Zeus & You: Analysis of the Underground's Most Popular Trojan

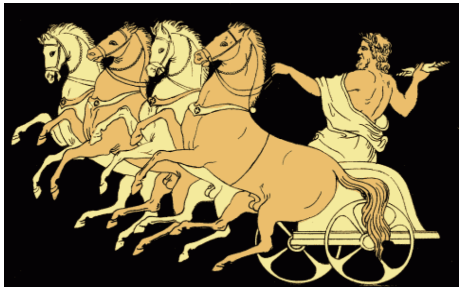
Alexander Heid
Fabian Rothschild
1/27/2010

OWASP

The OWASP Foundation
http://www.owasp.org

About

This presentation seeks to answer the following questions:



- What is Zeus?
- How does Zeus work? (Payload and C&C)
- How can I protect my web applications when my legitimate users are infected?

What is Zeus?

- Originally developed by Russian Business Network, many variants have been made by different groups

- One of the most common 'crimeware' trojans found in the wild

- It is specifically targeted towards the collection of banking credentials, e-mail accounts, credit card numbers, and other PII.

Who is using Zeus?

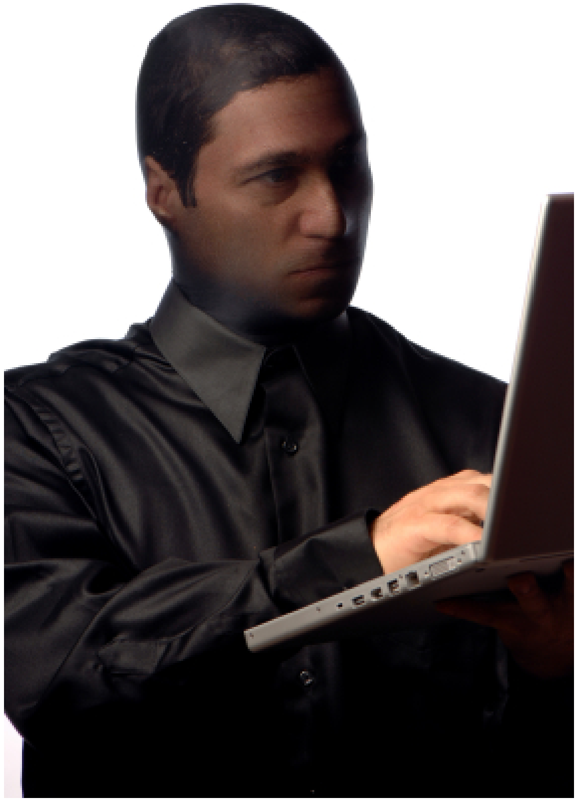
Carders

Carders use the CVV data collected by Zeus for monetization purposes.
Carders also resell the data.

Spammers / Phishers

Spammers and phishers e-mail out Zeus payloads in bulk with the hopes of a percentage of infection. In addition to fraud, spammers will use the e-mail account credentials gained to send out more spam.

Organized Crime



Organized crime uses Zeus to collect bank login and identity information in order to initiate fraudulent wire transfers.

Scr1pt K1ddi3s

Script Kiddies are attracted to Zeus because of it's easy to obtain, easy to use, hard to detect, and technical support is available for relatively low prices.

How does it work?

- **Propagation**

Spam, Phishing

P2P

Exploit packs on hacked or malicious websites

Social engineering (ie fake codecs, backdoored warez)

- **Payload / Infection**

Injects into services.exe, invisible to task manager

List of targets stored in encrypted file on infected machine

Configuration resides in hidden folders via rootkit techniques

Very low detection rate by AV (due to crypters, packers, and new variants)

- **Communication**

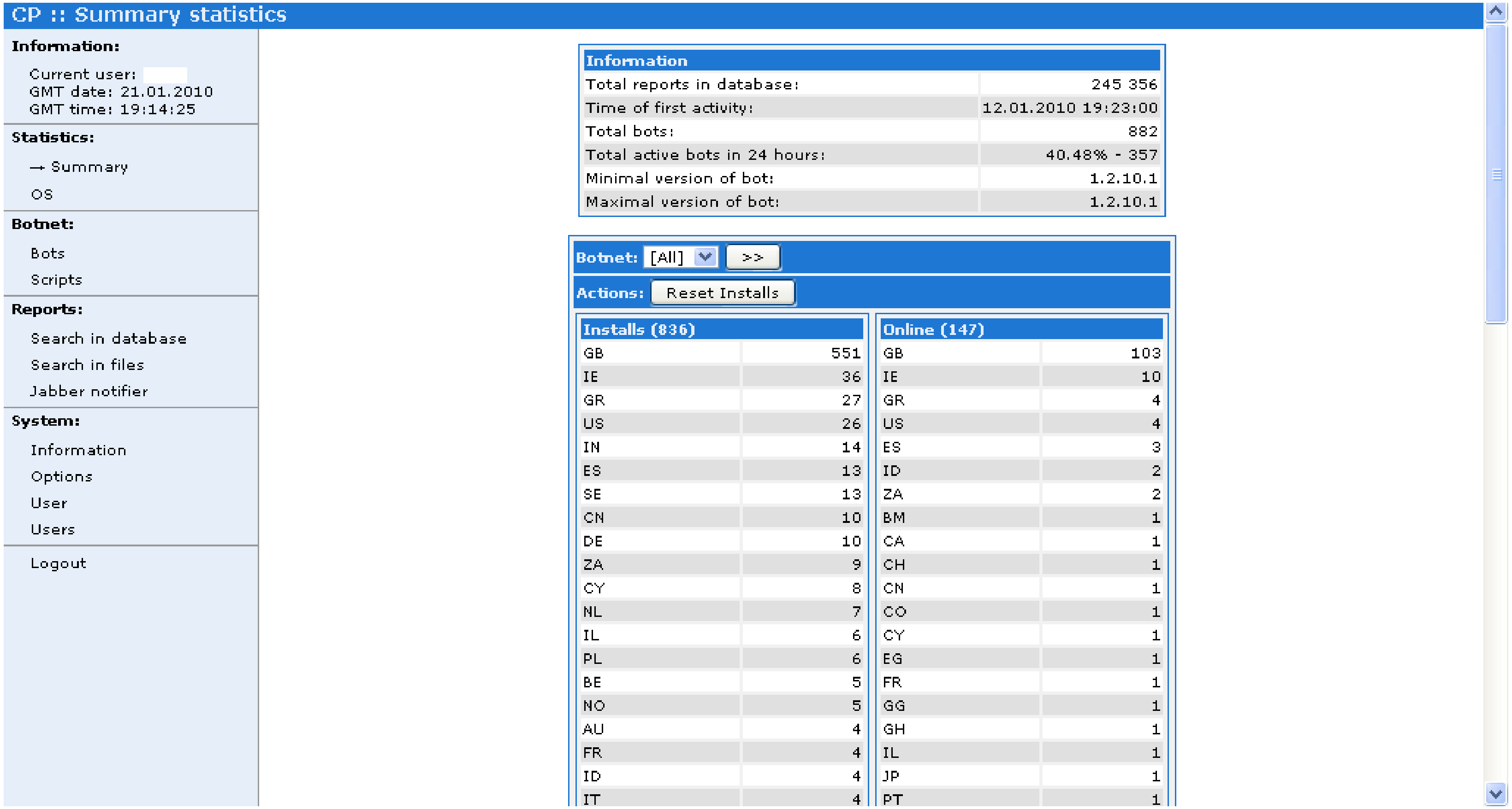
Command and control (C&C) is a user friendly PHP web app that runs on any server.

Infected machines communicate to a command and control server (C&C) web application via HTTP POST using RC4 encryption. Zeus will collect logins, password, cookies, VIEWSTATE parameters, and virtually everything else passed in a POST request.

Malicious DLL's hook the web browser and reports are entered into an SQL database and .txt files that contain logs of activity on infected machines.

How does it work?

- **Zeus Control Panel**



CP :: Summary statistics

Information:

Current user: [redacted]
GMT date: 21.01.2010
GMT time: 19:14:25

Statistics:

→ Summary
OS

Botnet:

Bots
Scripts

Reports:

Search in database
Search in files
Jabber notifier

System:

Information
Options
User
Users

Logout

Information	
Total reports in database:	245 356
Time of first activity:	12.01.2010 19:23:00
Total bots:	882
Total active bots in 24 hours:	40.48% - 357
Minimal version of bot:	1.2.10.1
Maximal version of bot:	1.2.10.1

Botnet: [All] >>

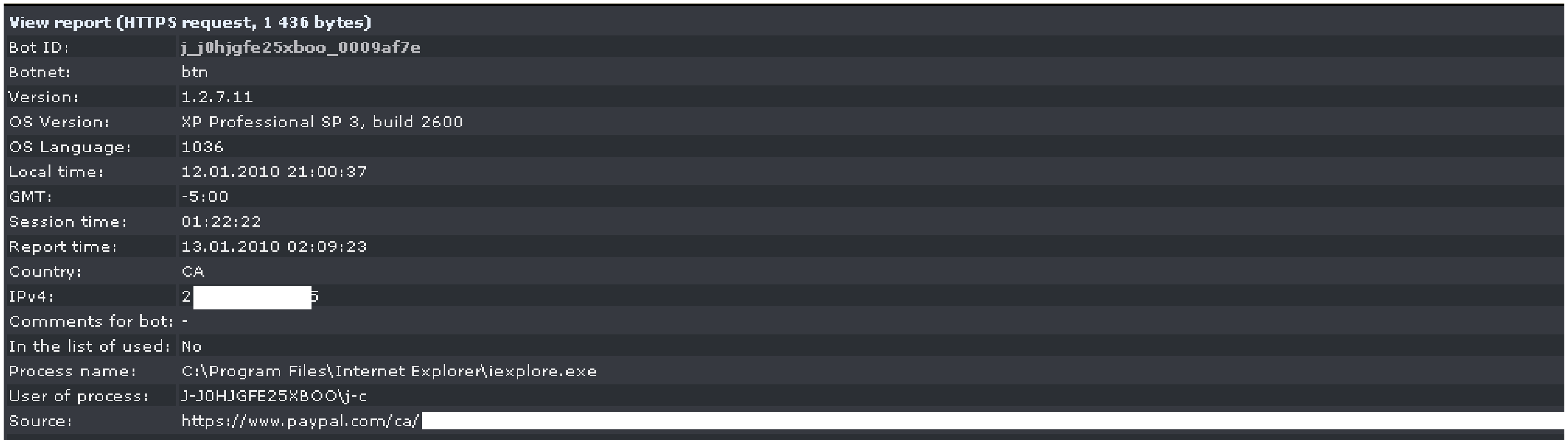
Actions: Reset Installs

Installs (836)	
GB	551
IE	36
GR	27
US	26
IN	14
ES	13
SE	13
CN	10
DE	10
ZA	9
CY	8
NL	7
IL	6
PL	6
BE	5
NO	5
AU	4
FR	4
ID	4
IT	4

Online (147)	
GB	103
IE	10
GR	4
US	4
ES	3
ID	2
ZA	2
BM	1
CA	1
CH	1
CN	1
CO	1
CY	1
EG	1
FR	1
GG	1
GH	1
IL	1
JP	1
PT	1

How does it work?

- **Sample Report File**

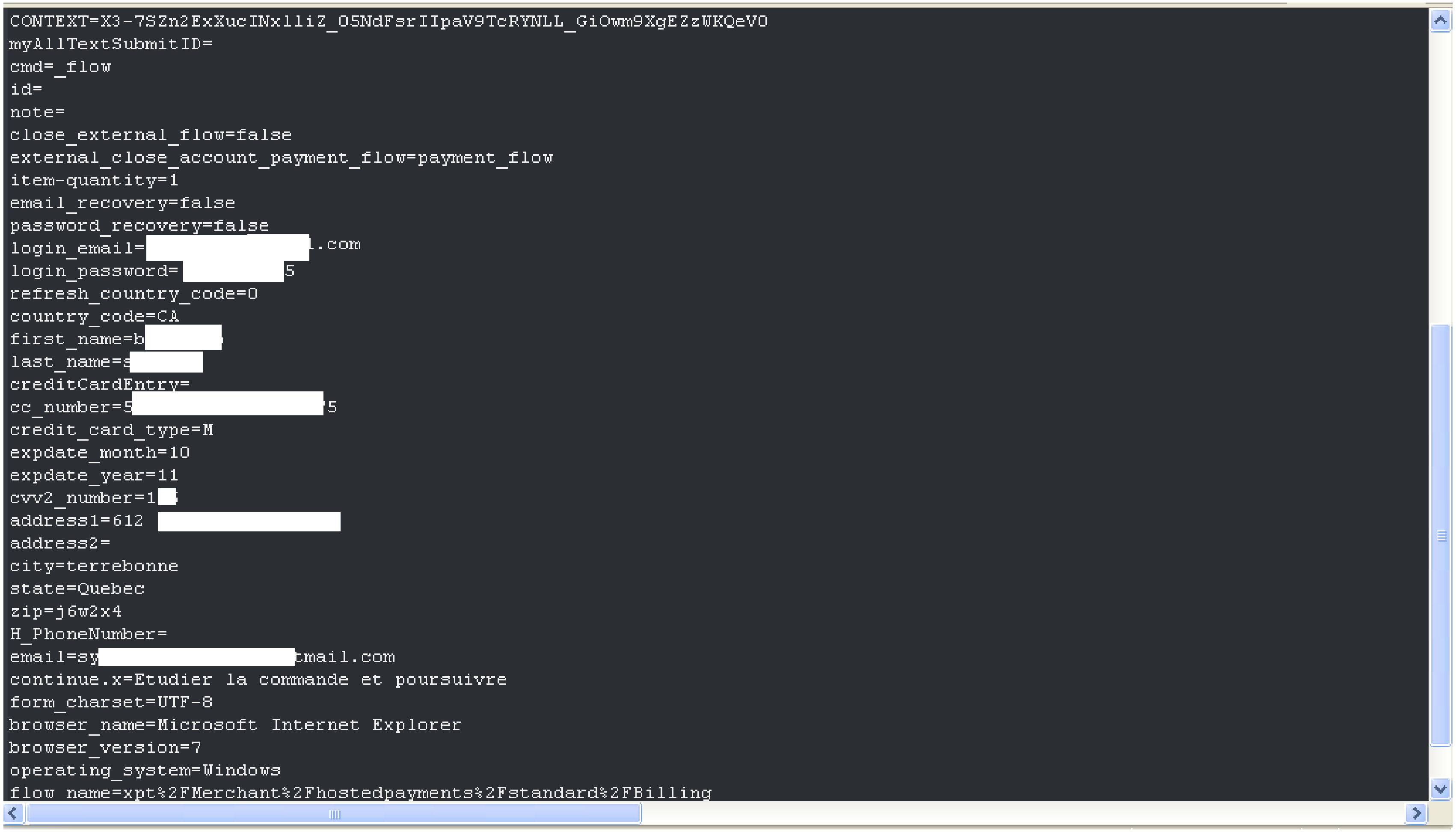


View report (HTTPS request, 1 436 bytes)	
Bot ID:	j_j0hjgfe25xboo_0009af7e
Botnet:	btn
Version:	1.2.7.11
OS Version:	XP Professional SP 3, build 2600
OS Language:	1036
Local time:	12.01.2010 21:00:37
GMT:	-5:00
Session time:	01:22:22
Report time:	13.01.2010 02:09:23
Country:	CA
IPv4:	2[redacted]
Comments for bot:	-
In the list of used:	No
Process name:	C:\Program Files\Internet Explorer\iexplore.exe
User of process:	J-J0HJGFE25XBOO\j-c
Source:	https://www.paypal.com/ca/[redacted]

OWASP

How does it work?

- **Sample Report File (continued)**



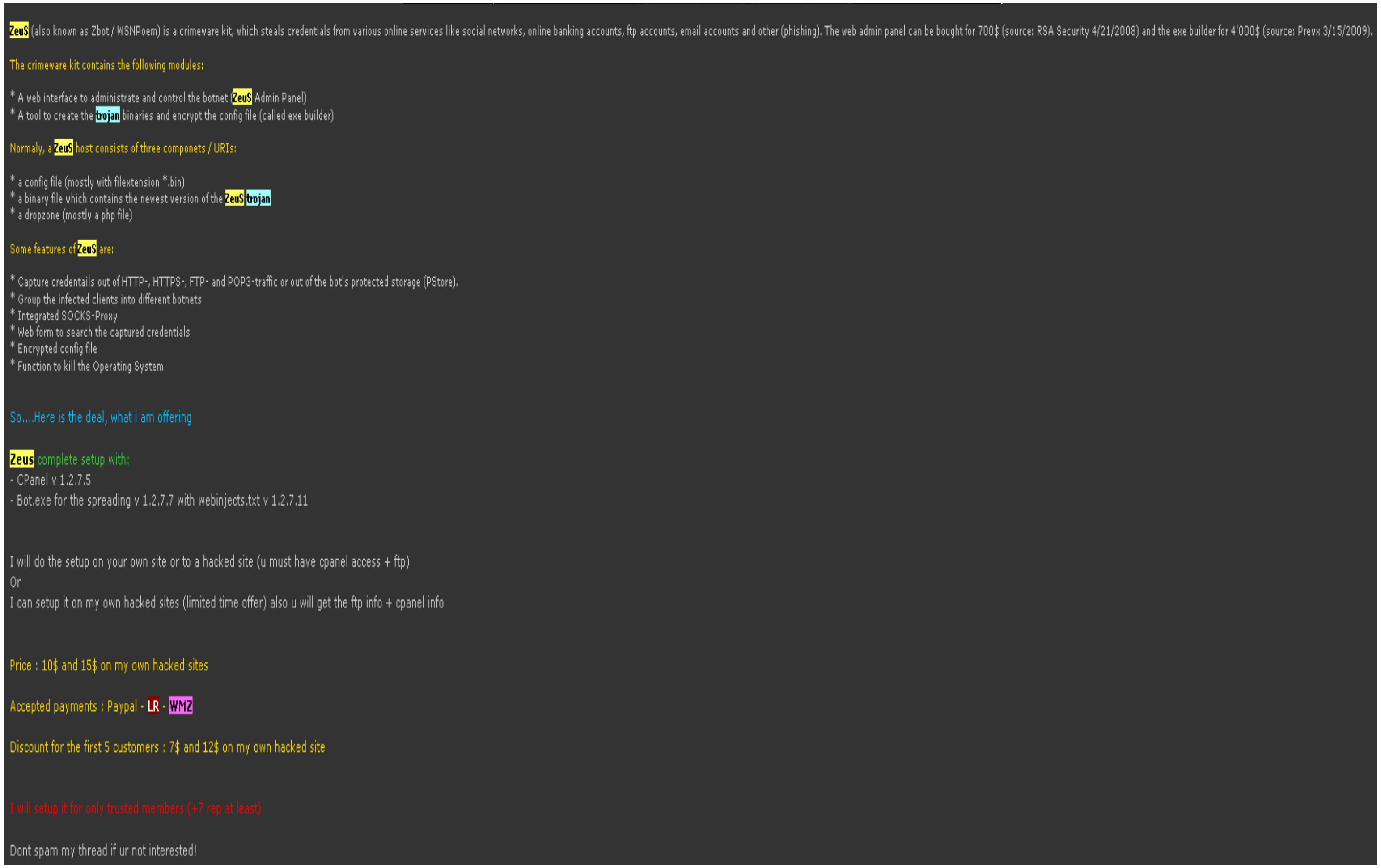
```
CONTEXT=X3-7SZn2ExXucINx1liZ_05NdFsrIIpaV9TcRYNLL_GiOwm9XgEZzWKQeVO
myAllTextSubmitID=
cmd=_flow
id=
note=
close_external_flow=false
external_close_account_payment_flow=payment_flow
item-quantity=1
email_recovery=false
password_recovery=false
login_email=[redacted].com
login_password=[redacted]5
refresh_country_code=0
country_code=CA
first_name=b[redacted]
last_name=s[redacted]
creditCardEntry=
cc_number=5[redacted]5
credit_card_type=M
expdate_month=10
expdate_year=11
cvv2_number=1[redacted]
address1=612 [redacted]
address2=
city=terrebonne
state=Quebec
zip=j6w2x4
H_PhoneNumber=
email=sy[redacted]tmail.com
continue.x=Etudier la commande et poursuivre
form_charset=UTF-8
browser_name=Microsoft Internet Explorer
browser_version=7
operating_system=Windows
flow_name=xpt%2FMerchant%2Fhostedpayments%2Fstandard%2FBilling
```

OWASP

Where can I get a copy?

- Old, backdoored versions are available free on public forums
- Installation services are available from underground forums for low prices.
- New versions of the payload builder and webpanel C&C are usually for sale on underground forums for high prices (over $1000)

Old Variant of Zeus for Sale on a Forum for $10-15



ZeuS (also known as Zbot / WSNPoem) is a crimeware kit, which steals credentials from various online services like social networks, online banking accounts, ftp accounts, email accounts and other (phishing). The web admin panel can be bought for 700$ (source: RSA Security 4/21/2008) and the exe builder for 4'000$ (source: Prevx 3/15/2009).

The crimeware kit contains the following modules:

* A web interface to administrate and control the botnet (ZeuS Admin Panel)
* A tool to create the trojan binaries and encrypt the config file (called exe builder)

Normaly, a ZeuS host consists of three componets / URIs:

* a config file (mostly with filextension *.bin)
* a binary file which contains the newest version of the ZeuS trojan
* a dropzone (mostly a php file)

Some features of ZeuS are:

* Capture credentails out of HTTP-, HTTPS-, FTP- and POP3-traffic or out of the bot's protected storage (PStore).
* Group the infected clients into different botnets
* Integrated SOCKS-Proxy
* Web form to search the captured credentials
* Encrypted config file
* Function to kill the Operating System

So....Here is the deal, what i am offering

Zeus complete setup with:
- CPanel v 1.2.7.5
- Bot.exe for the spreading v 1.2.7.7 with webinjects.txt v 1.2.7.11

I will do the setup on your own site or to a hacked site (u must have cpanel access + ftp)
Or
I can setup it on my own hacked sites (limited time offer) also u will get the ftp info + cpanel info

Price : 10$ and 15$ on my own hacked sites

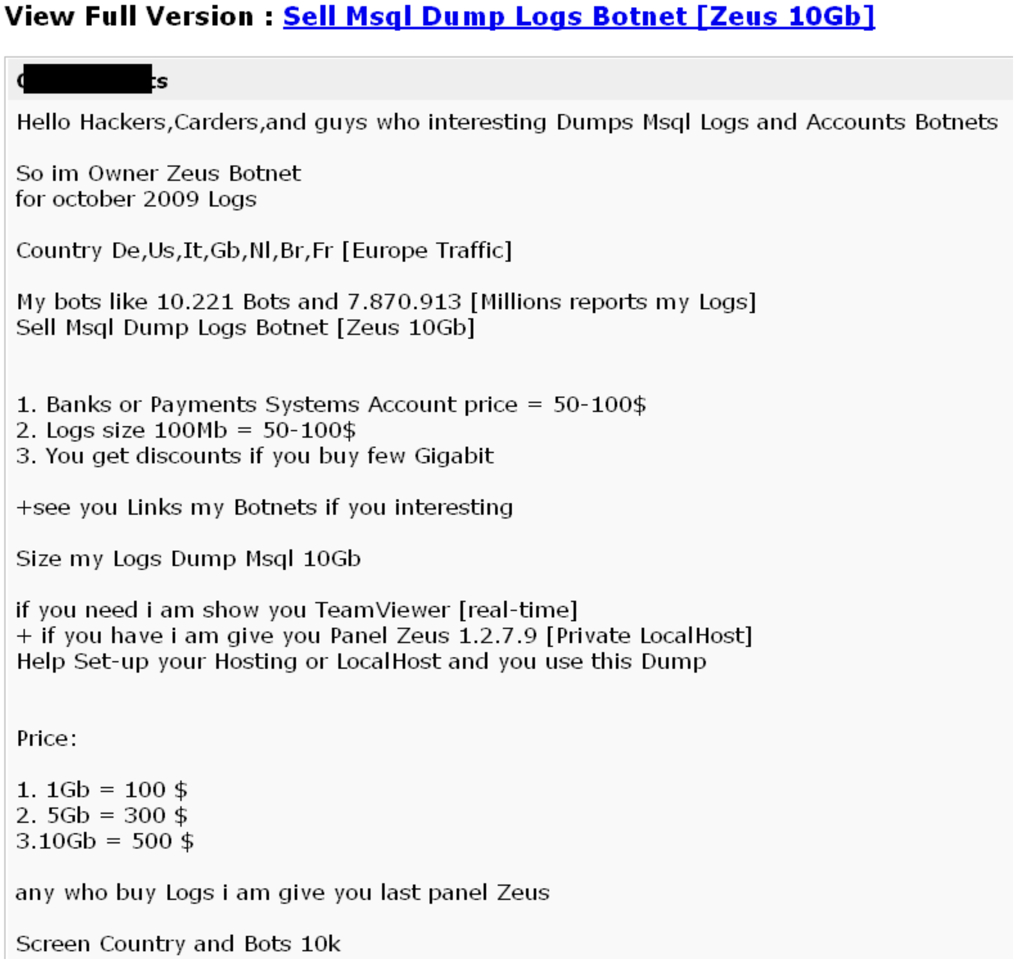
Accepted payments : Paypal - LR - WMZ

Discount for the first 5 customers : 7$ and 12$ on my own hacked site

I will setup it for only trusted members (+7 rep at least)

Dont spam my thread if ur not interested!

Zeus Databases for Sale on Underground Forum



View Full Version : Sell Msql Dump Logs Botnet [Zeus 10Gb]

[redacted]

Hello Hackers,Carders,and guys who interesting Dumps Msql Logs and Accounts Botnets

So im Owner Zeus Botnet
for october 2009 Logs

Country De,Us,It,Gb,Nl,Br,Fr [Europe Traffic]

My bots like 10.221 Bots and 7.870.913 [Millions reports my Logs]
Sell Msql Dump Logs Botnet [Zeus 10Gb]

1. Banks or Payments Systems Account price = 50-100$
2. Logs size 100Mb = 50-100$
3. You get discounts if you buy few Gigabit

+see you Links my Botnets if you interesting

Size my Logs Dump Msql 10Gb

if you need i am show you TeamViewer [real-time]
+ if you have i am give you Panel Zeus 1.2.7.9 [Private LocalHost]
Help Set-up your Hosting or LocalHost and you use this Dump

Price:

1. 1Gb = 100 $
2. 5Gb = 300 $
3.10Gb = 500 $

any who buy Logs i am give you last panel Zeus

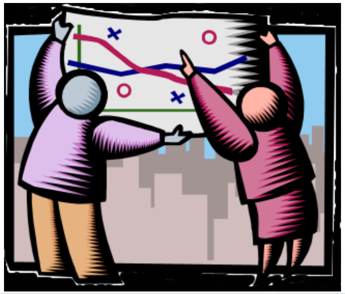
Screen Country and Bots 10k

- Zeus databases are sometimes sold in their entirety to 3rd parties.
- Prices from late 2009 are in the screenshot to the left.

How does this affect my organization?

User credentials can become compromised regardless of the effort put into password policies, pre-authentication web application security configurations, or anti-virus solutions.

- Due to the proliferation of Zeus and other trojans, if your organization is large enough there is a good chance that at least one set of credentials for an internet facing application has already been compromised.
- No amount of diligence will keep a zero day exploit from slipping in and executing a new/crypted variant of Zeus.
- Adobe PDF and Flash exploits continue to be popular zero day propagation technique because these formats are used by everyone and are constantly having new vulnerabilities discovered.



Sounds scary, what can I do?

Basic principles of web application security should be implemented on your sites. There should be a specific focus on the following post-authentication areas in order to help mitigate the impact of Zeus:

- Cookie handling / session management
- Privilege escalation
- Input sanitization
- VIEWSTATE encryption (for .aspx apps)
- Multifactor authentication (sometimes helps, but not always)

Focus on Privilege Escalation

Once credentials are compromised, the question then becomes:

How far can the attacker get once inside?

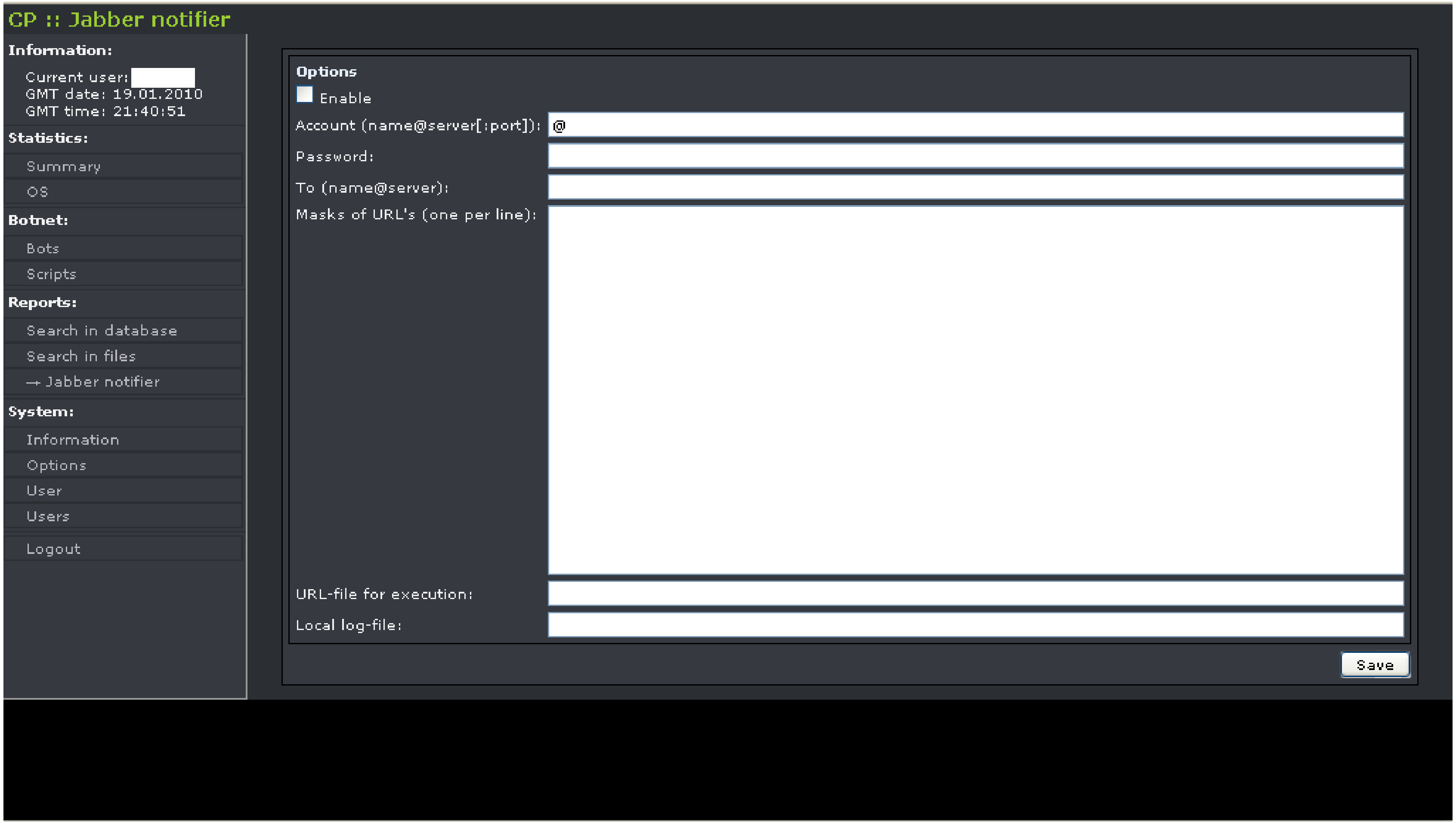
Diligence in making sure lower level users cannot forcefully access administrative areas or exploit unsanitized parameters is important in preventing the escalation of an attackers privileges.

Focus on Session Management

- Even one time use passwords are not safe from Zeus.
- Zeus grabs cookies, and an attacker can use these intercepted session identifiers to piggy back on legitimate sessions and gain access to the application and the user account.

- Enforce the rule of one user at a time. Do not allow the same user to be logged in with multiple sessions. This prevents an attacker from jumping on an active session while the user is signed in. New Zeus variants are utilizing Jabber for real time alerts to the botmaster.
- Web Apps should kill the cookie upon logout and enforce a timeout. This way, the attacker's window of opportunity for access dramatically shrinks.
- Never issue cookies pre-authentication.

Jabber Alert Panel



Current user: [redacted]
GMT date: 19.01.2010
GMT time: 21:40:51

Options

□ Enable

Account (name@server[:port]): @

Password:

To (name@server):

Masks of URL's (one per line):

URL-file for execution:

Local log-file:

PostAuth Input Sanitization

- Never forget the basics. Once an attacker is inside your application, make sure they are unable to make it error out through some kind of parameter tampering.
- SQL injection, XSS, etc., are still real possibilities once an attacker has gained access to the application.
- Even though the login and password change forms were sanitized, did you remember to sanitize that drop down menu?
- Use an automated vulnerability scanner against your application to check all your post-authentication inputs.
- Most of the time, attackers using Zeus are not skilled enough to pull off these advanced attacks. However, the possibility is still there.

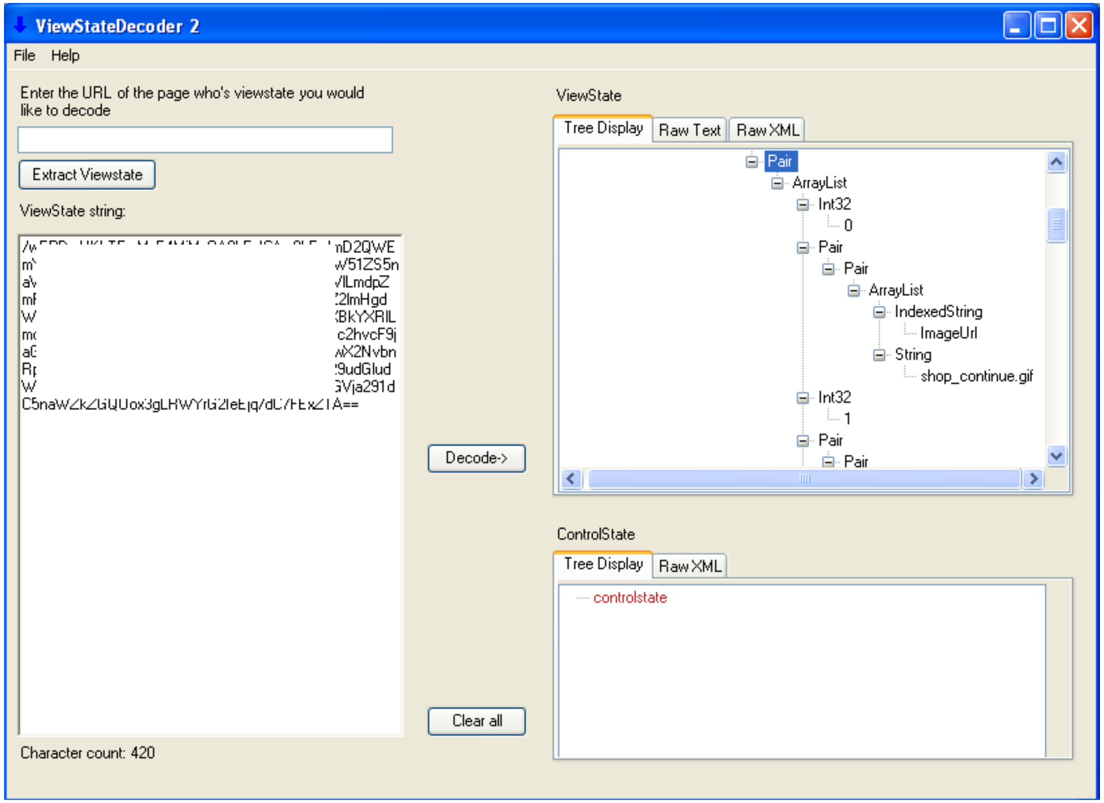
Note about VIEWSTATE

ASPX applications use VIEWSTATE parameters to pass along session data in POST requests.

- VIEWSTATE parameters are base64 encoded strings, and oftentimes contain information that can reveal information about the architecture of the application, and sometimes will even contain sensitive data such as logins or passwords.
- Simple Base64 decoding will reveal the content of VIEWSTATE parameters.
- .NET allows developers to encrypt VIEWSTATE, which should always be done. This prevents the reversal of Base64.

Note about VIEWSTATE

- VIEWSTATE parameters can be decoded with tools such as ViewState Decoder



Enter the URL of the page who's viewstate you would like to decode

ViewState string:

```
/w[redacted]nD2QWE
m`          w/51ZS5n
aV          VILmdpZ
mF          Z2lmHgd
W           3BkYXRIL
mc          c2hvcF9j
aG          wX2Nvbn
Rp          9udGlud
W           GVja291d
C5naWZkZGUQUox3gLRWYrG2IeEjq/dC7FExZ1A==
```

Character count: 420

```
Pair
  ArrayList
    Int32
      0
    Pair
      Pair
        ArrayList
          IndexedString
            ImageUrl
          String
            shop_continue.gif
    Int32
      1
    Pair
      Pair
```

```
controlstate
```

Note About MFA

- Zeus makes solutions like Multi Factor Authentication much weaker. MFA is more of a speed bump for an attacker using Zeus. It can slow them down, but not for long.
- The credentials needed for MFA are usually collected by the trojan, and Zeus also injects fake fields that ask for sensitive data (social security, mothers maiden name, PINs, place of birth, etc) on web forms.
- If an attacker gets tripped up by an MFA prompt, he usually only needs to examine the report for that infected machine to obtain correct credential.

Conclusion

- Focus on post-authentication web application security is vital because Zeus grabs everything it needs for initial access to the application.

- Specific focus on session management, privilege escalation, VIEWSTATE encryption, and input sanitization will go a long way in mitigating the threat posed by Zeus.

Resources

- Technical information about the workings of the Zeus payload and C&C:

http://blog.threatexpert.com/2009/09/time-to-revisit-zeus-almighty.html

- Resources for testing your web apps:

http://www.owasp.org/index.php/Category:OWASP_Tools_Project