

The New Frontier For Zeus & SpyEye

By Ryan Sherstobitoff

Join the Discussion
Connect

The author's research into Zeus/SpyEye banking Trojans demonstrates the sophistication of the malware and reveals that cybercriminals are now targeting smaller financial institutions such as local/regional banks and credit unions.

Abstract

This research will discuss the most recent adaptations used by cybercriminals when deploying variations of Zeus/SpyEye. New research conducted into the modus operandi and some of the differences between variants reveals sophisticated operations now focusing on a smaller segment of the financial services market.

Community and regional banks and credit unions have come under the recent focus of Zeus and SpyEye banking Trojans.¹ These malware families are no longer targeting the Bank of Americas of the world. Instead there is a dramatic shift in the type of targets fraudsters are going after. There are many Zeus/SpyEye variations deployed by fraudsters that target community-style banks, the really small banks that serve a local city as opposed to larger financial institutions.

I conducted research into many different versions of Zeus/SpyEye over a period of six months to answer several key questions:

- What are the targets that Zeus/SpyEye primarily focus on now?
- What is the exact process that these criminal operations follow to extract funds from victim accounts? How do they remain hidden?
- What kind of forensics evidence is available to detect their presence from a log-collection standpoint?

The data collected was in collaboration with several leading security firms along with a couple boutique forensics shops all derived from sensor networks and other proprietary collection methods. The following data were analyzed:

1. Zeus/SpyEye configuration files: decrypted, decompressed, and analyzed for target data (triggers)
2. Configuration files from many different in-the-wild samples: analyzed to determine evidence indicating the criminal's exact process in stealing funds from victim bank accounts
3. Credential drop zone log files: retrieved to determine the type of data stolen and from which particular financial institution
4. Botnet drone data: collected and analyzed to understand the scope and size of these malware families

¹ <http://about-threats.trendmicro.com/Search.aspx?language=us&p=calbanktrust.com>.

The trend is that more fraud cases will occur in the lower end of the financial services market. There are a couple of reasons for this and why this strategy is working:

- Smaller banks are less likely to employ multi-factor, strong authentication (Figure 1).
- Smaller banks run common identifiable banking platforms with very little customization, making large scale generic attacks workable without much effort on the part of the fraudster.
- The larger banks have been a constant target for years; the strategy now is to focus on smaller banks that have fewer resources to combat fraud.

The image shows a web form for logging into a bank account. It has two input fields: 'ID' and 'Password'. Below the 'Password' field is a blue 'Login' button. To the right of the 'Password' field is a blue link that says 'Reset Password'.

Figure 1 – Authentication scheme used by a small city bank in Arkansas

The banks observed in this research, according to evidence analyzed, will target two countries primarily when speaking about community-style banking: the USA and Australia. Zeus/SpyEye variants discovered contain evidence that in their configuration files fraudsters are creating custom triggers to target the lower end of the market.²

For example several variations of Zeus contain custom triggers (target data) for smaller banks³ such as:

- [...] Citizens Bank
- [...] Bank & Trust
- First [...] Bank & Trust

Infection life cycle

1. Hackers distribute popular exploit kits such as the Phoenix Exploit kit.⁴
2. Hackers poison legitimate advertisements, search results, or other web content that re-directs users to the exploit kit.
3. User visits or views a page containing malicious advertisement(s).
4. The malicious advertisement has code to call the script from the hosted exploit kit or simply redirect the user to a web page hosting it.
5. The kit exploits a known or zero-day vulnerability in the user's browser, allowing for remote execution of arbitrary code.
6. Zeus or SpyEye is downloaded and installed on the user's PC.

2 Editor's note: Institution names and URLs found in the malware files have been sanitized for confidentiality. The fourth directive of the ISSA Code of Ethics states: "Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities." Rest assured that the findings presented in this article are true and have been verified.

3 Trend Micro Virus Encyclopedia - http://about-threats.trendmicro.com/malware.aspx?language=us&name=TSPY_ZBOT.WHZ - click "Technical Details."

4 <http://blog.trendmicro.com/now-exploiting-phoenix-exploit-kit-version-2-5>.

7. The malware contacts the command and control server (C&C) for the first time and retrieves the configuration file, usually config.bin.
8. The malware remains dormant until the user visits one of the pages specified by a trigger in the configuration file. For example if a user visited one of these URLs (institutions mentioned above), the malware would activate:
 - [https://www.\[...\]citizensbank.com/olbb/_Tlogin.asp](https://www.[...]citizensbank.com/olbb/_Tlogin.asp)
 - [https://banking.\[...\]banktrust.com/iLogin.jsp](https://banking.[...]banktrust.com/iLogin.jsp)
 - [https://cbs.firstfirst\[...\].com/cb/servlet/cb/login-fcbnc.jsp](https://cbs.firstfirst[...].com/cb/servlet/cb/login-fcbnc.jsp)
9. Depending on the configuration file, the malware will usually grab the username and password as the user logs in.
10. The credentials are sent via an encrypted HTTP POST back to the C&C server drop zone where they are stored for later retrieval by hackers.
11. Hacker can take over the account now.

Configuration file

The configuration file – the heart of Zeus/SpyEye – will determine specifically what targets to hit in addition to containing JavaScript code that will tell the malware how to steal the information. This file is built using the toolkit to create the infection binary, and targets are often custom defined by the fraudster before deployment to victims. Also keep in mind the configuration file is encrypted and the decryption key is unique per C&C server, therefore, making analysis of such data difficult for researchers. These triggers are being defined by the fraudster to steal information such as usernames, passwords, etc. In some cases you will see specific pages referenced in the URL such as *balances*, which indicates the malware intends on grabbing the balance and storing it in its cache. Zeus uses the stored balance details to inject into the same page at a later time to persistently hide the fact that money was fraudulently transferred from the user's account. The configuration file can be updated dynamically by the C&C server to hit other pages or to add new custom triggers.

This reference is evidence that this particular variant likely uses a process known as the Automatic Transfer Mechanism or Transaction Modification (ATM)⁵ (see below for detailed discussion). This is where the malware automatically changes the recipient information in real time on a funds transfer so it ultimately ends up in the criminal's account as opposed to the intended recipient.

Three credit unions targeted in a variant of malware contained account balance pages as the target to activate what is known as the balance grabber module, which exists in both Zeus and SpyEye as a component.⁶ In addition there were a total of 64 variants of both Zeus and SpyEye combined that contained a reference of some kind targeting the balances

5 http://www.securelist.com/en/blog?print_mode=1&weblogid=155.

6 http://viewer.media.bitpipe.com/1039183786_34/1295279253_317/CYBRC_WP_0111-RSA.pdf.

page of a particular bank, for example, [https://cuonline.\[...\].org/\[...\]/hbnet/accountinfo/balances.aspx](https://cuonline.[...].org/[...]/hbnet/accountinfo/balances.aspx)^{*}. This is out of a total sample bed of several thousand malware variants. The data indicates a unique focus towards particular data-grabbing mechanisms such as account balances.

Furthermore, because Zeus/SpyEye uses the stolen balance information to inject a fraudulent amount as the means of hiding the fact the account holder was a victim, this is probable evidence that these variants employ automatic transaction modification. Also, you will see that triggers for Bank of America and Wells Fargo still remain, but these are known to be what is called default triggers and in many cases were not intentionally added by the fraudster – these come with the purchase of the crimeware kit.

During my research evidence was uncovered in the configuration files from a number of in-the-wild samples that these families target even the most obscure financial institutions. Normally you would not find custom triggers for these smaller institutions as you would for Wells Fargo; rather they will be attacked generically through a platform services provider that hosts the web application in a datacenter environment.

Hacking the platform

You will usually find that smaller financial institutions will be running a common banking platform as opposed to an “in house” solution that will be also used by a number of other banks. The software is custom branded⁷ as far as the bank’s look and feel and is usually hosted in a data center environment maintained by the platform provider. In some cases larger banks will host the application in their own environment, but that depends on the provider and the bank.

When fraudsters decide to attack the platform, they do this by creating custom triggers that target the authentication system in a way that allows them to bypass or simply steal the credentials. This way the fraudsters can perform a generic attack against the software platform to capture login credentials for hundreds of different banks that all run on the same system.

The banks that run these platforms will allow for users to enter their ID on the main website (Figure 2), just like Wells Fargo does, but ultimately will be re-directed to a common login page to enter their password in (Figure 3). This login page will be branded for that particular bank as far as the logo is concerned, but the general layout is all defined by a CSS file.

Figure 2 – Login ID field on main website

Figure 3 – Common authentication page the user is redirected to running on a common URL

Trigger URLs used by Zeus to generically target banks running the online banking software:

- https://*.ebanking-services.com*SignIn.aspx
- http://*/onlineserv/CM/*

The “generic” attack works by activating an html form grabber to steal the username and password as soon as the user lands on the authentication page.

The URL is formatted in such a way that it does not matter if it contains a unique ID to identify the bank, since the domain is the same and the use of a wildcard in place of actual characters will allow for the malware to directly target the authentication page. The username and password will still be stolen and sent to a drop server.

Here is an example of the URL formatting commonly used by one leading manufacture of online banking software. This URL is formatted in a way that it includes the following pieces of information that make up access to the platform; in this case it’s a business banking platform:

- Bank name
- Banking platform domain (ebanking-services.com)
- Sign-in page for authentication (BeB.SignIn.aspx?)
- A bunch of randomized data that serves as an identifier

[https://\[...\].bank.ebanking-services.com/Auth/SignIn/BeB_SignIn.aspx?auth_data=JjNTUSM30PVZEXVplhBlqmOphp0%3d%3aacQP9MA2gaJipVdB6mX2GDOsRH3uJDyUHL EYoEyFFFTL0Xf3j0T5Bf9DdMZKE6t2iwpr%2fxcyrssueb97luNyFc5Gupd8BF5gk4jPAKksiVSccePJS1BBfzQmDZZ5D6-Oh1UNPzcwFyoa%2fXyhyFLtSKSOuvjzOi6Ynp96xwEavbmKjQJNh2Mj%2fMY3leSsyRzhincYFkGBOKnCwWPSTMzGyIc3It0m6VAPi7leGh0hwyXNAK7kcevUcxBhAcyjR0-CgQmguDJAeuMprVYZgL7KKT8DSw65j%2bMsT3H4TBJ9MZ8zg5Pp%2bAMxsUvjyDC9nFzOmMN%2fB6ngR9g6z%2bEzvxVoL70IYyDMxQvWdfrjGYSVM4mDDolgLoISCs9RWzIYk8nZZ8QX7AtHePKvit9OoCIZiSx3L28j%2b5%2bsXXsgGM%2fMUn9C%2ftWaogG](https://[...].bank.ebanking-services.com/Auth/SignIn/BeB_SignIn.aspx?auth_data=JjNTUSM30PVZEXVplhBlqmOphp0%3d%3aacQP9MA2gaJipVdB6mX2GDOsRH3uJDyUHL EYoEyFFFTL0Xf3j0T5Bf9DdMZKE6t2iwpr%2fxcyrssueb97luNyFc5Gupd8BF5gk4jPAKksiVSccePJS1BBfzQmDZZ5D6-Oh1UNPzcwFyoa%2fXyhyFLtSKSOuvjzOi6Ynp96xwEavbmKjQJNh2Mj%2fMY3leSsyRzhincYFkGBOKnCwWPSTMzGyIc3It0m6VAPi7leGh0hwyXNAK7kcevUcxBhAcyjR0-CgQmguDJAeuMprVYZgL7KKT8DSw65j%2bMsT3H4TBJ9MZ8zg5Pp%2bAMxsUvjyDC9nFzOmMN%2fB6ngR9g6z%2bEzvxVoL70IYyDMxQvWdfrjGYSVM4mDDolgLoISCs9RWzIYk8nZZ8QX7AtHePKvit9OoCIZiSx3L28j%2b5%2bsXXsgGM%2fMUn9C%2ftWaogG)

So, for example, wildcards are used in this case to allow the Trojan to intercept any variation of the URL as long as it adheres to the common base URL. So far the success rate of these triggers being used in malware to target online banking platforms has been quite good, according to the data recovered from over a dozen Zeus drop zones during my research.

Over a course of two months a leading online banking platform was observed to be the target of fraudsters; however, fraudsters have been using triggers targeting online banking

⁷ <http://www.fisglobal.com/products-ebanking>.

platforms in Zeus variants dating back to 2010.⁸ During this two-month monitoring period credentials from 179 account holders were recovered from over a dozen malware drop zones across the world. Additionally 130 unique banks ranging from small town local community banks to national state banks were affected by Zeus between June and July 2011.

Here is another example of a recent Zeus malware variant targeting local city and state banks:

- MD5: ba03ce21f64c265a7fcfcf448b947037
- Date discovered: August 4th, 2011
- Targets: [...] Citizens Bank, [...] Bank & Trust, First [...] Business Banking.

Furthermore, an analysis was performed against numerous Zeus/SpyEye samples found in the wild to determine the distribution ratio that target community banks (Figure 4). This data was compiled from a number of in-the-wild samples derived from Trend Micro Labs, which maintains active lists of various targets⁹ that came from the configuration files. The data clearly shows that these smaller brands are being targeted often by sophisticated malware that have the capabilities of performing automatic transfers of funds out of the victim's account.

I also analyzed the data to determine the rate in which the actual online banking platform was being targeted generically.¹⁰ The analysis resulted in clearly showing that each platform found in the market had some form of generic attack against it – meaning there was evidence amongst the encrypted configuration files that contained triggers customized to affect any bank that uses that platform to run their online banking. However, you will notice in Figure 5 that some brands were targeted more often than others; this is likely due to popularity amongst financial institutions.

Zeus automatic transaction modification

Zeus has the capability to modify transactions in real time for any type of account from credit unions, regional banks, etc. In the configuration file, it is specified how the injection will occur and what the injected contents will look like when displayed to the user. In the cases of injecting fraudulent balance information, only certain areas of the page are modified.

Distribution of malware targeting Credit Unions, Community and Regional Banks by frequency of appearance

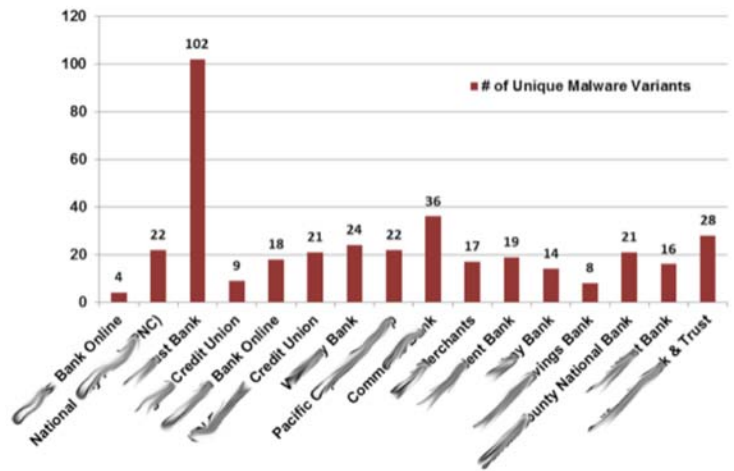


Figure 4 – Distribution of malware variants targeting community type banks

Distribution of Online Banking Platforms Targeted by Malware

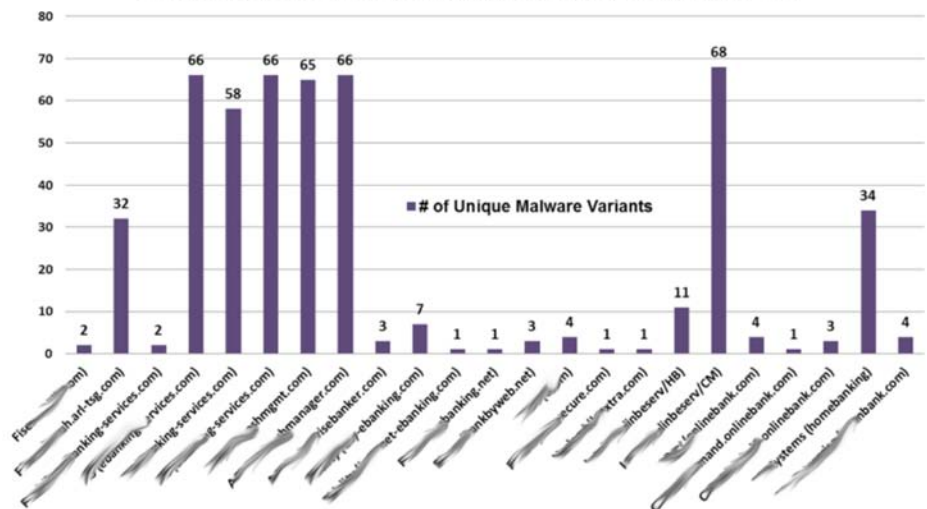


Figure 5 – Distribution of malware variants targeting online banking software

Furthermore, the hackers use exploit kits such as the Phoenix kit¹¹ to exploit the user's browser and install the Trojan. The Pphoenix exploit kit is a popular toolkit amongst hackers that comes with many pre-defined exploits that are usually known. This methodology combined with publishing advertisement content will allow for Zeus to target specific populations that the targeted financial institution serves.

The injection techniques used in Zeus are advanced and do not require much customization as far as how the transaction modification occurs. When performing injections, Zeus does not need to know the literal path of the target page it wishes to modify – that is why you will see partial URLs with the use of a wildcard in the configuration files:

- [https://onlineaccess.\[...\]org/login.aspx*](https://onlineaccess.[...]org/login.aspx*)

8 http://about-threats.trendmicro.com/malware.aspx?language=us&name=TSPLY_ZBOT.BFS.
 9 <http://about-threats.trendmicro.com/Search.aspx?language=us&p=calbanktrust.com>.
 10 Trend Micro Virus Encyclopedia – <http://about-threats.trendmicro.com/ThreatEncyclopedia.aspx?language=us&tab=malware>.

11 <http://labs.m86security.com/2011/06/phoenix-exploit-kit-2-7-continues-to-be-updated>.

Read the Headlines...



Don't BE the Headlines!

Security Awareness Incorporated delivers a full line of security awareness training tools to help make your employees a front line of defense. Call us today to discuss an effective and affordable program for your organization.

PCI DSS training courses also available!



www.securityawareness.com

1-888-807-0888

sales@securityawareness.com

AWARENESS IS THE KEY TO SECURITY®

ISSA member discounts

- [https://secure.\[...\].com/\[...\]WebClient/accountList.do*](https://secure.[...].com/[...]WebClient/accountList.do*)
- [https://is2.\[...\]net/mvpamp/*](https://is2.[...]net/mvpamp/*)
- https://*/efs/servlet/efsonline/myprofile.jsp*
- [*\[...\]reserve.com/EN/customer/account/](*[...]reserve.com/EN/customer/account/)
- [https://banking.first\[...\].com/efs/servlet/efs/jsp-ns/auth-login2.jsp*](https://banking.first[...].com/efs/servlet/efs/jsp-ns/auth-login2.jsp*)
- [https://www.\[...\]tbank.com/ibank1/forwardFromJspToLogonManager.do?SubmitTimestamp=*](https://www.[...]tbank.com/ibank1/forwardFromJspToLogonManager.do?SubmitTimestamp=*)
- [https://online.\[...\]com/*servlet/efs*](https://online.[...]com/*servlet/efs*)

This is accomplished via the use of a regular expressions library used within the Trojan code, thus, allowing for precise injection into exact pages, regardless of the URL. It either will occur automatically as soon as users logs into the session, or during the exact moment they initiate a transaction themselves. Either way, Zeus has become very effective at facilitating both retail and Automated Clearing House (ACH) fraud.

A note on HTML injection

The injection methods used by Zeus are advanced and appear seamless to the user. The following are some details about how this operation works.

Zeus form grabber functionality can grab certain data from very specific pages without needing to inject or alter the page. This allows the malware to grab account balances and other user information such as displayed account numbers.

A regular expressions library adds the flexibility to target many more banks in a single attack. The malware does not need to know the precise URL associate with the bank; rather the regular expressions it uses will be sufficient.

Both of these transaction modification techniques are very difficult to detect as fraudulent information is injected continuously to hide the fact that theft has occurred. Zeus leaves almost no forensics evidence to aid investigators.

User-Initiated transaction modification

1. The user logs into his bank.
2. The login information is stolen and sent to the C&C server.
3. The malware then
 - Grabs the account balance and sends it to the C&C server;
 - Uses a Perl regular expressions library to select the target page to inject into; in this case it will be the ACH/EFT or wire transfer page;
 - Waits for the user to click 'Submit' on the transfer page after details are completed;
 - Grabs the user's intended transfer amount;
 - Freezes the session: does not allow for the transaction to be sent to the online banking platform;

- Injects a fake page to make the user think that it's taking a little extra time to load the transfer confirmation page, a method to avoid suspicion;
- Makes a call to the C&C server and retrieves information regarding an appropriate mule (criminal recipient) account that can be used;
- Injects the mule account information and alternate transfer amount into the corresponding fields in the HTML POST;
- Releases the session, allowing the modified transaction to be sent to the online banking platform to be processed; and
- Injects a fake balance into the *Account Balances* and or *Account Summary* pages showing the user's amount deducted when in fact the amount was much more, which is hidden by the malware.

Automatic transaction modification (happens in less than a minute):

1. The user logs into his bank.
2. The login information is stolen and sent to the C&C server.
3. The post-login page is not loaded immediately. Zeus injects a fake page to make the user think that it is taking a little extra time to load with messages such as "updating" or "loading, please wait"; while this process takes place the remaining steps occur.
4. The malware then
 - Grabs the account balance and sends it to the C&C server;
 - Uses a Perl regular expressions library to select the target page to inject into; in this case it will be the ACH/EFT or wire transfer page that it will modify. In Figures 6 and 7,¹² JavaScript code was found within the Zeus configuration file to automate the funds transfer process from the victim's account to a mule account.
 - Makes a call to the C&C server and retrieves information regarding an appropriate mule account that can be used. Updates the information in the transaction page;
 - Automatically skips to the transfer page and injects information into the page: money mule account and intended transfer amount. Unfortunately there are several cases in which the transfer to the mule is not reversed by the bank and is counted as a fraud loss, especially in commercial banking situations;

```
if(!titl.indexOf('makeapayment') != -1 && titl.indexOf('step1of4') != -1 && next == 1)
{
    top.document.title='online banking';
    if(!drok)
    {
        step2();
        return false;
    }
    else
    {
        new_mkPay1();
        return false;
    }
}
```

Figure 6 – Script code used to prepare a payment

```
function step2()
{
    var ax = document.body.getElementsByTagName('a');
    try
    {
        for(var j=0; j<ax.length; j++)
        {
            if(ax[j].innerText.indexOf('add a new payee') != -1)
            {
                setTimeout('document.getElementById(""+ax[j].id+"").click();', 1200);
                break;
            }
        }
    }
    catch(e){aout(1)}
}
```

Figure 7 – Script code used to add a recipient (mule)

- Sends the transaction to the online banking platform, post-modification;
- Injects a fake balance into the *Account Balance* and or *Account Summary* page, showing the balance prior to the malware-initiated transaction; and
- Allows for the main page to continue loading as normal.

ACH transaction modification

1. User logs into a business banking account.
2. The login information is stolen and sent to the C&C server.
3. The malware then
 - Grabs the account balance and sends it to the C&C server;
 - Uses a Perl regular expressions library to select the target page to inject into; in this case it will be the ACH transaction page; and
 - Waits for the user to click 'Submit' on the ACH transaction page.
4. User initiates an ACH batch and clicks submit.
5. Malware injects a fake page to make the user think that it's taking a little extra time to load to confirm ACH batch;
 - Makes a call to the C&C server and retrieves information regarding appropriate mule accounts that can be used; and
 - The payee information is manipulated and replaced with fraudulent payees belonging to mules. This is performed by injecting into the transaction page and altering the information in the HTML POST.
6. User is challenged and is required to enter a secondary factor of authentication to approve. User enters answers to challenge questions and or one-time password. Clicks *continue*.
7. Modified transaction is sent to the online banking platform for the ACH batch.

¹² http://www.securelist.com/en/blog?print_mode=1&weblogid=155.

Furthermore, HTML injection is used to steal a host of other personal information directly from pages. This personal information is used to access one or more additional accounts and for a number of other fraudulent purposes, including sale of this data on the black market. One particular function found in a sample discovered in the wild (described below) is used to steal the password associated with initiating an external transfer. These challenge questions and passwords are often seen in business banking accounts that employees use to validate and approve a transaction. As seen in other examples, Zeus has injected authentic fake pages to either capture additional information or to stall the user while the fraudster takes over the account.

```

===== SECURITY QUESTIONS =====
[1:] Your favorite TV show?
E id="dgrdQuestionList_ct13_MYctl_1">*selected="selected"*value=* </option>1
[2:] Your favorite flower?
: name="dgrdQuestionList_ct14_MYctl_2:txtNumber"*value="| "@ =====
[3:] Your favorite leisure time activity?
: name="dgrdQuestionList_ct15_MYctl_3:txtNumber"*value="| "9 =====
[4:] Your favorite type of music?
D id="dgrdQuestionList_ct16_MYctl_4"*selected="selected"*value=* </option>6
[5:] Your favorite professional football team?
E id="dgrdQuestionList_ct17_MYctl_5">*selected="selected"*value=* </option>6
[6:] Your favorite professional baseball team?
D id="dgrdQuestionList_ct18_MYctl_6"*selected="selected"*value=* </option>)
[7:] The color of your first car?
D id="dgrdQuestionList_ct19_MYctl_7"*selected="selected"*value=* </option>%
[8:] Your favorite holiday?
E id="dgrdQuestionList_ct110_MYctl_8"*selected="selected"*value=* </option>-
[9:] Your favorite place to vacation?
E id="dgrdQuestionList_ct111_MYctl_9"*selected="selected"*value=* </option>G
[10:] what is the first letter of your mother's maiden name?
F id="dgrdQuestionList_ct112_MYctl_10"*selected="selected"*value=* </option>7
[11:] In which month were your parents married?
F id="dgrdQuestionList_ct113_MYctl_11"*selected="selected"*value=* </option>G
[12:] what is the first letter of the name of your high school?
F id="dgrdQuestionList_ct114_MYctl_12"*selected="selected"*value=* </option>?
[13:] what is the first letter of the name of your pet?
F id="dgrdQuestionList_ct115_MYctl_13"*selected="selected"*value=* </option>7
[14:] In which month was your first child born?
F id="dgrdQuestionList_ct116_MYctl_14"*selected="selected"*value=* </option>R
[15:] what is the first letter of your maternal grandmother's maiden name?
F id="dgrdQuestionList_ct117_MYctl_15"*selected="selected"*value=* </option>Q
[16:] what is the first letter of the name of the town of your first job?
F id="dgrdQuestionList_ct118_MYctl_16"*selected="selected"*value=* </option>P

```

Figure 8 – Injection code for stealing security question answers

Stealing an external transfer password

1. The script code resets the cookie, requiring the user to re-enter the information. The code also will establish a new cookie for the user. In some cases, Zeus will create an array of possible challenge questions and will define in the configuration file how to inject in order to steal the answers to these questions, all based on the contents of the cookie (Figure 8).
2. The code will inject a popup that will ask for additional information relating to the banking session, including a critical element – the external transfer password. This external transfer password in this case will be used to authorize business payments. This fake AJAX popup titled “Online Security” will be injected directly into the users browser. The following fields appear along with official sounding text with an authentic look and feel:
 - Day of birth
 - External transfer password
3. Fraudsters are now capable of taking control in real time of the user’s session. Since they have captured the external transfer password or other challenge questions, they can approve a transfer without additional effort.
4. The script will continue by injecting a completely new account balance page. This page will have the same look and feel as the real page used by the financial institution. Every time the user logs into his online banking account he will see a fraudulent balance displayed. This fake information will persist as long as the malware is on the system and altering transactional behavior – the transfer amount is

always hidden if initiated by the fraudster, but will be the balance minus the user’s transfer if the user invokes it.

Conclusions

Credit unions and regional/community banks are now the focus of Zeus/SpyEye banking malware. A multi-layered approach is required to stop these types of threats. Since smaller financial institutions do not have the same resources as their larger counterparts to combat fraud, specialized solutions are recommended to aid their existing strategy. Fraud anomaly and detection services are one of the key elements in helping to stop this ever growing threat.

From evidence analyzed, targeted generic attacks have been used to compromise the credentials from hundreds of different banks.

The underlying web applications that run online banking for these small community banks are being targeted generically; theft of credentials in a wide-scale fashion is being conducted against these brands. Evidence in the malware configuration files has shown that a number of high profile and even less profiled brands are being attacked by Zeus/SpyEye.

About the Author

Ryan Sherstobitoff is an independent security researcher. He formerly was the Chief Corporate Evangelist at Panda Security, where he managed the US strategic response for new and emerging threats. Ryan is widely recognized as a security & cloud computing expert throughout the country. He can be contacted at sherstobitoff52@gmail.com.

