Cybercriminals Target Online Banking Customers

Use Trojan and Exploit Kits to Steal Funds from Major UK Financial Institution

BACKGROUND

In July 2010, an organized network of cybercriminals launched a complex, multi-level scheme that targeted online customers of a large UK financial institution. Based on information M86 Security Labs found on the malicious Command & Control (C&C) server, we assume that close to £675,000 was stolen from the bank between July 5 and Aug. 4, 2010, and approximately 3,000 customer accounts were compromised. Exact figures are being verified at this time.

The M86 Security Labs malware team detected this illegal operation after discovering a malicious code attack used to infect users’ PCs with a Trojan. The team then followed the trail to the Command & Control center. According to our research, these cybercriminals used a combination of the new Zeus v3 Trojan and exploit toolkits to successfully avoid anti-fraud systems while robbing bank accounts.

This indicates a new level of technical sophistication and signals the continuation of a cybercrime trend that has evolved since our last report, URLZone/Bebloh Trojan Banker. Two years ago, M86 Security Labs identified Zeus, which became one of the most popular Trojans used by cybercriminals. Today, the latest iteration, Zeus v3, not only acts a data collector -- it also performs illegal online banking transactions.

In this report, we will expose the architecture, business model, tools and methods used by this cybercriminal organization.

THE ATTACK

Multiple techniques were used to spread malicious code to as many systems as possible within the UK with the ultimate goal of targeting online customers of a specific bank. These techniques included:

- Infecting legitimate websites with malware
- Creating fraudulent online advertisement websites
- Publishing malicious advertisements among legitimate websites

The cybercriminals used the Eleonore Exploit Kit and the Phoenix Exploit Kit (located on the same server), both of which are notorious for efficiently exploiting victim’s browsers to install Trojans onto their PCs.

Once the Zeus v3 Trojan successfully installed on victims’ PCs and after the victims logged into their online bank accounts, the Trojan initiated the money transfer from their accounts, via money mules, to the cyber-thieves. Using various techniques, the Trojan remained under the radar of common anti-fraud detection systems. It appears that the C&C server was hosted in Eastern Europe.
Cybercriminals Target Online Banking Customers

Figure 1: Flow of the Attack

1. Uploads malicious advertisements to legitimate and fraud advertisements servers
2. The malicious advertisements published among the legitimate websites
3. User accesses to an infected website
4. The website content contains redirection to the malicious Exploit Kit
5. The user is redirected to the malicious Exploit Kit
6. The user’s PC exploited, the payload was downloaded successfully
7. The Trojan reports for a new bot to the C&C
8. The C&C sends instruction to the Trojan
9. User access to financial institution
10. The Trojan reports for the user activities
11. The C&C sends commands to the Trojan to manipulate user bank transactions
12. Trojan manipulates User’s bank transaction
13. Trojan reports the C&C about successful/failed transaction
SPREADING MALWARE: EXPLOIT KITS

An exploit kit is a Web application that serves multiple exploits through browsers (Internet Explorer, Firefox and Safari) or applications (JAVA, Flash and PDF) to a victim’s system. The owner of the exploit kit can control what is served to a victim’s PC and monitor the results of the attack. Today, cybercriminals can easily buy these kits, including Phoenix Exploit Kit, Siberia Exploit Kit, and the Eleonore Exploit Kit for a few hundred dollars.

In this case, the cybercriminals used the Eleonore Exploit Kit 1.4.1, which M86 Security Labs experts researched a year ago and continue to update regularly.

The Eleonore Exploit Kit includes exploits for the following vulnerabilities:

- IE MDAC Vulnerability - [CVE-2006-0003](#)
- Adobe Reader Collab GetIcon Vulnerability - [CVE-2009-0927](#)
- Adobe Reader CollectEmailInfo Vulnerability - [CVE-2007-6653](#)
- Adobe Reader newPlayer Vulnerability - [CVE-2009-4324](#)
- Java Development Kit Vulnerability - [CVE-2008-5355](#)
- Java Web Start Vulnerability - [CVE-2010-1423](#)
- Social Engineering Attack – Requires the user to download and execute the payload
Administration Panel
In addition to the included exploits, the author of the toolkit enables his customers to review and analyze incoming traffic.

<table>
<thead>
<tr>
<th>Operation Systems:</th>
<th>Totals:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>121582</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>105600</td>
</tr>
<tr>
<td>Windows 7</td>
<td>5626</td>
</tr>
<tr>
<td>Mac OS</td>
<td>9851</td>
</tr>
<tr>
<td>Linux</td>
<td>559</td>
</tr>
<tr>
<td>Power PC</td>
<td>312</td>
</tr>
<tr>
<td>PlayStation</td>
<td>208</td>
</tr>
<tr>
<td>Windows 2000</td>
<td>204</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>205</td>
</tr>
<tr>
<td>Windows 98</td>
<td>80</td>
</tr>
<tr>
<td>Beta</td>
<td>53</td>
</tr>
<tr>
<td>Unknown OS (1)</td>
<td>27</td>
</tr>
<tr>
<td>Symbian OS</td>
<td>22</td>
</tr>
<tr>
<td>Ninendo Wii</td>
<td>7</td>
</tr>
<tr>
<td>Windows NT 4</td>
<td>2</td>
</tr>
<tr>
<td>iPhone OS</td>
<td>1</td>
</tr>
<tr>
<td>SunOS</td>
<td>1</td>
</tr>
<tr>
<td>Windows ME</td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure 3:** Exploit statistics organized by the operating system of the incoming machines and amount of successful exploits divided by the exploit’s name

<table>
<thead>
<tr>
<th>Exploit</th>
<th>Loads:</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>1</td>
</tr>
<tr>
<td>S0206dmac</td>
<td>2</td>
</tr>
<tr>
<td>S0206dmac</td>
<td>2</td>
</tr>
<tr>
<td>_new</td>
<td>53</td>
</tr>
<tr>
<td>_geticon</td>
<td>155</td>
</tr>
<tr>
<td>_email</td>
<td>255</td>
</tr>
<tr>
<td>midac</td>
<td>1468</td>
</tr>
<tr>
<td>...</td>
<td>2492</td>
</tr>
<tr>
<td>java_gpl</td>
<td>10033</td>
</tr>
<tr>
<td>x11f</td>
<td>17557</td>
</tr>
</tbody>
</table>

**Figure 4:** Incoming traffic from websites

Typically, the “Referer” column includes a list of infected sites used to redirect users to the exploit kit. In this case, most of the incoming traffic was delivered through malicious advertisements. Fraudulent advertisement sites are marked in red, and legitimate sites that have been infected are marked in blue. For example, “yieldmanager.com” is operated by Yahoo.
The Eleonore Exploit Kit also enabled the controller to view the source locations of victims’ machines. The following screenshot proves that this is a professional cybercriminal network whose goal was to steal money using online banking accounts. The victims’ PCs were located in Britain, which was relevant to the next step of the crime.

<table>
<thead>
<tr>
<th>Country</th>
<th>Traffic</th>
<th>Loads</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>GB</td>
<td>287685</td>
<td>36802</td>
<td>12.79%</td>
</tr>
<tr>
<td>RU</td>
<td>75</td>
<td>5</td>
<td>6.67%</td>
</tr>
<tr>
<td>US</td>
<td>37</td>
<td>14</td>
<td>37.84%</td>
</tr>
<tr>
<td>IE</td>
<td>22</td>
<td>4</td>
<td>16.10%</td>
</tr>
<tr>
<td>DE</td>
<td>7</td>
<td>5</td>
<td>71.43%</td>
</tr>
<tr>
<td>NL</td>
<td>5</td>
<td>1</td>
<td>20.0%</td>
</tr>
<tr>
<td>JP</td>
<td>5</td>
<td>3</td>
<td>60.0%</td>
</tr>
<tr>
<td>CN</td>
<td>4</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>FR</td>
<td>2</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>BR</td>
<td>1</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>PE</td>
<td>1</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>PS</td>
<td>1</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>SA</td>
<td>1</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>SG</td>
<td>1</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>NC</td>
<td>1</td>
<td>1</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

Figure 5: Fraud advertisement website used by the cybercriminals

Figure 6: Statistics of incoming traffic divided by country
To generate this much traffic from one country, we can assume, according to the referrer’s panel, that the malicious advertisements and infected websites were located within the UK.

Because the infected pages delivered by the Phoenix and Eleonore Exploit Kits are well-obfuscated, it was difficult to detect them through antivirus technology alone. This is evidenced in Figure 7, which shows that only a few anti-virus vendors would have detected the exploit.

REPORTING: ZEUS v3 TROJAN

After the exploit kit successfully downloaded to the victim’s machine, it began to communicate with its C&C server.

The screenshot above shows the Trojan communicating with the C&C. Once the new configuration file was retrieved, the Trojan monitored specific online banking sites and reported to the C&C server. In this attack’s configuration file, the cybercriminal targeted one bank.

This Zbot/Zeus v3 version is an evolved mutation of Zbot 2. Unlike the older version, this one focused specifically on online banking. The malware began reporting to a different C&C server once the user accessed the desired bank.
After the user logged in to his personal banking account, it appears the Trojan transferred the login ID, date of birth, and a security number to the C&C server. The system processed the incoming data and exported it into a log file along with the victim’s machine IP:

```plaintext
11-07-10 03:39:31
Log: XXXXXXXXXXX MemAnsw: NNNNNNN Psw: MMMMM
```

Figure 9: VT results 5/42 -- only three vendors find this malware as Zbot

After the user logged in to his personal banking account, it appears the Trojan transferred the login ID, date of birth, and a security number to the C&C server. The system processed the incoming data and exported it into a log file along with the victim’s machine IP:
Once the user accessed the transactional section of the site, the Trojan reported to the C&C. It then received new JavaScript code to replace the original bank JavaScript that was used for the transaction form.

```php
if (!isset($_REQUEST['init']) || empty($_REQUEST['init'])) {
    if ($REQUEST['id'] === 'GB' || $REQUEST['id'] === 'NL') {
        if (!$_REQUEST['init'] == 'd') {
            header("Location: get_dr.php?e=".$_REQUEST['e']);
            exit;
        }
        if ($_REQUEST['init'] == 'i') {
            header("Location: get_inf.php?e=".$_REQUEST['_execv']);
            exit;
        }
        if (preg_match('/https?:///\w+/.*/i', $referer)) {
            if ($_REQUEST['init'] == 'i') {
                if ($browser == 'IE')
                    include("./resources\_ie.js");
                if ($browser == 'FF')
                    include("./resources\_ff.js");
            } else {
                include("404.html");
            }
            exit;
        }
    }
}
```

Figure 10: The code that sends new JavaScript for the bank transaction form

After the user submitted the transaction form, the relevant data was sent to the C&C system instead of the bank.

Figure 11: HTTP log -- the requests committed by the Trojan from the victim machine to the C&C system

The Trojan's activity, noted in red in the screenshot, shows encrypted data being sent to the C&C system. The system analyzed and decrypted the information sent by the Trojan.

```php
function hor_decode($str) {
    $result = "";
    $str = explode(';', $str);
    foreach ($str as $char) {
        $result .= chr($char / 3);
    }
    return $result;
}

$str = explode("&", hor_decode($_REQUEST['e']));
```

Figure 12: Decryption algorithm of the data
After analyzing the data, the system determined whether the user had enough money in the account. It selected the most appropriate mule account to retrieve the money, wrapped all the data, and sent it back to the Trojan installed on the victim's machine.

The Trojan then updated the data in the form and sent it to the bank to complete the transaction. The bank received the requested operation and sent back the transaction result as the Trojan continued to listen to the bank response, reporting it to the C&C system.

Figure 13: HTTP log -- the Trojan reports the result of the transaction committed by the user

```plaintext
country=YYYY
block=1
content=YYYY::AANNNNNNNNNN::AAAAAAAAAA::XXXXXXXXX::YYYYYYYY::jot::806.04
inf=Firefox

Holder Info: SOMENAME XX-YY-ZZ XXXXXXXX
```

Figure 14: The system updated the transaction result in the database
COMMAND & CONTROL MANAGEMENT

Stealing money from a major financial institution by exploiting customers’ online transactions is a complex operation. It requires a professional cybercrime business model, for which each individual has a specific role. Members operate simultaneously and use money mule accounts to transfer the funds from compromised accounts. Using the administration panel, the operator could manage each team member in the group.

![Money mule tab screenshot](image)

Figure 15: Nicknames of gang members controlled by the manager

![Money mule account list screenshot](image)

Figure 16: A list of the money mule’s account, including the money each account holds and the member of the network who stole it

The screenshot above displays the money mule tab, where the manager adds new money mule accounts, including the minimum/maximum amount to transfer to those accounts, and the operator of each money mule.
The “Robin Hood” system in the screenshot above enabled the manager to define how much money to transfer from the compromised bank accounts to the money mule’s account. The system only stole money from accounts that held more than a specified amount of money.

**Communication with the Banking Command & Control System**

Unlike the older version of Zeus, this new Trojan communicated with HTTP over SSL.

**MONEY MULES**

Money mule accounts are legitimate banking accounts controlled by valid bank users. These users are typically unsuspecting middlemen who transfer stolen money from one country to another to muddle the cybercrime trail. Money mules aren’t aware that the money they deliver to cybercriminals is stolen from compromised bank accounts.

Cybercriminals recruit money mules by posing as legitimate companies that hire them as employees. They ask their “employees” to transfer received money from their bank account to a different account which is related to the fraudulent company. And they do not use non-banking transactions, such as Western Union, to transfer money.

To avoid warning signs by anti-fraud systems, the money mule accounts are only used a few times within a certain timeframe. Since banks monitor large transfers, the amount of money deposited in a money mule account is predefined in an effort to elude detection.
TRANSACTIONS

In this case, the controller monitored each transaction performed within the compromised bank accounts, the amount of money delivered to money mules, and the status result reported by the bank.

For example, the controller could see the third transaction result that stated, “Your payment has been sent and will be credited to the beneficiaries account immediately, subject to our normal fraud checks.”

CONCLUSION

Because cybercrime is a lucrative business, illegal operations such as the one discussed in this paper are on the rise. These criminals continuously seek new, sophisticated ways to steal information and money without detection. And it’s increasingly difficult for security companies to stay ahead of the proliferation of new, dynamic malware.

In this scenario, the M86 Security Labs malware team detected the crime because a potential victim used our secure Web gateway solution, which proactively prevents emerging threats in real time. It’s the only effective way to protect users and organizations from today’s sophisticated attacks via the Web.

Immediately after the discovery, M86 Security representatives informed the relevant law enforcement agencies of all criminal activities and methods used by the perpetrators.
ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry’s leading Secure Web Gateway provider. The company’s appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

ABOUT M86 SECURITY LABS

M86 Security Labs is a specialized global team of security experts and researchers who detect current and emerging Web and email threats and mitigate them quickly. By using data feeds from the Internet security community and internal intelligence gathered from M86 Security customers and products, the team analyzes information and provides comprehensive, always-adapting defense against email and Web threats. In addition, M86 Security Labs provides zero-day protection to its customers, securing them from new exploits the day they’re discovered.