The SHIELD
A Security Newsletter for Businesses

MALWARE: IT'S A BEAR FOR BUSINESS

- NOTHING PERSONAL: LEARN HOW CYBERTHIEVES ARE CLEANING OUT BANKING ACCOUNTS
- TURNKEY THEFT: DISCOVER HOW SOPHISTICATED SOFTWARE MAKES COMPUTER FRAUD EASY
- DON'T BE A VICTIM: TAKE STEPS THAT COULD SAVE YOUR BUSINESS

Malware: It's a Bear for Business

All of us serving you™
Introduction

It’s never been easier for cybercriminals to steal money from businesses like yours.

There’s a wealth of malware - software tools used to commit online crime - available to online gangs. One family of malware is designed to steal your business account log-in credentials and allow cybercriminals to set up unauthorized transfers while posing as an approved account manager. This fraud is relatively low risk for a criminal and because the request appears to come from a legitimate account holder, it can be challenging for a Financial Institution (FI) to detect.

U.S. Bank takes this malware threat, collectively referred to as “Banking Trojans,” extremely seriously. We have our own controls in place to identify potentially fraudulent transactions but the easiest and safest approach to protect your corporate finances is to ensure that individuals and companies take some basic steps that may prevent them from becoming victims of fraud in the first place. Prevention is always better than detection, and that’s where the Shield newsletter comes in.

In this edition we reveal how Banking Trojans work as well as the best practices that will help you reduce the risk they pose to you and your company.

U.S. Businesses Are Under Attack

According to FBI case files, cybercriminals were able to loot the business accounts of hundreds of American businesses in 2010-2011, stealing a total of $85 million. In most cases, the criminals used unauthorized Automated Clearing House (ACH) and wire transfers to siphon money out of business accounts.

One of the most effective Banking Trojans, dubbed ZeuS, may have accessed over 13 million personal and business accounts. Another, nicknamed EuroGrabber, has been used to steal over $47 million dollars.

How is this possible?

A large increase in availability of simple and cheap tools make it easy for non-technical thieves to spread and profit from malware. Banking Trojans are becoming increasingly sophisticated; better able to avoid detection by security programs and their targets, using non-intrusive techniques to steal log-in and banking credentials, automating unauthorized transfers, and covering their tracks to delay discovery of the fraud for as long as possible.

Business accounts are the preferred target because they typically give criminals access to larger sums of money than a consumer account. Also, because many business accounts are used to make multiple transfers of large sums as part of routine business, a cautious cybercriminal’s unauthorized transactions may not be detected as quickly.

Table of contents

pg. 2 Introduction
pg. 2 U.S. Businesses Are Under Attack
pg. 4 How Banking Trojans Work
pg. 5-6 Layered Defenses: Fraud Prevention Steps for Safer Banking

The Shield Newsletter Is for...  
- Business professionals and leaders with responsibility for business account management, including payroll, wire transfer and/or ACH services  
- Business owners without IT support, or businesses that do not have Information Security and/or business account management policies or processes in place  
- Customers of U.S. Bank and also other financial institutions

Information shared in this newsletter is not intended to supersede your existing IT, account management, and/or security processes, systems, or policies in your workplace, or those of your current FI. Please consult your IT support and your FI providers for more assistance.

This newsletter outlines certain practices that businesses should consider to reduce the likelihood of loss caused by online fraud and identity theft. The content does not purport to identify all existing online fraud and identity theft practices and all fraud mitigation measures that your business should consider implementing. There is no way to guarantee that any set of protective measures will eliminate loss caused by online fraud and identity theft. U.S. Bank is not responsible for losses caused by online fraud and identity theft.
It starts with stealthy infiltration

A Banking Trojan doesn’t need to hack your company’s bank accounts. Once one gets onto your computer, all it needs to do is lurk quietly in the background and wait for you to log into your corporate banking systems. It then invisibly steals your log-in credentials, enabling a cybercriminal to access your accounts as if he were you.

Different Trojans use different methods to swipe your banking details with little or no indication that a fraud is underway. Some will capture input from your keyboard. Others may create a fake log-in page designed to trick you into revealing information, some Trojans intercept the data for your online banking session from your browser and then seamlessly pass it on to your bank, so that nothing seems amiss.

Once a Trojan identifies your account holding institution, more sophisticated versions can install modules designed specifically to imitate your bank so that suspicion is less likely to be aroused during the fraud. These modules may also attempt to work around specific authorization controls.

Trojans can bypass some existing controls

Some recent Trojans are also able to bypass additional controls such as SMS text authorization messages. One approach uses one Banking Trojan to steal your mobile phone number and banking credentials, and then tricks you into installing a second Trojan on your smartphone by faking a text message seemingly from your FI that contains malware. If installed, it will intercept future SMS messages sent from your actual FI that may be used to confirm transactions, relaying them to the cybercriminal, who will confirm on your behalf.

Fraudulent transactions and covering tracks

Once your log-in credentials are stolen, what happens next will depend on the sophistication of the Trojan and the goals of the criminal. In some cases, the account details will be verified and the information will be sold on to others, minimizing the original cybercriminal’s risk. Alternatively, the cybercriminal may personally handle the unauthorized transactions, but some Trojans can even manage the transaction process automatically. The most sophisticated versions will even disguise the transaction activity from you, using faked data supplied to your Web browser to mask any evidence of the unauthorized money transfer.

The good news

Such sophisticated technology in the hands of criminals sounds intimidating, but you are not helpless. Cybercriminals are typically looking for easy pickings, so if you make it harder for them, it may be to your benefit. Cybercriminals are pragmatic and risk-averse, a tougher target may not be worth additional effort and risk of early detection against a return that’s far from guaranteed, particularly in an environment that’s rich in targets. If you take some basic precautions, you are more likely to avoid loss due to unauthorized access. After all, a company that takes extra measures to protect itself is also more likely to be vigilant about spotting fraud attempts early in the process, so most cybercriminals won’t spend much time on tough targets.
How Banking Trojans Work

Everyone knows the tale of the Trojan horse, when the ancient Greeks marked the end of an unsuccessful siege of the city Troy by presenting their foes with a large wooden horse. Once the Trojans brought the horse into the city, a platoon of Greek warriors hidden inside the horse snuck out to open the gates, turning defeat into victory.

Modern Trojans use similar principles, hiding inside apparently legitimate code in order to gain unauthorized access. Malicious code can be concealed in Web pages and in Web ads on legitimate sites, within software downloads, or file attachments. They can be disguised as software updates that the user needs to install. Links to malware can be hidden in emails that are disguised to look like they came from official sources (perhaps even faked to look like your bank), or placed in social media messages, ads, and status updates.

Simply surfing the Web can be risky

Sometimes a victim is tricked into installing malware, but not always. In fact, the most popular technique is an automated install that occurs when you visit a Web site that has been infected with malware. While you browse, malware stealthily searches your browser for installed software with vulnerabilities that can be exploited, allowing the malware to automatically and invisibly install itself. Many vulnerabilities have been identified by software providers who create “patches” available for download to fix an issue. Unfortunately, many people don’t know the importance of keeping software up to date, and new vulnerabilities are found all the time.

Social networks are tempting targets

In May 2013, the media reported an increase in Zeus malware attacks delivered via ads on Facebook. Unwary victims who clicked on the links got a Banking Trojan, which also copied the ad to their friends and contacts.

Malware on the move

Malware is also being adapted to target mobile smartphones. In fact, some newer strains can spread between desktop systems and smartphones during synchronization. And it isn’t only phones that can be used to propagate malware, some malware will detect and copy itself onto USB drives enabling it to covertly spread between systems, even on separate networks.

How Do They Spread?

80% of newly detected malware variants are Trojans
They’re popular in the cybercriminal community because they’re consistent and effective money-makers. (Source: Anti-Phishing Working Group)

35% of malware infections come from legitimate sites found via a search engine
According to Google, at the end of 2012 there were 150,000 hacked sites linked to malware. Many of these are the type that will scan your computer and exploit vulnerable programs to install a Trojan. (Sources: Blue Coat Security Labs & Google)

11% of malware attacks were made using email
Malware-poisoned attachments or links to a malware-infected site can be sent by email; figures for 2011 showed a 68% increase in this type of attack over the previous year. (Source: Blue Coat Security Labs)

1 in 16 malware attacks were launched via social media
Some malware is devoted to taking over social media profiles and then sending copies to everyone in a social network, taking advantage of our trusted networks. (Source: Blue Coat Security Labs)

Why is Patching So Important?

60% of the vulnerabilities targeted are at least two years old
This is why your IT department should be regularly patching your computer’s operating system and software programs, and why you should patch your home system. (Source: Malwarebytes Blog)

50% of software exploits used to install malware target Java
This popular software tool is heavily targeted and a wide number of vulnerabilities have been found by malware coders, Adobe Reader is next on the list at 28%. (Source: Kaspersky Labs)
Layered Defenses
Fraud Prevention Steps for Safer Banking

Because malware is so sophisticated and is always evolving, no one measure can be 100% effective. Your best option is a layered defense.

The first layer is prevention - Simple security measures can prevent your account holder systems from ever being exposed to a Banking Trojan.

The second is account control - Which requires implementing the security measures offered by your financial institution to prevent unauthorized money transfers; the added benefit is that these also mitigate the risks of employee fraud.

The third layer is detection - If you know what to look for, you or a fellow employee may be able to alert your IT department and stop malware from spreading to other systems.

Prevention

First follow any existing security / IT policies at work; do not attempt to patch or install software without first contacting your IT department.

Use a dedicated computer for account management

KEY TIP: Have a computer that is used only for financial transactions by authorized users and for no other purpose, not even email. That way, you significantly reduce the risk of infection from most typical malware threats.

Don’t use your work computer for non-work-related tasks
The more Web sites you visit, the more you are potentially exposed to malware. Risk also increases the more you use Webmail services, social media sites, or carry out software installs (particularly downloads of free software from unknown companies.)

Email attachments and links
Avoid clicking on links or opening attachments in emails from unknown senders. Even an email that appears to have been sent from someone you trust may actually be part of a malware scheme. If you have any doubts, contact the sender and verify that they sent it.

Pop-ups
Avoid clicking on a pop-up window – especially if it mentions malware. Ironically, pop-ups claiming to scan for malware may actually deliver the malware they claim to prevent. Don’t click the ‘X’ in the upper right-hand corner to close the pop-up – that can also load malware. Instead, right click over the ad and select “Close.”

Anti-virus, anti-malware & security controls
Microsoft research using data from over one billion systems worldwide indicates that a computer with an up to date anti-virus solution is 5.5 times less likely to suffer from a malware infection than one without. However, you can’t assume anti-virus will detect all malware - malware writers spend a lot of time figuring out new ways to avoid detection. Every computer should have an anti-virus solution and a firewall, and both need to be kept up to date.

- Install security software from a reliable company (look for heavily reviewed products on sites such as CNET or Amazon), and set up automatic updates.
- Use anti-malware tools such as Trusteer Rapport if they are offered by your financial institution.

Keep software fully patched; remove software you don’t need
You should ensure that:

- Software regularly targeted by malware writers such as Adobe Reader, Adobe Flash, and Oracle Java are current versions, and that they have been set to automatically receive patches.
- Your operating system and related systems like browsers are receiving patches – Microsoft, for example, offers an automatic update service.
- Programs that you don’t use are removed as they may offer vulnerabilities for malware to exploit.
- Software versions, including the operating system, should be kept up to date. Older versions have more vulnerabilities, lack the latest security features, and may no longer be supported with patches.

“Security is a constantly moving target and devices become less secure over time. How quickly this happens is determined by the speed and diligence with which security updates and patches are applied.”

Jason Witty,
Chief Information Security Officer
U.S. Bancorp

Because malware is so sophisticated and is always evolving, no one measure can be 100% effective. Your best option is a layered defense.

The first layer is prevention - Simple security measures can prevent your account holder systems from ever being exposed to a Banking Trojan.

The second is account control - Which requires implementing the security measures offered by your financial institution to prevent unauthorized money transfers; the added benefit is that these also mitigate the risks of employee fraud.

The third layer is detection - If you know what to look for, you or a fellow employee may be able to alert your IT department and stop malware from spreading to other systems.

Prevention

First follow any existing security / IT policies at work; do not attempt to patch or install software without first contacting your IT department.

Use a dedicated computer for account management

KEY TIP: Have a computer that is used only for financial transactions by authorized users and for no other purpose, not even email. That way, you significantly reduce the risk of infection from most typical malware threats.

Don’t use your work computer for non-work-related tasks
The more Web sites you visit, the more you are potentially exposed to malware. Risk also increases the more you use Webmail services, social media sites, or carry out software installs (particularly downloads of free software from unknown companies.)

Email attachments and links
Avoid clicking on links or opening attachments in emails from unknown senders. Even an email that appears to have been sent from someone you trust may actually be part of a malware scheme. If you have any doubts, contact the sender and verify that they sent it.

Pop-ups
Avoid clicking on a pop-up window – especially if it mentions malware. Ironically, pop-ups claiming to scan for malware may actually deliver the malware they claim to prevent. Don’t click the ‘X’ in the upper right-hand corner to close the pop-up – that can also load malware. Instead, right click over the ad and select “Close.”

Anti-virus, anti-malware & security controls
Microsoft research using data from over one billion systems worldwide indicates that a computer with an up to date anti-virus solution is 5.5 times less likely to suffer from a malware infection than one without. However, you can’t assume anti-virus will detect all malware - malware writers spend a lot of time figuring out new ways to avoid detection. Every computer should have an anti-virus solution and a firewall, and both need to be kept up to date.

- Install security software from a reliable company (look for heavily reviewed products on sites such as CNET or Amazon), and set up automatic updates.
- Use anti-malware tools such as Trusteer Rapport if they are offered by your financial institution.

Keep software fully patched; remove software you don’t need
You should ensure that:

- Software regularly targeted by malware writers such as Adobe Reader, Adobe Flash, and Oracle Java are current versions, and that they have been set to automatically receive patches.
- Your operating system and related systems like browsers are receiving patches – Microsoft, for example, offers an automatic update service.
- Programs that you don’t use are removed as they may offer vulnerabilities for malware to exploit.
- Software versions, including the operating system, should be kept up to date. Older versions have more vulnerabilities, lack the latest security features, and may no longer be supported with patches.

“Security is a constantly moving target and devices become less secure over time. How quickly this happens is determined by the speed and diligence with which security updates and patches are applied.”

Jason Witty,
Chief Information Security Officer
U.S. Bancorp
Account Control

Managing your corporate financial accounts requires setting up and managing access controls, transaction controls, and administration processes to prevent unauthorized transfers.

Dual authorization

KEY TIP: Set up dual authorization so that all significant transactions initiated must also be approved by a second trusted individual. It is one of the most effective anti-fraud measures for both internal and external fraud.

With dual authorization, even if a Banking Trojan steals one set of log-in credentials, the cybercriminals controlling the Trojan may not be able to complete a money transfer. For this to work, the second authorization must never take place on the same device used by the first authorized requester. If you both use the same malware-infected system or if both authorizing devices are infected, this protection will fail.

You should have dual authorization in place for:

- Setting up money transactions, and creating or modifying ACH and wire templates
- User administration activities like adding or changing users and profiles, particularly those with any power to authorize accounts and processes (contact numbers and email addresses, etc.)
- System administration; administrators should have two different accounts - one for admin purposes and the other for transactions

Both authorizers should:

- Use different computers; one being a dedicated banking computer
- Think before approving: look for unexpected changes in transactions or transaction activity, or to your account management tools and processes - it could be a sign that you or your co-approver have malware
- Enable all appropriate notification features to get early warning of suspicious activity
- Review audit reports and monitor account activity on a daily basis
- Make sure to keep up to date on user administration as roles and responsibilities change
- Keep access limited to those who really need it, and set their permissions at the minimum levels necessary for job requirements
- Set your own limits for transaction notifications as often the defaults set by financial institutions are very high, and specify limits at the individual user level, if necessary

Learn more about U.S. Bancorp’s business account control features

- Commercial & Government: Please contact your Commercial Customer Service team.
- Small Business: Please contact your U.S. Bank relationship manager or treasury management consultant.

Detection

There could be one or more warning signs if the worst happens.

Possible Banking Trojan indicators

An account log-in form may have new data fields that you’ve never seen before, asking for additional personal or financial information. If you see this:

- Call your FI to check whether they have changed the log-in process before continuing with the log-in process
- Keep your FI’s phone number handy and don’t use any number provided on a possibly-compromised computer

Error pages may appear during a banking session either when you attempt to visit your banking site or after you attempt to log-in. Cybercriminals don’t want you logging in when they are active in your account. If you see a warning that your bank site is down for maintenance, call your bank to check.

Other possible malware warning signs

- More pop-up windows than usual appear or pop-ups with concerning messages (FBI warnings, for example) display, even when you’re not browsing the Web
- Your browser displays a Web page you didn’t intend to visit or your search engine is delivering unusual or unhelpful results as a matter of course
- You can’t visit anti-virus Web sites or look up malware removal information in search engines
- New toolbars or icons appear without your permission
- Your computer experiences unexpected errors or crashes
- Your contacts get email or social media messages from you that you didn’t send
- Your anti-virus and/or firewall software vanishes or is disabled

What to do if you suspect malware

- Stop using the system, particularly for online activity that requires passwords, and contact your IT support (if available)
- If you handle your own IT, update your security software, run a system scan using your previously installed and updated Anti-Virus, and delete anything that’s flagged as a problem
- If you use Microsoft Windows, you should also run the Microsoft Safety Scanner (www.microsoft.com/security/scanner)
- Change all of your passwords (for financial and corporate accounts and online services like Amazon, Facebook, or Gmail) using an uncompromised computer