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

Alexander Heid
Fabian Rothschild
1/27/2010
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 use the CVV data collected by Zeus for monetization purposes. Carders also resell the data.
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.
Script Kiddies are attracted to Zeus because of its 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: [blank]
GMT date: 21.01.2010
GMT time: 19:14:25

Statistics:
- Summary
- DE

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: 802
- 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 (436)

<table>
<thead>
<tr>
<th>GB</th>
<th>IE</th>
<th>GR</th>
<th>US</th>
<th>IN</th>
<th>ES</th>
<th>SF</th>
<th>CN</th>
<th>DE</th>
<th>ZA</th>
<th>CY</th>
<th>NL</th>
<th>IL</th>
<th>PL</th>
<th>BE</th>
<th>NO</th>
<th>AU</th>
<th>FR</th>
<th>ID</th>
<th>IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>551</td>
<td>36</td>
<td>27</td>
<td>26</td>
<td>14</td>
<td>13</td>
<td>13</td>
<td>10</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

Online (147)

<table>
<thead>
<tr>
<th>GB</th>
<th>IE</th>
<th>GR</th>
<th>US</th>
<th>IN</th>
<th>ES</th>
<th>SF</th>
<th>CN</th>
<th>DE</th>
<th>ZA</th>
<th>CY</th>
<th>NL</th>
<th>IL</th>
<th>PL</th>
<th>BE</th>
<th>NO</th>
<th>AU</th>
<th>FR</th>
<th>ID</th>
<th>IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>103</td>
<td>19</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
How does it work?

Sample Report File

<table>
<thead>
<tr>
<th>View report (HTTP request, 1.436 bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bot ID: j_10hjgfe25xbo_0009af7e</td>
</tr>
<tr>
<td>Botnet: btm</td>
</tr>
<tr>
<td>Version: 1.2.7.11</td>
</tr>
<tr>
<td>OS Version: XP Professional SP 3, build 2600</td>
</tr>
<tr>
<td>OS Language: 1036</td>
</tr>
<tr>
<td>Local time: 12.01.2010 21:00:00</td>
</tr>
<tr>
<td>GMT: +5:00</td>
</tr>
<tr>
<td>Session time: 01:22:22</td>
</tr>
<tr>
<td>Report time: 12.01.2010 02:09:22</td>
</tr>
<tr>
<td>Country: CA</td>
</tr>
<tr>
<td>IPv4: 2</td>
</tr>
<tr>
<td>Comments for bot: -</td>
</tr>
<tr>
<td>In the list of used: No</td>
</tr>
<tr>
<td>Process name: C:\Program Files\Internet Explorer\explore.exe</td>
</tr>
<tr>
<td>User of process: 1-10HJ3FE25XBOO0-c</td>
</tr>
<tr>
<td>Source: <a href="https://www.paypal.com/ca/">https://www.paypal.com/ca/</a></td>
</tr>
</tbody>
</table>
How does it work?

- Sample Report File (continued)
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 Zeus/MMP) is a malicious kit, which steals credentials from various online services like social networks, online banking accounts, FTP accounts, email accounts and others (phishing). The web admin panel can be bought for 700$ (source: RSA Security 4/21/2010) and the key builder for 490$ (source: Press 3/19/2010).

The Zeus malware contains the following pieces:

* A web interface to administrate and control the botnet (Zeus Admin Panel)
* A trojan to create the Zeus database and encrypt the config file (cracked key builder)

Primarily, Zeus most consists of these components:

* a config file (ready with username "168")
* a binary file which contains the password version of the config file

Some features of Zeus:

* Captures credentials out of HTTP, HTTPS, FTP, and POP3/IMAP traffic or out of the victim’s protected storage (Pipes).
* Bypass the victim’s defenses into different browsers
* Configured [POF02] 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**:
- Config v: 1.2.7.3
- Botnet for the spreading v: 1.2.7.7 with ahtmptools v: 1.0.7.11

I will do the setup on your own site or to a hacked site (you must have panel access + ftp)

Or

I can setup it on my own hacked sites (limited time offer) also you will get the ftp info + panel info

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

Accepted payments: PayPal 

Discount for the first 5 customers: 75 and 12$ on my own hacked sites

I will setup it for only trusted members (at least 5 registered)

Don’t spam my thread if you are not interested!
Zeus Databases for Sale on Underground Forum

View Full Version: Sell Msq1 Dump Logs Botnet [Zeus 10Gb]

Hello Hackers, Carders, and guys who interesting Dumps Msq1 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 Msq1 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 Msq1 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

Information:
- Current user: [username]
- GMT date: 19.01.2010
- GMT time: 21:49:51

Statistics:
- Summary
- OS

Botnet:
- Bots
- Scripts

Reports:
- Search in database
- Search in files
- Jabber notifier

System:
- Information
- Options
- User
- Users
- Logout

Options
- Enable

Account [name@server[port]]: [username]
Password:
To (name@server):
Masks of URL's (one per line):

URL file for execution:
Local log file:

Save
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.
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:
  

- Resources for testing your web apps:
  