IBM Software

Thought Leadership White Paper

February 2015

Battling fraud at the root cause

How cybercriminals bypass your security defenses and what you can do about it

Contents

Introduction

In the 2014 IBM Chief Information Security Officer assessment, nearly 60 percent of security leaders interviewed felt that “the sophistication of attackers was out stripping the sophistication of their organization’s defenses.”[1]

It’s no wonder. Analysis of attacks over the years have shown that cybercriminals are studying their prey closely—understanding the security solutions, policies and procedures each bank implements—and devising successful countermeasures to circumvent their targets’ protections.

Today, banking malware, such as Citadel, Zeus, Dyre and Bugat, incorporate advanced functionality that enables attackers to “fly under the radar” and elude detection by both the end user and banking security systems.

In fact, recent attacks have shown that once a user’s endpoint is infected with advanced malware, criminals can bypass most security layers, including two-factor authentication, device ID systems, risk engines and behavioral analytic systems.

Effectively combating cybercriminals requires understanding how they operate. How do they render endpoint protection solutions inoperable? What methods do they use to sidestep two-factor authentication? How do they trick device ID systems and behavioral analytic and risk engines into believing their transactions are legitimate?

This white paper provides an overview of how cybercriminals circumvent security measures at each stage of a transaction’s lifecycle—pre-login, during login and post-login—and offers strategies to help financial organizations combat malware-driven attacks.

Why malware is the weapon of choice for cybercriminals

Of the most common threats used in financial fraud—phishing, social engineering and malware—malware has emerged as the weapon of choice for financial fraudsters.

That’s not to say that cybercriminals aren’t using phishing or social engineering to help them obtain user credentials and ultimately steal funds. In fact, in its trends report for the second quarter of 2014, APWG reported the second-highest number of phishing sites ever observed in a quarter.[2]

Phishing and social engineering remain viable and effective methods for stealing user credentials. However, to evade all of a financial institution’s security layers and complete a fraudulent transaction, more advanced and stealth capabilities are needed—and that’s where malware comes in.

Criminals gain immense power

Early variants of banking malware featured basic keylogging capabilities to steal user credentials. Virtual keyboards were promoted in response to protect user credentials from keyloggers. Cybercriminals fired back by adding screen scrapers and form grabbers to their malware so they could capture credentials entered by virtual keyboards. And the battle continued.

Each time banks add new security measures to protect their customers, cybercriminals simply build better malware. In addition to keylogging, screen scrapers, and form grabbers, banking malware now commonly include sophisticated functions that give criminals immense power when launching an attack. These functions include:

- HTML injection that enables attackers to inject HTML content into a legitimate Web page in order to modify the page and steal information from the user. They can display fake security warnings, request credentials and other personally identifiable information (PII), and more.
- Evasive capabilities that can automatically shut down antivirus programs before the malware is downloaded, and even stop installation of the payload in potentially hostile environments (such as sandbox environments).
- Encryption to help thwart attempts by security researchers to analyze the malware and combat its operations.
- Video capturing to record a user's login process and see exactly how the user interacts with the online banking application, helping the fraudster better mimic the user's online behavior.
- Remote control capabilities using Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC) that give cybercriminals full control over a user's PC and enables them to launch an attack directly from a user's system.

Consider, for example, one variant of the Bugat malware that incorporates multiple elements for stealing credentials, overcoming two-factor authentication, dealing with IP reputation and other counter-security measures. In attacks using this variant, users with infected endpoints never reach the real bank login page. Instead, they are directed to a malicious site and are requested to provide their login information. In real time, the criminal captures the credentials and connects to the bank via the victim's IP address. If the bank requests more information from the criminal during the transaction process, such as a one-time password or an answer to a security question, the criminal can obtain these data elements using HTML injection. These requests are presented to victims in real time.

How cybercriminals use malware to evade your defenses

Using these powerful functions embedded in today's banking malware, cybercriminals can bypass security protocols at all three points of the user's interaction:

1. Pre-login: before users log in to their accounts
2. Login: while the user is logging in to an online banking session
3. Post-login: after an authenticated session has been initiated and transactions can be performed

Pre-login: Downloading the exploit

For cybercriminals, the first goal in initiating fraud is simply getting the malware on the victims' endpoints before they log in to their online banking sessions.

To do so, the criminals must potentially bypass two security layers—first, a user who has been educated by the bank about malware, and second, endpoint protection solutions. Three techniques have evolved to help criminals achieve their goal.

Leveraging mass distribution capabilities

Consumer education has helped users better understand the risks they face when banking online and become more skeptical of unknown links and attachments. As a result, cybercriminals use mass distribution techniques, such as drive-by downloads, watering-hole attacks, and malvertising to silently infect user PCs without the user's knowledge. There's no link or attachment the user must click on. Users can simply become infected as they visit legitimate websites.

Bypassing endpoint protection solutions

The hope is that even if infection is attempted, endpoint protection solutions will detect and prevent installation of the malware. However, attackers have designed malware with these solutions in mind. Evasive software embedded in the malware act as a scout to obtain vital reconnaissance about the endpoint before it deploys the malware. This defensive layer can identify if endpoint protection software is present and initiate a "kill" sequence that shuts the security software down—all while leaving the icon in the system tray to trick users into believing that they are still protected.

The software can also search for any indications, such as the use of virtual environments, sandboxes or reverse engineering tools, that the endpoint may be used by security researchers to investigate malware. If the program identifies one of these potential hazards, it can abort the mission to download the payload and tag the device so the cybercriminal can study it at greater length in the future.

Thwarting security researchers

As a defensive layer, cybercriminals also have developed ways to prevent security researchers from analyzing the malware code. By running their malware through cryptography programs, called Crypters, cybercriminals can easily encrypt their code, so even when security researchers uncover new variants of malware, they can't easily reverse engineer the software to understand and combat its operations.

It's important to note that Crypters have become so popular that an entire industry has sprouted in the underground to support it, and attackers can now outsource the work to crypting services.

Login: Initiating an authenticated session

Once the user's endpoint is infected, the attacker's next goal is to initiate an authenticated session. They must remain undetected by the user, bypass authentication measures, including any two-factor authentication solutions required during login, and outsmart device ID systems and risk engines.

There are a number of approaches cybercriminals can use to accomplish their goals.

Stealing credentials with HTML injection

HTML injection is a classic feature of man-in-the-browser (MitB) attacks to steal credentials from users logging in to their online banking site. Cybercriminals can inject forms into the financial institution's web application that pretend to gather the user's credentials and as well as one-time passwords.

Stealing credentials on mobile devices

It's not surprising that as more users access their bank accounts with their mobile devices, cybercriminals have developed new mobile malware to steal credentials through this channel as well. Svpeng has emerged as a PC-grade mobile malware designed to perform overlay attacks. Once downloaded on a user's mobile device, the malware silently observes what appears on the user's screen. As soon as the user accesses an online banking site, the malware initiates an overlay attack to capture the user's credentials and other financial information.

Forging device IDs

Once cybercriminals capture the user's credentials and any one-time passwords, they must still bypass device ID systems, which will block sessions coming from suspect systems.

Device forging systems enable criminals to mimic the attributes of the user's device, including operating system, language and IP address, so they can log in from their own devices without red flags.

Taking control of user devices

While device forging tools enable cybercriminals to mimic a user's device, remote control capabilities, such as RDP or VNC, embedded in banking malware enable criminals to initiate fraud directly from the user's device.

Once the victim logs in to his or her online banking session, the attacker is notified and can initiate remote control to take over the authenticated session using the victim's machine. The user sees a message "from the bank" to wait for security reasons and the criminal can perform a transaction in the background unbeknownst to the user.

From the device ID system's perspective, the session is originating from the user's device, and therefore is not suspect.

Most advanced types of malware have this ability today, including SpyEye's use of RDP, and Zeus' and Citadel's use of VNC. And, this type of attack has been so successful that new Citadel variants can ensure VNC capabilities remain persistent on the targeted device even if the Citadel malware is removed.

Riding the session with automatic transfer systems

Automatic transfer systems (ATS) enable cybercriminals to successfully transfer money from a user's bank account instantly—even before the victim reaches the bank's welcome screen. As soon as a user's credentials are approved, the malware runs a script that launches a series of commands to transfer money to a mule account. The session is authenticated, and the script and transfer run in the background. From the bank's perspective, it appears as if the user initiated the money transfer. Cybercriminals often combine ATS attacks with HTML injection so when the welcome screen does appear, users see their original balance instead of the actual balance following the fraudulent transfer.

What's more, as risk engines became better at detecting ATS activity, cybercriminals updated ATS scripts so that the process occurs much more slowly so as to appear more human than automated.

Gathering intelligence before an attack

Not all solutions to bypass bank security require complex technological capabilities. Cybercriminals track and share not only what security solutions banks use, but also what security procedures they have in place. This insight is often used to trick both device ID systems and risk engines.

For example, in one case, IBM® Security Trusteer® researchers were asked by a large European bank to examine more than 10 million login attempts for three weeks across 1.5 million accounts. Interesting insight was obtained.

The researchers found that cybercriminals were circumventing the bank's device ID system simply by logging in and out of a victim's account daily without performing a transaction. The attackers waited patiently knowing that after two weeks, the device ID solution would add their devices to its database of trusted devices since no high risk transactions or operations were performed.

During this examination, researchers also found that the criminals were also using mobile devices to bypass the bank's device ID systems. Since mobile device characteristics are very similar across device types, device ID systems often can't distinguish a criminal from a legitimate user logging in to the online banking system. In their examination, the researchers found that 30 percent of users were accessing the online banking platform via the browser from a mobile device and they were able to confirm fraud attempts from the mobile channel.

Post-login: Performing the transaction

The final step in the fraudster's attack is transferring the victim's money to a mule account. To do so, cybercriminals must outwit behavioral analytic and risk engines, and circumvent any additional two-factor authentication.

Bypassing two-factor authentication

As mentioned earlier, HTML injection is commonly used to not only steal user credentials, but also enable cybercriminals to obtain one-time passwords required to initiate transactions, such as ACH or wire transfers.

Using HTML injection, the fraudster can collect the one-time password in real time while blocking the user for several minutes from accessing the genuine bank web site. HTML injection is also often used to gather personally identifiable information for use in cross-channel attacks for high-risk activities, such as adding a new payee. Once the information is captured, the criminal has everything needed to contact the call center and add a payee.

Cybercriminals can also use remote control capabilities to bypass two-factor authentication required to process transactions. Take the case of another European bank that required commercial customers to use SmartCard readers prior to initiating a transaction. Criminals circumvented the system using remote control capabilities coupled with intelligence.

Once the user's device was infected with RDP-capable banking malware, the cybercriminals monitored usage over the course of the month and found that the user inserted the SmartCard inside the reader each morning and didn't remove it until the end of the day. The fraudster then simply waited until the user went to lunch, took control of the device and initiated the fraudulent transaction.

Outsmarting behavior analytics

Video capturing enables cybercriminals to record a potential victim's online behavior. Why would they go to the trouble? It offers them the ability to understand how users interact with their online banking applications. Which pages do they navigate, and in which order? When do they typically pay their bills online? How quickly do they enter information and move from page to page? Attackers can then use this intelligence to emulate a user's behavior and outsmart behavior analytic engines.

What you can do to stay ahead

Given all the tools that cybercriminals have to circumvent security, what can you do?

Fighting fraud requires the same building blocks as counterterrorism efforts: prevention, detection, mitigation and remediation.

No single building block is sufficient today. By implementing robust strategies at each level, financial institutions can more effectively fight fraud.

Prevention

An important step in battling fraud at the root cause is prevention—stopping the malware infection in the first place. How quickly can your endpoint protection solutions adapt to new threats? How do your solutions protect against zero-day threats? How will you know if the endpoint protection software has been disabled? Real-time monitoring of customer endpoints is the first step of any effective prevention strategy.

Additionally, monitoring the landscape provides insight into what malware cybercriminals are using now, how they're using it, how it's migrating from region to region, and how it is changing. With this insight, institutions can initiate countermeasures to stay one step ahead.

Detection

Detecting financial fraud in today's landscape requires an integrated approach to threat detection as criminals will look to exploit any holes in your architecture.

Can you correlate data from multiple sources and multiple channels to conclusively detect an attack? Does your online banking solution talk to your check fraud solution? Does your endpoint protection system talk to your risk engine?

Additionally, how quickly can you analyze the data and uncover potential criminal activity? Real-time analysis is essential for early detection.

Mitigation

When an attack occurs, how quickly can you respond and mitigate the damage? How quickly can you implement countermeasures to prevent similar attacks in the future? Speed again is vital. Real-time application of security intelligence is essential to minimize any damage.

Remediation

The first step of remediation is often re-credentialing users. However, if the user's credentials were stolen via malware versus a phishing attack, re-credentialing won't solve the problem. As a result, financial institutions need processes in place to help customers clean their devices.

At each stage, transparency is essential—for both end users and security staff. Given the challenges security teams face today, fraud protection processes, policies and technologies must be easy to implement and easy to adapt so that security professionals can remain focused on the big picture. Minimal customer intervention and inconvenience is also required, especially to drive adoption of endpoint protection solutions. As many banks have found, when security measures become burdensome, users find a workaround, leaving a gap that criminals can exploit.

Conclusion

There's no silver bullet when it comes to stopping fraud. As financial institutions have deployed more sophisticated security solutions, criminals have created more sophisticated and evasive tactics to bypass bank security and steal funds.

More effectively battling malware-driven fraud requires real-time, adaptable and transparent strategies for prevention, detection, mitigation and remediation that span every point of the user's interaction—pre-login, during login and post-login.

For more information

To learn more about how to battle fraud at the root cause, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

About IBM Security Trusteer software

IBM Security Trusteer software delivers a holistic endpoint cybercrime prevention platform that helps protect organizations against financial fraud and data breaches. Hundreds of organizations and hundreds of millions of end users use IBM Security Trusteer solutions to protect their web applications, computers and mobile devices from online threats, such as advanced malware and phishing attacks.

Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
February 2015

IBM, the IBM logo, ibm.com, Trusteer, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

[1] Marc van Zadelhoff, Kristin Lovejoy and David Jarvis, "Fortifying for the Future: Insights from the 2014 Chief Information Security Officer Assessment," IBM Center for Applied Insights (Research report), p. 3, December 2014. Retrieved from: http://www.ibm.com/smarterplanet/us/en/centerforappliedinsights/article/ciso_insights.html

[2] APWG. (August 28, 2014). APWG Phishing Trends Activity Report 2nd Quarter 2014 [Trend Report]. 4. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf

Please Recycle