Understanding Their Impact and How to Defend Your Institution Against Trojan-Aided Fraud

Banking Trojans

Who should read this paper

Banking malware, specifically banking Trojans, are reaching alarming new levels of sophistication. Go behind the scenes to understand how these attacks operate and how a layered security solution that includes fraud detection and strong authentication can help protect your business and your customers against online fraud.
Banking Trojans
Understanding Their Impact and How to Defend Your Institution Against Trojan-Aided Fraud

Contents

Introduction ............................................................................................................................ 1
Banking Trojans: A growing threat .................................................................................... 1
A look inside the beast ......................................................................................................... 2
Statistics and logs ................................................................................................................ 2
Advanced controls ............................................................................................................. 3
Sophisticated backdoor ....................................................................................................... 3
Extensive command list ..................................................................................................... 3
Detecting and preventing trojan-assisted fraud ................................................................. 4
A multilayer security solution from Symantec ................................................................. 6
Detecting and protecting against fraud ............................................................................. 7
Protecting identity with two-factor authentication .......................................................... 7
Conclusion ......................................................................................................................... 7
Glossary ............................................................................................................................... 8
Introduction

Banking malware, specifically banking Trojans, are reaching alarming new levels of sophistication. New variations are constantly being introduced to thwart detection by antivirus software on the victim’s PC. And real-time capabilities built into the Trojans make it difficult for banks and account holders to spot fraud attempts as they occur.

Trojans today pose a clear threat to the trust in online banking that financial institutions have worked so hard to establish for their consumer and business customers. Plus, there’s the threat to the bottom line: extensive fraud losses and potential lawsuits can add up to significant hard dollar costs. In 2009, a Maine-based construction firm sued its local bank after cyber thieves stole more than a half million dollars through illegal transfers from the company’s online account — a precedent that could set off further lawsuits against banks for not taking steps to prevent this type of fraud.

What steps can your company take to defend itself against sophisticated malware that’s running on business employees’ and consumers’ devices? Industry experts agree that deploying a layered security strategy is your best defense. A multilayer security solution can help your institution establish a continuum of protection to detect, prevent, and mitigate fraud stemming from cybercriminals using banking Trojans.

This paper examines the current threat of banking Trojans, taking you behind the scenes of the most prevalent Trojan, Zeus, for a look at the power it can give cyber thieves. We’ll cover the implications of these sophisticated Trojans for your business and how a layered security solution that includes fraud detection and strong authentication can help protect your business and your customers against online fraud.

Banking Trojans: A growing threat

Malware continues to grow at exponential rates, with Trojans now being the most common type at 66 percent of all malware. Trojans infect a victim’s computer to enable a cybercriminal to perform malicious functions like making it part of a botnet (collection of remotely-controlled computers) or stealing confidential data like passwords and credit card information. Hundreds of criminal groups are operating Zeus-fueled botnets called Zbot botnets. The number of infected PCs is estimated at 3.6 million in the U.S., or 1 percent of all PCs in the country.

Trojans like Silentbanker and Clampi have been infecting users’ PCs for years, but by far the most prevalent of the banking Trojans is Zeus. This data-stealing Trojan has been circulating since 2006, capturing infected users’ banking logon credentials and sending them back to a command-and-control hub. Zeus is propagated through scams such as spam messages purportedly from Verizon Wireless®, a fake password reset request from MySpace®, a notice from the IRS, and a critical update for Microsoft Outlook®.

Zeus infects PCs, waits for their users to log on to a list of targeted banks and financial institutions, and then steals their credentials and sends them to a remote server in real-time. Additionally, it may inject HTML into the pages rendered by the browser, so that its own content is displayed together with (or instead of) the genuine pages from the bank’s Web server. In this way it is able to ask the user to divulge additional personal information, such as payment card number and PIN, one-time passwords, and more.

To evade detection and removal, Zeus uses rootkit techniques. The Zeus kit is a binary generator. Each use creates a new binary file, and these files are different from each other — making them notoriously difficult for antivirus or security software to detect. To date, very few variants have had effective antivirus signatures against them, and each use of the kit usually makes existing signatures ineffective.

---

4- “Antivirus Rarely Catches Zbot Zeus Trojan,” Kelly Jackson Higgins, DarkReading, September 16, 2009
Zeus is also spawning a next generation of banking Trojans with even higher levels of sophistication. These newest Trojans not only collect credentials, but use them in real-time to thwart basic fraud detection measures. For instance, researchers recently identified a Trojan dubbed URLZone. URLZone is programmed to calculate on-the-fly how much money to steal from an account based on how much money is available.⁶

**A look inside the beast**

To understand just how powerful a Trojan like Zeus can be, let’s look briefly at a sample of the capabilities it provides to cybercriminals.

![Remote Commands Tab](image)

**Figure 1. Remote Commands Tab**

**Statistics and logs**

Zeus provides statistics like the total bot count and total logs in the database. A cybercriminal can also search the logs using specified strings, log type, or a time range. For example, Zeus lets a cybercriminal search for FTP or HTTPS credentials captured on a specific date. The Trojan can steal credentials for online bank accounts from HTTPS connections and protected storage.

---

⁶ “New Banking Trojan Horses Gain Polish,” Robert Vamosi, Computerworld, November 25, 2009
Advanced controls
Zeus also lets hackers arrange infected PCs into groups. For instance, a hacker can group all the PCs with fast Internet connections together for a high performance botnet. The Remote Commands Tab shown in Figure 1 lets cybercriminals define commands for an entire botnet, bots from a certain country, or just a single computer.

Sophisticated backdoor
With the Screenshot function, a fraudster can get a screenshot of each infected system currently online. The Zeus Trojan installs a backdoor, which creates a SOCKS proxy and a Web proxy on the infected system. Fraudsters can use these proxies to hide their identities while they access victims’ online bank accounts to steal money. Figure 2 shows that by clicking on a proxy, the fraudster can get useful information about the proxy (for example, on which port the proxy is installed or whether the proxy is already being used or not).

Figure 2. Proxy Information for an Infected Machine

Extensive command list
Zeus includes more than a dozen different commands to enable hackers to control infected PCs. For instance, a command can be executed to make an infected client download additional malicious code as shown in Figure 3.
Detecting and preventing trojan-assisted fraud

Using Zeus or other banking Trojans, cybercriminals can bypass many of today’s standard security mechanisms. That’s why a layered security defense is critical: no one security component is failproof against every possible threat. It takes a multilayer strategy to defend against sophisticated fraud attempts.

By layering technology such as two-factor, or strong, authentication and fraud detection, financial services companies can better protect themselves and their customers. For instance, some cybercriminals don’t have the wherewithal to mount a Zeus scam. It takes technical know-how, resources, and time to execute a real-time Trojan attack. For this reason, two-factor authentication (2FA) is particularly effective at preventing many fraud attempts. However, comprehensive fraud detection is needed to stop more sophisticated attempts originating from Trojans.

Using transaction monitoring and applying transaction verification processes, a comprehensive fraud detection system can detect a suspicious transaction that is out of profile for the legitimate user or that includes risky fraud patterns. For instance: a fraudster uses Zeus, accesses a victim’s online banking account, and transfers money to a money mule. Since this is probably the first time money is transferred to the money mule’s account, the fraud detection system flags this transaction as suspicious. Out-of-band (OOB) transaction verification can then stop the fraudster by contacting the legitimate account owner offline to confirm the transaction.
The more clever criminals may try to thwart detection by attempting multiple, low-value transactions to several money mules. This is a known fraud technique to avoid the value limit applied by many banks. The fraud detection system can and should be configured to detect such a scenario, creating an alert (OOB challenge), and stopping the scheme.

To illustrate the effectiveness of a sophisticated fraud detection system, consider the following scenarios: a transfer with a Trojan-infected PC where the bank has no fraud detection system and a transfer with a Trojan-infected PC where the financial institution is using a fraud detection system.

**Scenario A: Money transfer flow with a Trojan-infected PC - no fraud detection**

- The user wants to transfer $5,000 from account A to account B
- The Trojan alters the request to move a different amount to a different account

![Diagram of Scenario A](image)

- The bank application asks the user to confirm the transaction request after validating it
- The Trojan alters the response from the bank so that it reflects the original details and appears legitimate to the end user, who confirms the order
Scenario B: Money transfer flow with a Trojan-infected PC - with fraud detection

- The user wants to transfer $5,000 from account A to account B
- The Trojan alters the request to move a different amount to a different account
- The bank application verifies the transaction against the fraud detection system

The fraud detection system identifies the transaction as suspicious
- The bank application sends an SMS to the customer (alternatively, automated voice calling can be used) with the transaction details as recorded by the bank application together with a one-time password
- The bank application asks the user to confirm the transaction with the one-time password as it appears in the SMS text message
- The customer sees information in the confirmation request screen that doesn't match the information in the SMS text message and doesn't enter the code. The transaction is not completed and fraud is thwarted

A multilayer security solution from Symantec

With the Symantec layered security approach, our state-of-the-art security products and services, such as fraud detection and strong authentication, complement each other to create a solution that is even stronger than the sum of its parts. Symantec provides financial services organizations with not only the means to protect against identity theft and fraud, but also the opportunity to reinforce consumer
trust at the same time. These layered security solutions empower companies to make security protection conspicuous while deploying sophisticated fraud detection and prevention capabilities in the background.

**Detecting and protecting against fraud**

VeriSign® Identity Protection Fraud Detection Service works in real-time for detecting and preventing identify theft and transaction fraud, providing effective protection against cybercriminals using banking Trojans. Combining complex business logic with advanced machine learning techniques, Fraud Detection Service provides an efficient and robust transaction monitoring solution to block criminal acts attempted with stolen identities. Behavioral patterns, including machine fingerprints, are learned for each user based upon previous legitimate activity, while anomalous actions are detected and reported as suspicious.

Business rules are also applied for identifying high-risk characteristics and scenarios. When the risk score exceeds a predefined threshold, the user is challenged and required to pass a higher level of authentication. With OOB verification, a fraud attempt can be effectively halted.

For financial institutions and other account holders, Fraud Detection Service includes modules that monitor the three most sensitive events for these businesses: log on, trading, and money transfer. All three of these modules identify suspicious scenarios related to deceptive entries into the system, unauthorized money movements, and criminal scams. And particularly important when it comes to real-time Trojan attacks, Fraud Detection Service has the capacity to process more than a thousand transactions per second to detect anomalies in real time.

**Protecting identity with two-factor authentication**

Symantec™ Validation and ID Protection Service (VIP) is a cloud-based, two-factor authentication (2FA) service that protects enterprises and users from unauthorized account access—above and beyond simple user name and password—with an additional factor of authentication. Symantec VIP cloud-based service is hosted by Symantec, and users can choose from a variety of supported 2FA credentials, ranging from security hardware tokens to software-generated credentials to SMS and voice for OOB authentication.

Using Symantec VIP OOB authentication features, banks can defeat man-in-the-middle and man-in-the-browser attacks. Simple, automated voice call or SMS messages can be delivered on devices customers typically carry. Symantec VIP is easy to deploy and integrates with existing infrastructure. Symantec VIP OOB authentication is highly customizable, with templates that fit current workflows, and custom prompts that can be integrated with a bank’s brand.

**Conclusion**

As this paper has shown, banking Trojans are formidable threats. But there is a way to defend against these and other forms of cybercrime attempts: with a layered security solution that includes a fraud detection system designed to recognize and prevent fraudulent transactions. Symantec VIP Authentication Service and VeriSign® Identity Protection Fraud Detection Service deliver the superior fraud prevention and detection that banks and other financial institutions need to protect themselves and their customers. As part of a comprehensive suite of identity protection and authentication services, Symantec delivers the multilayer security needed to help thwart today’s and tomorrow’s cybercriminals.
# Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>The process of confirming that something is genuine. In computer security, authentication is usually an automated process of verifying the identity of someone or something, such as a computer or application.</td>
</tr>
<tr>
<td>Credential</td>
<td>Proof of qualification, competence, or clearance that is attached to a person. A digital certificate, token, smart card, mobile phone, or installed software are credentials that may be used to enable strong or multifactor authentication.</td>
</tr>
<tr>
<td>Two-Factor Authentication, Strong</td>
<td>All of these terms refer to the authentication practice of requiring confirmation of something you know, such as a user name and password, and something you have, such as a smart card, token or certificate.</td>
</tr>
</tbody>
</table>
About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com