Cyphort Labs 2015 Financial Malware Report

Cyphort Labs Knocks Down the
Top 8 Financial Malware
Why Financial Malware Matters

Malware is a topic that everyone is talking about. Giant movie studio’s network is hacked? The attackers used malware. Big retailer’s point-of-sale system is breached? Malware did it. Hackers breached ATMs at multiple banks? They used malware. The litany of blame seems endless – in technical trade publications and in general news publications alike. Statistically, “malware” was the top keyword during 2014 and 2013 ousting “security,” according to the HP Cyber Risk Report 2015. Interest in this topic is high because malware is an exceptionally effective attack vector. And if you work for a bank, an e-commerce company, or any other financial service provider, it’s vital to study the key financial malware threats that often are uniquely targeted at your enterprise in order to prevent breaches.

The twentieth century U.S. criminal Willie Sutton was said to rob banks because “that’s where the money is.” International cyber criminals know this too, which is why the risk of financial malware threatens the fabric of our financial system. Forget about blasting into a bank vault to steal paper money! Stealing it electronically is much easier, and safer for the thieves. Hackers are also exploiting vulnerabilities in payment systems. The sheer volume of electronic payments is breathtaking. In the U.S., for example, in 2013 about $4.6 trillion in purchases were made with credit and debit cards. By 2018, this will rise to over $7 trillion – about two-thirds of the value of all purchases. Another $2 trillion will be spent with other electronic payments like PayPal and mobile, and many of these are backed by payment cards.¹

Targets like these are too attractive to ignore, which is why cyber criminals are using specially tailored financial malware to breach banks and payment systems for profit. Our report explains how they are doing it by analyzing the top eight financial malware. By understanding these threats, you will know where to address security systematically for protecting your customers’ money, and safeguarding corporate financial assets.

Detecting financial malware is a big challenge because traditional antivirus and antimalware applications usually fail to detect sophisticated evasion tactics that are intrinsic to the targeted threats. Advanced security technology such as the Cyphort Platform will help you to accurately detect and analyze financial malware, and provide actionable, contextual intelligence that enables security teams to respond to attacks faster, more effectively, and in as surgical a manner as their attackers.

Threat Landscape and Common Traits

Financial malware is quickly evolving in sophistication. Newer versions often feature stealthy command-and-control botnet membership designed to steal account credentials, according to the Verizon 2015 Data Breach Investigations Report. Based on Verizon’s forensic investigations, five malware events occur every second, and financial services firms experience an average of 350 malware events every week.\(^2\) The study notes: “Malware is part of the event chain in virtually every security incident…. 84.4% are C2 [command-and-control] and bank record and credentials are top two targets (59.6% and 29.6%).”\(^3\)

Propagation to victim PCs usually occurs via spam and targeted phishing campaigns – requiring a user to either click on a Trojan-infected attachment or an embedded link to an infected website. About 59% of malicious spam includes attachments, according to Trustwave.\(^4\) Embedding malware in web browser add-ons is another successful infection vector because many users trust them or believe they are benign, according to the Cisco 2015 Annual Security Report.\(^5\)

Financial malware also hides itself from signature- and hash-matching techniques used by antivirus solutions. Simple modifications to the code make the malware unique while providing the same desired behavior. Verizon says this technique can create millions of “different” variants of the “same” malware – and with targeting victims, “we found that 70 to 90% (depending on the source and organization) of malware samples are unique to single organization.”\(^6\) Financial institutions are also challenged by persistence of old malware. “Virtually every distribution we generated during our malware analysis was long-tailed,” says Verizon.\(^7\)

**Common traits of financial malware include:**

- **Man-in-the-Browser** – Controls the user’s browser without their knowledge. It’s similar to a “Man-in-the-Middle” Internet communication attack as it covertly steals login credentials and controls account transactions in a way that’s invisible to the user and hosted web application.
- **Support for configuration file for targets** – To take control of a computer and its applications.
- **Injects into processes** – To stay hidden and evade detection.
- **Steals all data, not just credit cards** – Raises the potential for theft of all login and account information for cardholder data, personally identifiable data, and sensitive corporate data such as intellectual capital, customer lists, project development plans, and other strategic information.
- **Display fake fields in bank login pages** – A user is unaware of actions applied to their account because what they see on the screen is not what’s actually executing in the background.
- **Distribution via Exploit Pack** – Relatively unsophisticated cyber criminals are able to apply sophisticated attack methodologies and technologies with “user friendly” financial malware.
- **Written and operated by Russian cyber gang** – Financial malware is unique in that virtually all major deployments are produced by criminals in Russia.


\(^7\) Verizon 2015 Data Breach Investigations Report, p. 21; also see 2014 Trustwave Global Security Report, p. 56.
Typical Attack Process

Financial malware usually employs a two-phase attack process. Phase 1 is infection: the process of getting a financial malware Trojan onto victim PCs. Phase 2 is exfiltration: leveraging the injected malware to steal credentials for financial accounts to provide cyber criminals with unimpeded access to financial accounts and systems. Verizon notes: “Larger breaches tend to be a multi-step attack with some secondary system being breached before attacking the POS [point-of-sale] system.” Clearly, this requires sophisticated planning and careful execution – so your financial institution becomes the target of a malicious campaign. The end game is monetization.

---

Cyphort Labs Knocks Down the Top 8 Financial Malware
Zeus

Aliases: ZeuS or Zbot

What
Zeus is the most successful banking malware. Attackers use Zeus to steal targeted login credentials, intercept online banking transactions, and breach financial systems. Zeus is a Trojan horse computer worm that targets PCs running versions of the Microsoft Windows operating system. It has infected tens of millions of computers worldwide since it debuted in 2007. Its success is fueled by being modular, flexible, hard to detect, and persistent. Its developer released Version 2 in 2010, a peer-to-peer version in 2011, and a 64-bit version in 2013. As with most malware, Zeus is spread via phishing and drive-by downloads.

How
Zeus uses a technique called “Man-in-the-Browser” to exploit vulnerabilities in browsers that covertly modify web transactions. Neither a user nor web host knows what’s happening – even if they use security controls such as encryption or multi-factor authentication.

After infecting the user’s PC with the Zeus Trojan, the PC is automatically connected to the attacker’s command-and-control server and receives instructions. Typically this entails stealing the user’s login credentials, and subsequently stealing specific amounts of money from the user’s account. The attacker protects his identity by collecting the money through an online “money mule.” Zeus monitors HTTP for the bank site and modifies the numbers in real time such that if the user sees the transactions, they will be innocuous to avoid drawing suspicion. Zeus is careful not to draw down the account below balance. Security experts say Zeus has created the largest botnet on the Internet with millions of PCs infected. With its capabilities, financial service professionals consider Zeus to be the most severe threat to online banking.

Detection of Zeus is challenging because it uses sophisticated techniques to achieve stealth. These include steganography, rootkit, anti-debugging, digital signatures, and a new hooking implementation. These techniques are difficult to catch with antivirus and antimalware software, and require advanced solutions for detection. For example, with steganography, Zeus embeds data inside a place nobody expects it – an image file. In the adjacent Facebook logo, the black marks represent the information added by Zeus.

Links
http://blog.phishlabs.com/the-unrelenting-evolution-of-vawtrak
http://krebsonsecurity.com/tag/zeus/
SpyEye

**Aliases:** none

**What**

Like Zeus, attackers use SpyEye to steal targeted login credentials, intercept online banking transactions, and breach financial systems. SpyEye is a Trojan horse computer worm. It has infected about 1.4 million computers worldwide since it debuted in 2009. At the time, it was considered as the most advanced financial malware kit used by cyber criminals. Like Zeus, it is making cybercrime easier as it offers attackers a user-friendly bot control panel and builder. The creator of SpyEye, Russian Aleksander Panin, was arrested in the Dominican Republic in 2013.

**How**

SpyEye also uses the "Man-in-the-Browser" technique to exploit vulnerabilities in browsers that covertly modify web transactions. Neither a user nor web host knows what's happening – even if they use security controls such as encryption or multi-factor authentication.

After infecting the user's PC with the SpyEye Trojan, the malware creates a custom encrypted configuration file to guide exploitation of the financial system. The configuration file contains plugins, web injection code, and a collector's list to direct exfiltration of stolen data. SpyEye can inject HTML attack code into Firefox, Internet Explorer, Chrome, and Opera browsers.

Attackers use SpyEye to steal banking information in two ways. One is via a keylogger application, which captures all keystrokes entered into a web form and saves the stolen data into a log file. The other is the bot's ability to take screenshots on the victim machine. The bot is activated when a bank website is loaded into the victim's browser. SpyEye intercepts transmissions with the site, steals the login credentials, and sends those to the attacker's command-and-control center. All this happens in the background so the victim is unaware of the theft of credentials and subsequent financial account breach.

**Links**

http://blog.kaspersky.com/the-big-four-banking-trojans/
http://krebsonsecurity.com/tag/spyeye/
http://www.newsweek.com/2014/03/21/500000000-cyber-heist-247997.html
Torpig

Aliases: Sinowal, Answerin, Mebroot

What

Torpig is used to steal targeted login credentials to access bank accounts and financial systems. Other applications include modifying data on infected computers and loading additional malware for secondary objectives. Torpig is a botnet spread by a Trojan horse called Mebroot that infects Windows-based PCs. It sidesteps antivirus software with a rootkit, which hides its subsequent execution of processes to gain unauthorized access to the victim. Detection is difficult because Torpig hides its files and encrypts its logs. Once Torpig gains access, it scans the infected PC for account data and access credentials. By 2008, Torpig was considered to be highly advanced malware. In 2009, researchers accessed the botnet and conducted considerable analytics on its operations. Torpig continues to be used by criminals to breach bank accounts and other financial systems.

How

Torpig uses the "Man-in-the-Browser" technique to exploit vulnerabilities in browsers to steal information such as ftp passwords, email addresses and credentials for bank accounts. The malware uses phishing to carry out malicious activities. Figure 2, from the IEEE, shows the process flow from infection to exploitation.

Step 1: Attackers modify vulnerable webpages.
Step 2: Modified page redirects victim’s browser to drive-by download server.
Step 3: Vulnerable browser requests JavaScript.
Step 4: Victim downloads and executes Mebroot to become a bot.
Step 5: Bot obtains Torpig modules.
Step 6: Bot uploads data stolen from victim’s computer.
Step 7: When browsing a targeted site, victim is redirected to HTML injection server to execute Man-in-the-Browser attack.

Links

http://en.wikipedia.org/wiki/Torpig
http://www.cmu.edu/iso/aware/be-aware/torpig.html
Vawtrak

**Aliases:** Snifula, Neverquest, Papras

**What**

Vawtrak is a backdoor and a sophisticated, dangerous banking Trojan able to spread itself via social media, email and file transfer protocols. It may arrive as unsolicited email pretending to be an “ACH Notification,” a “rejected FED TAX payment,” or a “Fax from Epson.” After it infects a victim PC, Vawtrak steals bank account credentials and sends them to its command-and-control server. The hacker can use a virtual network computing (VNC) server to take control of the compromised computer and use it to access the bank account and perform the theft. Vawtrak also can modify the content of a web page and inject rogue forms on bank sites.

Vawtrak’s unique feature is being able to hide evidence of the fraud by changing (on the fly) the balance shown to the victim. It uses a classical Man-in-the-Browser attack similar to Zeus. It also can recognize hundreds of financial institutions and contains a function that monitors certain keywords, allowing the cyber criminals to expand the list of targeted banks.

**How**

Vawtrak is a sophisticated piece of malware in terms of supported features and extensibility with regular updates of available command-and-control servers, Vawtrak executable, and web-inject frameworks. As polymorphic malware, it features a small, efficient client written in Microsoft Visual C and provides all standard spyware functions. Vawtrak will log keystrokes; take screenshots and video captures; open a remote command shell; download and run files; check what processes are running on the victim PC; capture a list of visited websites; delete the browser cache and files; steal digital certificates and cookies on the PC; and start or stop processes like the browser, Windows Outlook, Windows Explorer, Command prompt, and Task Manager.

The Russia-based command-and-control center hides Vawtrak’s processes. Update servers are hosted on the Tor “dark web” and communication is via SSL/TLS. Communication is done only while the user is browsing the Internet and producing network traffic “cover” to avoid exposing Vawtrak operations. For example, Vawtrak uses steganography by hiding update list inside favicon’s 4kB favicon image files to carry data in the least significant bits. A “Pony module” enables Vawtrak to harvest email clients, file transfer protocol and stored browser credentials. While Vawtrak focuses on financial targets, Cyphort has detected other attack sectors such as gaming, social networks and media.

**Links**

http://blog.phishlabs.com/the-unrelenting-evolution-of-vawtrak
http://blog.phishlabs.com/vawtrak-gains-momentum-and-expands-targets
https://securelist.com/analysis/publications/57881/online-banking-faces-a-new-threat/
Bebloh

**Aliases:** URLzone, Bublik

**What**
Bebloh is banking malware used to steal targeted login credentials, intercept online banking transactions, and breach financial systems. Bebloh is a Trojan horse computer worm that targets PCs running versions of the Windows operating system. Its unique feature is the ability to hide evidence of the fraud by changing (on the fly) the balance shown to the victim.

Bebloh uses a classical Man-in-the-Browser attack methodology. After infecting the user’s PC with the Bebloh Trojan, the PC is automatically connected to the attacker’s command-and-control server and receives instructions. Typically this entails stealing the user’s login credentials, and subsequently stealing specific amounts of money from the user’s account. The attacker protects his identity by collecting the money through an online “money mule.” Bebloh monitors HTTP for the bank site and modifies the numbers in real time such that if the user sees the transactions, they will be innocuous to avoid drawing suspicion. Bebloh is careful not to draw down the account below balance.

**How**
While Bebloh is similar to other banking malware, there are notable characteristics. Distribution has occurred via spam mails, according to a report from Trustwave. The mail contains a malicious PDF attachment in which the payload is Bebloh. The malicious PDF file exploits vulnerability in Adobe Reader 9.3 and earlier, which crashing that application and executes the malicious code. Bebloh modifies the registry to force the use of Internet Explorer, even if the user launches Chrome, Opera, Safari, or Netscape Navigator. It disables use of a proxy and monitors keywords entered into the browser, including: banking, portal, banking.postbank.de, meine.deutsche-bank.de, and interbanking.gad.de. Bebloh encrypts its data before sending it to the command-and-control server. After downloading its configuration file, Bebloh encrypts it along with data for the target bank in the %system% folder with a random file name.

Bebloh persistently evades antivirus detection by deleting the original Trojan file after injecting its code into explorer.exe. The malware runs hidden in explorer.exe memory, which leaves no trace of a malicious process. Figure 4 shows how Bebloh waits for a message announcing system shutdown, writes its executable file out of explorer.exe memory to the hard disk, and creates an autostart file pointing to the new executable malware. The autostart entry does not directly reference the executable file; it relies on a link (.lnk). The new executable gets a new randomly generated filename upon each shutdown. Thus, there is no visible clue of its presence in the registry or on the hard disk while the malware is running.

**Links**
Shylock

**Alias: Caphaw**

**What**

Shylock is another banking Trojan targeting login credentials for European banks via Man-in-the-Browser exploits. Shylock has infected at least 60,000 computers running Microsoft Windows worldwide. The Shylock moniker stems from excerpts of Shakespeare’s play, The Merchant of Venice, embedded within the malware code. The attackers behind Shylock have an advanced, targeted distribution network that allows them to infect victims in selected countries through multiple channels. For example, distribution has been spotted in YouTube malvertisements and through Skype. The malware is also known to be distributed with the Blackhole and other exploit kits. The malware is modular in nature, which allows the attackers to easily extend or change its functionality. The Shylock Trojan is privately owned and not for sale on the underground market. Its owners have a professional attitude and Shylock has been continually updated in response to security countermeasures employed by targeted banks. Shylock was first spotted in 2011. A coordinated international effort in 2014 by law enforcement agencies and security industry organizations substantially reduced the use of Shylock, but it remains a persistent threat to online banks and financial institutions.

**How**

Shylock’s use of Man-in-the-Browser works like other banking Trojans as it attempts to steal login credentials and financial information via infected PCs. One of its signature traits is persistence in evading detection by antivirus and antimalware scans. To do this, Shylock uses a process similar to that used by Bebloh, where it drops itself into temporary files and creates a run entry to self-execute on system reboot. Browsers subject to infection include Internet Explorer and Firefox. Theft of login credentials usually occurs from ftp clients and Microsoft Outlook.

**Links**

https://www.europol.europa.eu/content/global-action-targeting-shylock-malware
https://securelist.com/blog/research/64599/shylockcaphaw-malware-trojan-the-overview/
http://en.wikipedia.org/wiki/Blackhole_exploit_kit
Dridex

**Aliases:** Cridex, Feodo, Bugat

**What**

Dridex is another sophisticated banking Trojan targeting login credentials for banks globally via Man-in-the-Browser exploits, similar to Zeus banking malware. Dridex relies on phishing to carry out malicious activities. It has executed malicious code on victim PCs via executable attachments, and Microsoft Word documents containing macros that download a second-stage payload, which then downloads and executes the Trojan.

Dridex has globally infected victim PCs, with more than half in the US.

**How**

Dridex's use of Man-in-the-Browser works like other banking Trojans as it attempts to steal login credentials and financial information via infected PCs. An XML-based configuration file specifies targeted banking website and malware options. When the victim-infected machine visits a targeted banking site, Dridex sends a request to its injection server, which presents a login page similar to the banking site. The injection server then drops a .dll file onto the victim PC and downloads the manager module. The manager module is responsible for stealing the bank information. It downloads other plugins responsible for stealing different sensitive information from the system such as ftp passwords, email addresses and bank accounts. Dridex uploads this information to the command-and-control server. Unlike other banking Trojans, Dridex can act as a Remote Access Trojan (“RAT”), which allows an attacker to control the victim PC as if the operator had physical access to the system.

**Links**

https://www.proofpoint.com/us/threat-insight/post/LogIn-Waz-Here
http://www.bankinfosecurity.com/bugat-new-malware-choice-a-3011

---

Figure 5. Dridex has infected victim PCs around the world. (Source: PaloAltoNetworks.com)
Dyre

Alias: Dyreza

What
Dyre is another dangerous banking Trojan targeting login credentials for banks globally via Man-in-the-Browser exploits, similar to Zeus banking malware. Dridex relies on phishing to carry out malicious activities. It often uses malicious PDF attachments that can exploit unpatched versions of Adobe Reader. The emails may use the misspelled subject line “Unpaid invoic” as well as the attachment “Invoice621785.pdf.” Dyre uses infected victim PCs to harvest credentials for bank accounts and other online services.

How
After the Dyre Trojan infects a victim PC, it initiates a Man-in-the-Browser attack by sending user information to its command-and-control server for bot configuration. The server sends a webinject configuration file to the victim PC in encrypted form. After setup, the victim PC can intercept SSL traffic in browsers to steal login credentials during authentication processes. The Man-in-the-Middle proxy server intercepts user requests to target banking sites and returns bogus data such as fake login pages and popup screens. Following acquisition of critical data, the attacker can remotely control the victim PC with a built-in Virtual Network Computing module to perform banking transactions and exfiltrate data.

Links
https://www.us-cert.gov/ncas/alerts/TA14-300A
https://devcentral.f5.com/articles/dyre-malware-analysis
Conclusion

The threat of cyber criminals using financial malware is a clear and present danger to banks and other financial institutions. Financial malware campaigns to steal your money are targeted, persistent, and can be very effective because they evade detection by traditional signature-based protection such as antivirus scanners. The authors of financial malware continuously change and fine-tune capabilities that can easily drain bank accounts before customers or security professionals are aware of the attack.

To successfully defend attacks with financial malware, it is critical for your company to explore and deploy advanced threat protection solutions. The goal here is to accurately detect and analyze financial malware, and provide your first responders on the security team with actionable, contextual intelligence that empowers them to respond to attacks faster and more effectively. Your responses must be nimble and surgical. As a result, you will be able to minimize the threats of financial malware, avoid potential legal and regulatory penalties, and ensure the confidence of your customers. Cyphort is an innovative provider of advanced solutions that deliver a complete defense against financial malware, and other targeted attacks and vulnerabilities.

Contact us to learn how we can help info@cyphort.com

About Cyphort

Cyphort is an innovative provider of Advanced Threat Protection solutions that deliver a complete defense against current and emerging Advanced Persistent Threats, targeted attacks and zero day vulnerabilities. Cyphort’s unique software solution delivers complete Next Generation APT defense, correlating threats from Web and Email, as well as internal vectors for lateral spread and post breach activity detection. The addition of correlation and context for each threat plays a key role in helping prioritize responses and containment actions. The purpose-built integrations to existing enforcement solutions (Firewalls, Proxies etc.) allows customers the ability to extract maximum value from IT assets without compromising the security of an organization. Cyphort is a privately held company headquarterd in Santa Clara, California. For more information, please visit www.cyphort.com and follow us @Cyphort.