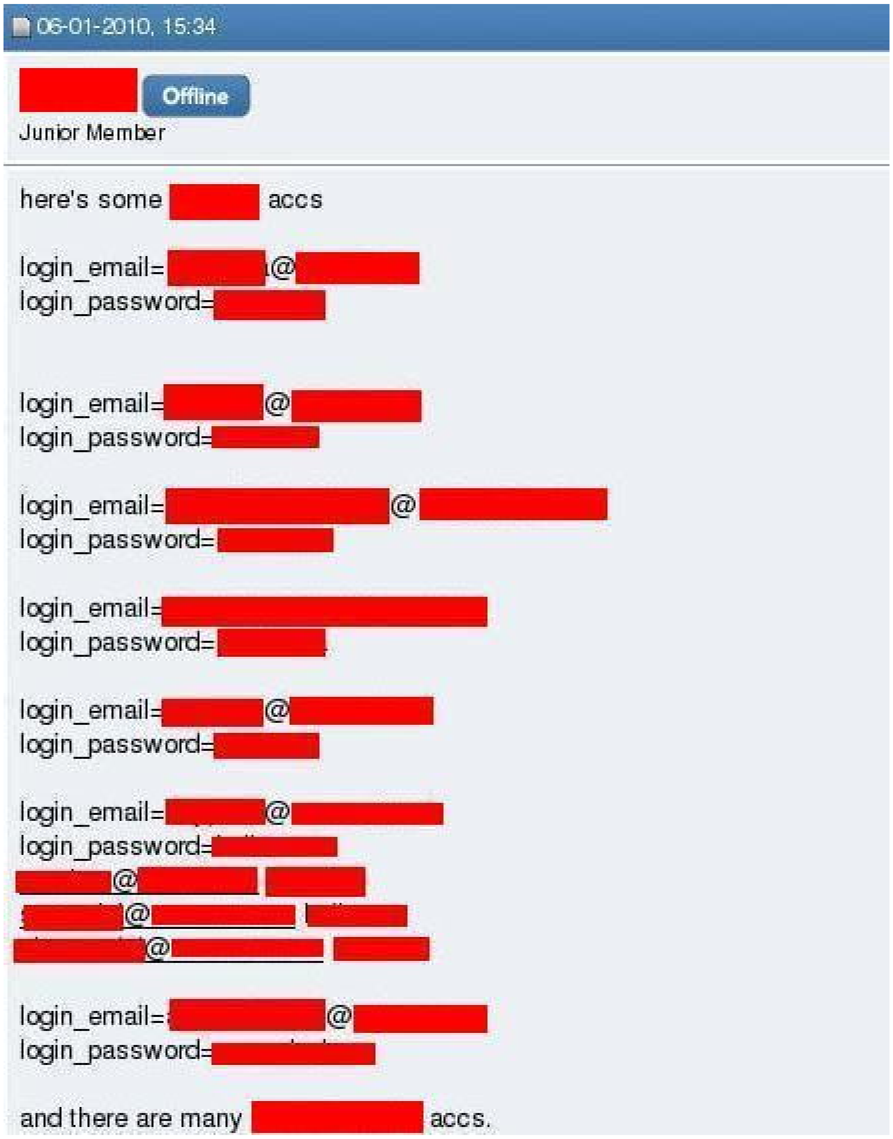
Spyware status on this system

Spyware not founded on this system.

Figure 11. Message advertising hacked ZeuS server content.

Data Stolen by ZeuS

The total size of the PHP files for the ZeuS server is 20MB, and the stolen database is 900MB. The database contained login credentials from 1,827 victims located in the US, UK, Canada, Europe, etc. These login credentials were for banking, stock trading, credit union, online payment, insurance, social networking, government, and military accounts. The bank account, credit union, stock trading, and online payment credentials were for many large and medium sized institutions in the US, UK and Canada.



06-01-2010, 15:34

[redacted] Offline

Junior Member

here's some [redacted] accs

login_email=[redacted]@[redacted]
login_password=[redacted]

login_email=[redacted]@[redacted]
login_password=[redacted]

login_email=[redacted]@[redacted]
login_password=[redacted]

login_email=[redacted]
login_password=[redacted]

login_email=[redacted]@[redacted]
login_password=[redacted]

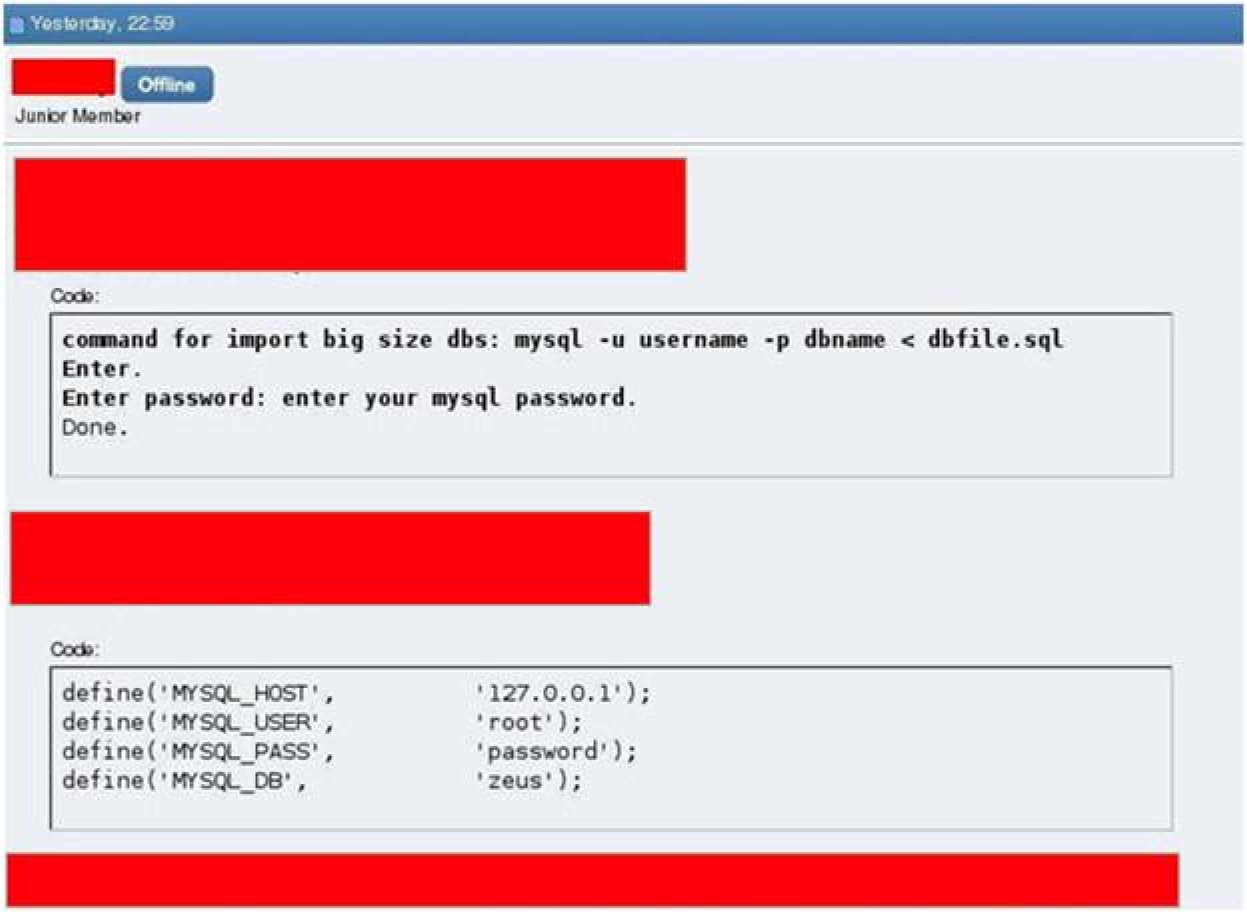
login_email=[redacted]@[redacted]
login_password=[redacted]
[redacted]@[redacted] [redacted]
[redacted]@[redacted] [redacted]
[redacted]@[redacted] [redacted]

login_email=[redacted]@[redacted]
login_password=[redacted]

and there are many [redacted] accs.

Figure 12. Message listing account credentials from the ZeuS database.

Figure 12 shows the same user posting account usernames and passwords to try to prove that there is valuable data in the stolen ZeuS database file.



Yesterday, 22:59

[redacted]

Junior Member

[redacted]

Code:

```
command for import big size dbs: mysql -u username -p dbname < dbfile.sql
Enter.
Enter password: enter your mysql password.
Done.
```

[redacted]

Code:

```
define('MYSQL_HOST',          '127.0.0.1');
define('MYSQL_USER',          'root');
define('MYSQL_PASS',          'password');
define('MYSQL_DB',            'zeus');
```

[redacted]

Figure 13. Message explaining how to import the ZeuS database in MySQL.

The same user then gives details on how to import the database into a MySQL server so that anyone can start sorting through the data. He also gives the username and password for the login. Figure 13 mentions the same person that was looking for a partner in Figure 10. The CTU has observed other ZeuS databases for sale on various underground black markets. Their size is typically over 10GB, which is a botnet of approximately 23,000 infected computers (bots).

How to Protect Yourself from ZeuS

The CTU recommends that businesses and home users carry out online banking and financial transactions on isolated workstations that are not used for general Internet activities, such as web browsing and reading email which could increase the risk of infection.

Businesses may even consider using an alternative operating system for workstations accessing sensitive or financial accounts. Keep your antivirus, operating system and software patches up to date. Also do not open suspicious e-mail attachments or links from people that you do not know and even if you do know them, check with them to find out if they sent you something prior to opening the email. Additionally, awareness for both customers and employees is crucial. In particular, employees who interface with clients should be made aware of these types of threats to help triage potential victims.