The thriving malware industry: Cybercrime made easy

Technology and processes from IBM Security help your organization combat malware-driven fraud and achieve sustainable threat prevention

Contents

Introduction

The malware industry supplies all the components cybercriminals need to easily perpetrate malware-driven financial fraud and data theft. In today's virtual world, the scope of organizations vulnerable to malware-driven cybercrime is quite broad. In addition to banks and credit unions that are subject to online banking fraud, financial fraud can be perpetrated on insurance companies, payment services, large e-commerce companies, airlines and many others.

Most attacks do not target an organization's systems directly, but rather, their customer and employee endpoints. The reason for this is that organizations have invested substantially in multiple layers of security, such as firewalls, intrusion prevention systems and anti-virus gateways, in order to filter out cybercriminals on the perimeter. Conversely, for endpoint security, organizations have leveraged anti-virus software, which often detects less than 40 percent of financial malware.[1] Consequently, cybercriminals focus efforts on conducting malware-driven cybercrime, utilizing malware on user endpoints to commit financial fraud and steal sensitive data.

Seven basic steps for conducting malware-driven financial fraud

A vast array of tools and infrastructure services is available to aid cybercriminals engaged in fraudulent activities. However, for the sake of simplicity, this white paper will focus on one type of fraudulent activity—online banking fraud. Executing malware-driven fraud from the planning stage to the cash-out stage requires that cybercriminals follow seven basic steps:

- Step 1: Understanding online banking attacks
- Step 2: Setting up the supporting infrastructure
- Step 3: Obtaining and configuring malware
- Step 4: Infecting a significant number of end users
- Step 5: Avoiding detection by anti-virus applications
- Step 6: Malware attacks—executing fraudulent transactions
- Step 7: Cashing out—withdrawing the stolen funds

Step 1: Understanding online banking attacks

Successfully orchestrating fraud requires in-depth understanding of malware technology and how to set up the supporting infrastructure—often referred to as "cybercrime prepping." As with most other disciplines, materials on how to perpetrate online banking fraud are readily available for free on the web, including documents, forums and even training videos. In addition, more formalized training is available for a fee.

Furthermore, our research has identified training courses for creating malicious botnets—that is, networks of compromised endpoints centrally controlled by malware operators. These

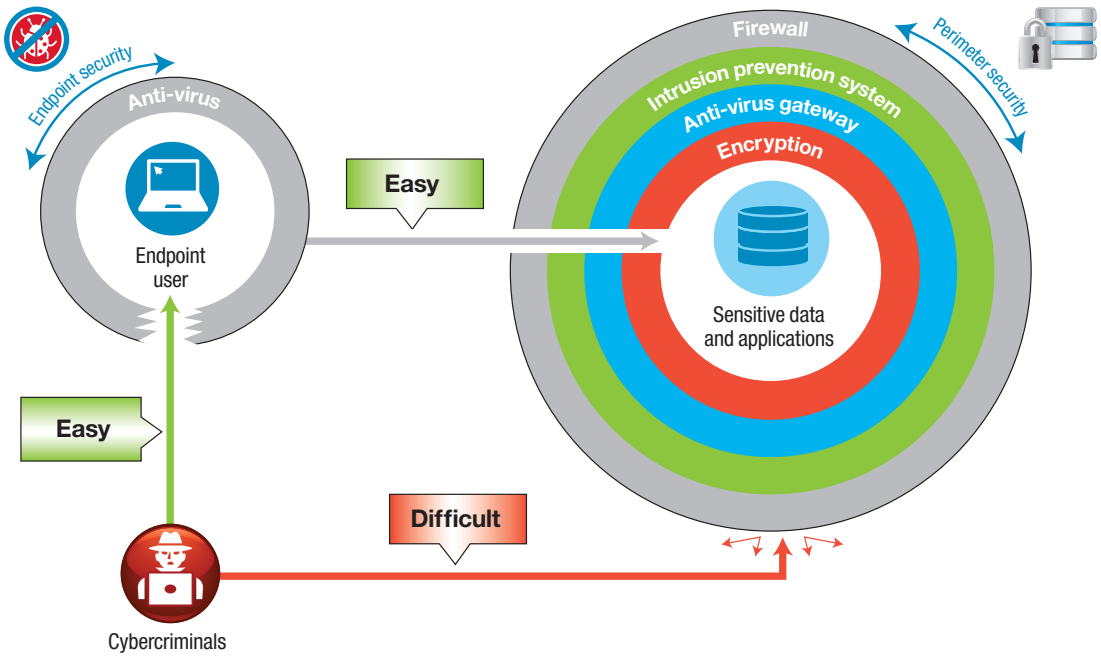


Figure 1: Cybercrime using malware on endpoints

courses discuss malware botnet installation and modification, as well as how to write web inject code or web page alterations and custom scripts. The training programs are well organized and include fully developed lessons with training guides and videos—all delivered in English. The companies claim that their customers do not require any special programming skills. The training package is equipped with unlimited versions of malware kits such as ZeuS and SpyEye with modules and web injects.

Step 2: Setting up the supporting infrastructure

Like any IT system, malware needs a sophisticated infrastructure to function effectively. Malware installed on end user machines (comprising a botnet) requires an open communication with a web-based cybercriminal command-and-control center. Upon infection, malware typically contains a predefined set of malicious configurations that include a target bank URL and web injects to perpetrate a man-in-the-browser attack. However, not all information is included in the initial configuration.

For example, payee or "mule" account information is extracted on the fly from the command-and-control center. In some cases, configurations that include new targeted banks and modified attacks are also updated post-infection via the command-and-control center. Malware that captures credentials needs to send this information to an external storage location, called a drop zone, which cybercriminals can access to extract the information.

Effectively operating a malware botnet requires servers to host command-and-control operations and credential drop sites. However, a variety of hosting and command-and-control services are available to cybercriminals online. One recent service discovered by IBM Security intelligence advertised bulletproof hosting services and dedicated servers for hosting malicious malware. The service, according to the advertisement, provides administrative tools, 24x7 technical support and an abuse- or distributed-denial-of-service (DDoS) attack-proof hosting service, which promises unlimited traffic and anonymity to the owner.

Step 3: Obtaining and configuring malware

Although cybercriminals require malware to perpetrate attacks, most cybercriminals do not have the technical skills or appetite to invest in developing their own malware. This "cybercrime market gap" has not escaped the eyes of hungry software developers, who create and sell off-the-shelf malware development kits that include the functionality required to perpetrate financial fraud.

Obtaining malware development kits

Commonly used malware kits such as ZeuS include malicious functionalities that include key-logging, screen capturing, HTML injections and certificate siphoning. Most malware development kits also provide application programming interfaces (APIs) that enable skilled cybercriminals to extend the basic development kit with additional custom-built code.

As early as 2009, analysts estimated that the ZeuS development kit was used in botnets compromising more than 3.6 million computers in the US alone.[2] During 2012, the FBI arrested more than 10 members of an international cybercrime network suspected of using ZeuS to steal more than USD70 million from hacked US computers.[3] Eventually, in May 2011, the ZeuS source code was leaked on several underground forums and other channels, making it readily available at no cost.[4]

Configuring malware development kits—web injects

Malware development kits provide the technical platform for conducting fraud, but it is still up to cybercriminals to configure malware to address a specific target. A major malware component, part of the attack configuration, is called a web inject. Man-in-the-browser attacks require cybercriminals to alter web pages of online banking websites—for example, by adding extra fields to collect credentials information or, in more elaborate social engineering attacks, by adding a set of pages that instruct users to install software or provide strong authentication information.

Developing web injects for a fraud requires highly skilled web developers and in-depth familiarity with the targeted website, as each web inject is specifically crafted to address a specific website. Nevertheless, cybercriminals lacking the relevant skill set can buy web injects on the open market. A typical price for a single web inject pack is USD60, while an entire pack to target several UK banks costs USD800. Typical update costs are USD20 each. One online forum advertised the price for a large pack of web injects at only USD15-20.[5]

Step 4: Infecting a significant number of end users

Once cybercriminals obtain and configure malware, they need to distribute the malware to infect their intended victims. To facilitate this, cybercriminals offer a variety of malware-distribution services for hire. As just one example, in 2011 IBM Security intelligence identified cybercriminals who sell infection services on the open market. For a minimum of 2,000 infections, one such service costs about 0.5 cents to 4.5 cents for each upload, depending on geography.[6]

Leveraging botnets

Some cybercriminals have been able to infect a large number of end user victim machines with malicious software, creating networks of infected machines that are controlled remotely. These are called botnets. Botnets are used for various cybercriminal activities, such as denial-of-service (DoS) attacks and sending spam. Machines that are part of a botnet are also infected with malicious software called a downloader. This software can download and install files on a machine without the victim's knowledge. To further capitalize on botnets, cybercriminals offer to download and install software on host machines—allowing cybercriminals, for a price, to provide botnet owners with preconfigured financial malware to be installed on botnet machines.

Drive-by downloads

Cybercriminals also infect end user machines by creating drive-by downloads, which exploit vulnerabilities in browsers and operating systems. With this tactic, cybercriminals incorporate exploit code into websites they set up or break into. Once a website has been embedded with exploit code, users are tricked into accessing the infected website instead of the legitimate website. Spam email, short message service (SMS) and fake social networking messages are common ways of luring users to enter exploit-infected websites. Exploit code kits are readily available for purchase on the open market, and cybercriminals can take advantage of these tools to create exploit code. However, not all cybercriminals possess the same level of expertise or aptitude required to successfully use exploit code. Instead, cybercriminals offer infection services that leverage exploit code.

Step 5: Avoiding detection by anti-virus applications

Most end user machines are protected by anti-virus software designed to prevent systems from being infected by undesired software such as financial malware. In response, effective infection campaigns advertise ways to avoid detection by anti-virus software. Anti-virus software vendors collect samples of malware files and apply a mathematical function on them to generate a unique signature for a given file. The software then propagates the malware file signatures to all endpoints that have the anti-virus application installed, so when a known malicious file tries to infect the machine, it is blocked. Since anti-virus protection is based on unique file signatures, cybercriminals have devised ways to frequently change malware files without changing the underlying crime logic or coding effort.

Polymorphic crypting

Crypting or "polymorphic crypting" of files is a common method of generating different malware files with different signatures. However, the crypting process requires savvy technical personnel. Cybercriminals have addressed this need by introducing file-crypting services that are widely advertised on black market forums. According to a recent advertisement, cybercriminals offer polymorphic crypting of malware files with their custom-designed cryptor, which supports all types of operating systems. The crypted files are used to bypass anti-virus security, inject system processes and launch other attacks.

Anti-virus checkers

Anti-virus checker services allow criminals to determine—prior to release—whether a specific malware file is detectable by anti-virus solutions. The service includes setting up multiple virtual environments with a variety of up-to-date versions of commonly used anti-virus software, and attempting to infect these environments with a malware sample.

Step 6: Malware attacks—executing fraudulent transactions

Online banking malware fraud can require multiple stages of attack at different stages of the process.

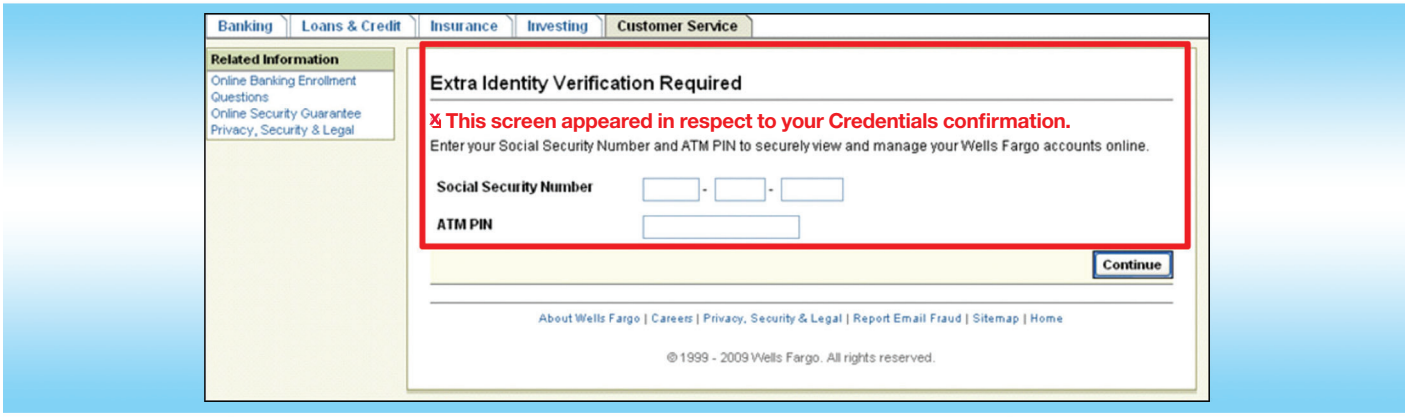
1. On login, cybercriminals use man-in-the-browser attacks to steal credentials from users logging in to legitimate banking websites. These attacks can inject fields into the login screen and obtain credentials even if they are entered via a virtual keyboard or two-factor authentication, such as requirements for one-time passwords.
2. Post-login, immediately after authenticating to an online banking website, malware can inject and subsequently capture an HTML page that requests additional credentials information from the user "for security reasons." Other post-login attacks consist of sophisticated man-in-the-browser techniques that redirect one-time passwords sent via SMS to cybercriminals[7] or convince end users through social engineering to perform the fraudulent transaction themselves.
3. In-transaction malware can "piggyback" on an authenticated money transfer transaction, changing its content on the fly—for example, changing the payee and the amount.
4. Post-transaction malware conceals the fraudulent activity from the end user. IBM Security research has identified malware hiding confirmation messages and modifying the balance and transaction details presented to the end user.[8] The FBI has warned users about a new type of post-transaction attack that leverages DDoS to prevent fraudulent transactions from being reversed.[9]

Figure 2: Login with additional malware-injected fields ("Generated Token Password" and "Wire PIN")

Step 7: Cashing out—withdrawing the stolen funds

Eventually, cybercriminals need to access the money they have stolen and to do so without leaving any trail that would lead back to them. Since most online banking transfers leave digital footprints, successful fraud requires cybercriminals to cash out funds—that is, withdraw them from ATMs and via wire transfers—after which the money is not traceable. Cybercriminals use various techniques to "hire" people who perform this cash-out process. Typically unaware of the illegal nature of their actions, these people are known as "mules."

However, not all cybercriminals have set up their own mule network. This service is widely available online as well. IBM Security research has found cybercriminals who advertise bank transfers and cashing services for money laundering purposes, or "mule-type" services. These criminals, who also sell stolen credit cards and bank-user details, charge commissions on the transfers they make. The advertisers mainly offer bank transfers and online money transfers via electronic money and online payment systems. The commissions generally depend on the amount transferred (discounts are often provided for high amounts), but mostly range from 5 to 10 percent. Mule service vendors compete with each other on transaction speed. Offered transaction performance time is 15 to 45 minutes via payment systems and a few hours via bank transfers.



Injected forms pretend to gather further credential information from the customer under the pretense of "Extra Identity Verification Required."

Figure 3: Malware forms in a financial institution's web application

Protecting against cybercrime with IBM Security solutions

Hundreds of financial institutions and organizations and tens of millions of their customers rely on IBM Security Trusteer products to protect their computers and mobile devices from online fraud and data theft. The global footprint, industry-standard technology and proven processes offered by IBM Security are designed to enable our customers to achieve sustainable cybercrime prevention and meet regulatory compliance requirements.

The IBM Security solutions difference

- **Crime logic, not signatures—**Through intelligence gathered from millions of protected endpoints, IBM Security processes tens of thousands of fraud attempts every day into crime logic—a distinct, compact and viable footprint of fraud targets and tactics.
- **Rapid adaptation to emerging threats—**The IBM Security adaptive protection process quickly turns zero-day attacks into known crime logic and automatically integrates new crime logic into IBM Security solutions to promptly detect and help block these attacks on protected endpoints.
- **Near real-time application protection—**IBM Security technology transparently secures the browser from zero-day advanced malware and phishing attacks. This distinct technology prevents malware from tampering with the browser while quickly alerting IBM Security of any abnormal behavior that could represent a new attack.

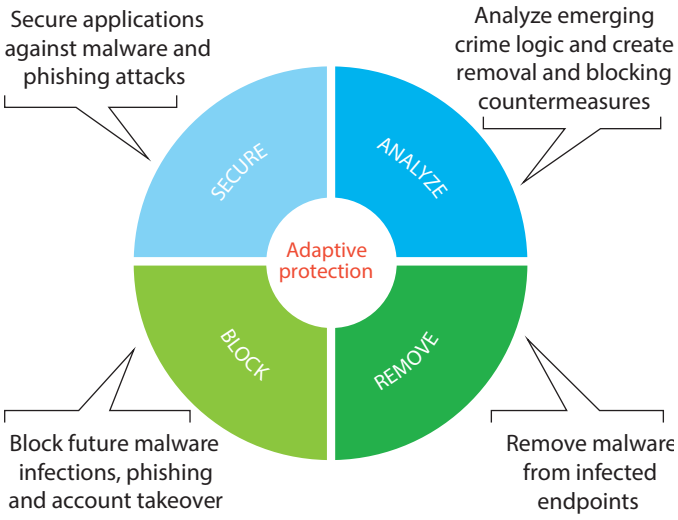


Figure 4: The IBM Security adaptive protection process

IBM Security Trusteer cybercrime prevention architecture

The IBM Security Trusteer suite of products offer multiple layers of protection across devices and the transaction lifecycle.

IBM® Security Trusteer Pinpoint Malware Detection

Trusteer Pinpoint Malware Detection provides financial institutions with clientless detection of fraudulent activity, identifying malware-infected web sessions and phishing attacks. Trusteer Pinpoint Malware Detection requires a small change to the online banking application and can be easily integrated with the bank's fraud-prevention processes. The software can help:

- **Prevent fraud by detecting malware—**Trusteer Pinpoint Malware Detection can detect malware infection and underlying crime logic on endpoints accessing online banking sites. The detection is performed in near real-time without requiring software installation on the endpoint, is transparent to the end user and has no impact on application response time.
- **Identify phishing incidents in near real-time—**IBM® Security Trusteer Pinpoint Criminal Detection can identify phishing and spear-phishing incidents in near real-time. It can detect credentials lost through phishing and notifies the financial institution. The user is quickly re-credentialed by the financial institution to help block the fraudster's access to the victim's account.

IBM® Security Trusteer Rapport

Trusteer Rapport helps prevent malware from infecting endpoints, secures the browser against tampering and data theft, and provides automated remediation. The software can help:

- **Defend against a wide range of attacks—**Trusteer Rapport helps prevent man-in-the-browser attacks and sensitive data theft by locking down the browser and blocking malicious key-logging and screen-capturing attempts. Trusteer Rapport can block man-in-the-middle attacks by validating that IP addresses and SSL certificates belong to the legitimate site.
- **Prevent malware infections and remove existing malware—**Once installed, Trusteer Rapport can remove existing malware from end user machines and help prevent future infections by stopping attempts to exploit browser vulnerabilities and install malware on the endpoint. Trusteer Rapport also provides a simple way for fraud, IT security and support teams to remediate threats on endpoints.
- **Stop phishing of sensitive data—**Trusteer Rapport helps prevent data theft by detecting suspected phishing sites on first access by a protected user. Trusteer Rapport alerts the user of a possible phishing attempt to help prevent data loss. IBM Security experts verify, in near real-time, that the site is in fact malicious. The site is added to the Trusteer Rapport blacklist to prevent other users from being phished.

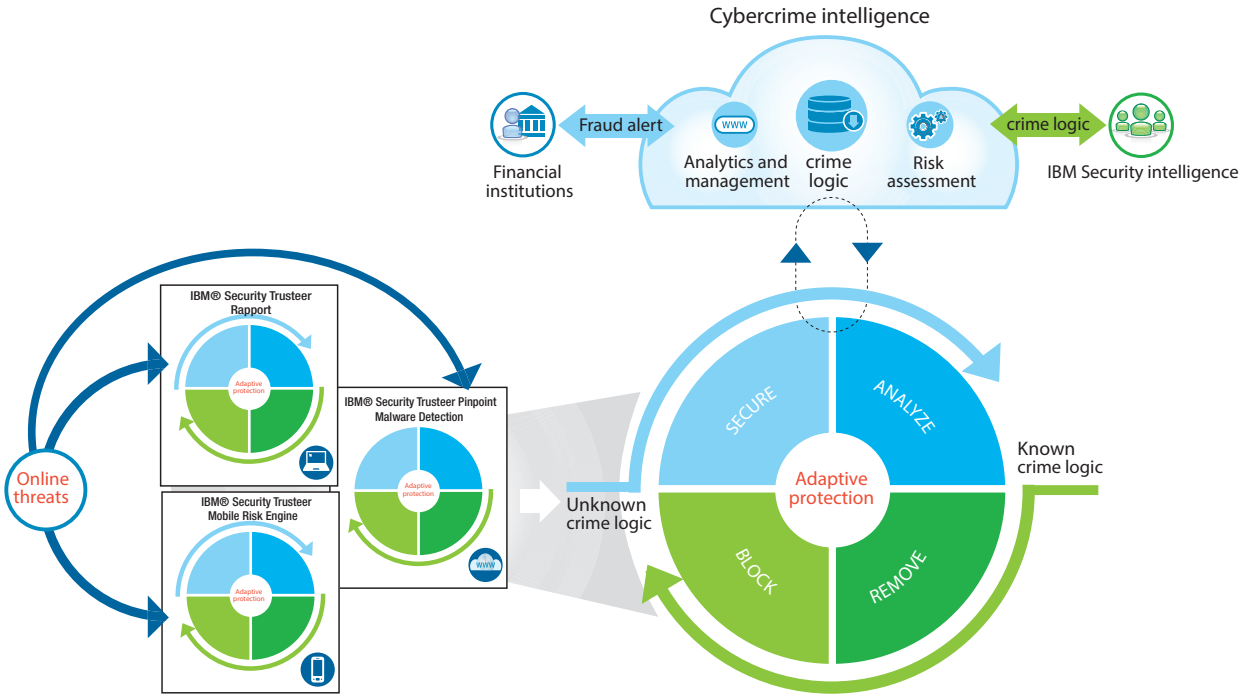


Figure 5: IBM Security Trusteer cybercrime prevention architecture

IBM Security Trusteer mobile solutions

IBM Security Trusteer mobile solutions helps organizations to mitigate mobile fraud risk by addressing complex cross-channel attacks as well as the unique challenges presented by the mobile channel. The software can help:

- **Assess mobile fraud risk and detect high-risk devices based on multiple device risk factors—**IBM® Security Trusteer Mobile Risk Engine is designed to protect organizations against mobile account takeover and high-risk mobile devices. It detects mobile account takeover by correlating mobile device and account risk factors (including geolocation, device time, IP address, missing operating system security patches, rooted/jailbroken device status, risky system configuration settings, malware infections, use of unsecured WiFi connection and more) across online and mobile channels, in near real-time, to reliably identify mobile channel fraud attempts.
- **Provide secure mobile web access—**IBM® Security Trusteer Mobile Browser provides end users with a secure mobile browser that helps ensure safe web access. Fake websites and man-in-the-middle attacks are detected by the secure mobile browser, and end users are prevented from accessing fraudulent sites. Device risk factors are collected and provided to the organization's website and Trusteer Mobile Risk Engine for mobile risk assessment. Users are alerted to the existence of device risk factors via a dedicated dashboard and receive step-by-step guidance on how to mitigate them.

- **Generate a persistent mobile device ID for unique device identification—**IBM® Security Trusteer Mobile SDK creates a persistent mobile device ID, allowing the organization to distinctly identify any device using the native mobile banking application. The persistent device ID is associated with the user's account and distinctly identifies the device, even across removal and re-installation of the mobile application. This helps ensure that new devices are identified, login attempts from known devices are not challenged and potential fraudster devices are flagged.

IBM Security intelligence

The IBM Security Trusteer portfolio also offers a cloud-based management and intelligence platform that provides deep insight into emerging crime logic and helps enable quick mitigation of cybercrimes within the user base. The platform provides:

- **Emerging crime logic analysis from millions of endpoints—**A network of tens of millions of protected endpoints can continuously detect new threats and propagate crime logic information to the IBM cybercrime intelligence cloud. IBM intelligence center experts use advanced data-mining and analysis tools to identify new crime logic.
- **Intelligence for shaping the IBM Security Trusteer portfolio—**The IBM intelligence center creates detection and protection countermeasures that are quickly integrated into our solutions to address emerging crime logic.
- **Cloud-based management and threat feeds—**The IBM Security Trusteer management application provides centralized management of IBM Securty solutions, as well as alerts on malware and phishing activity. Organizations can monitor endpoint security, review the use of IBM Security services and respond to alerts about specific threats. In addition, security teams can use detection alerts to help stop threats by performing mitigation activities, such as suspending transactions, patching endpoints, taking down phishing sites, removing malware from endpoints and elevating risk scores on risk engines.

Why IBM?

IBM Security solutions are trusted by organizations worldwide for fraud prevention and identity and access management. These proven technologies enable organizations to protect their customers, employees and business-critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives.

For more information

To learn more about the IBM Security Trusteer portfolio of fraud-prevention solutions, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com/**Security

About IBM Security solutions

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 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com/**financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
August 2014

Please Recycle

[1] MRG Effitas, "Online Banking Security Test," Effitas, Ltd., June 2011. http://www.mrg-effitas.com/wp-content/uploads/2012/06/MRG-Effitas-Online-Banking-Browser-Security-Project-3.pdf

[2] "UAB computer forensics links internet postcards to virus," *The Hindu*, July 27, 2009. http://www.hindu.com/the hindu/holnus/008200907271321.htm

[3] "Cyber Banking Fraud: Global Partnerships Lead to Major Arrests," I.V. Weekly-Chronicle, October 4, 2010. http://tribwekchron.com/2010/10/cyber-banking-fraud-global-partnerships-lead-to-major-arrests

[4] Peter Kruse, "Complete ZeuS sourcecode has been leaked to the masses," CSIS Blog, May 9, 2011. http://csis.dk/en/csis/blog/3229

[5] Amit Klein, "Webinjects for Sale on the Underground Market," Trusteer Blog, November 02, 2011. http://www.trusteer.com/blog/webinjects-sale-underground-market

[6] Amit Klein, "Cybercrime Services Ramp Up to Provide One-Stop-Shop to Meet Demand from Fraudsters," Trusteer Blog, November 30, 2011. http://www.trusteer.com/blog/cybercrime-services-ramp-provide-one-stop-shop-meet-demand-fraudsters

[7] Amit Klein, "SpyEye Changes Phone Numbers to Hijack Out-of-band SMS Security," Trusteer Blog, October 05, 2011. http://www.trusteer.com/blog/spyeye-changes-phone-numbers-hijack-out-band-sms-security

[8] Amit Klein, "Gift Wrapped Attacks Concealed Online Banking Fraud during 2011 Holiday Season," Trusteer Blog, January 04, 2012. http://www.trusteer.com/blog/gift-wrapped-attacks-concealed-online-banking-fraud-during-2011-holiday-season

[9] Amit Klein, "Post Transaction Attacks Expose Weaknesses in Fraud Prevention Controls," Trusteer Blog, January 17, 2012. http://www.trusteer.com/blog/post-transaction-attacks-expose-weaknesses-fraud-prevention-controls

Trusteer was acquired by IBM in August of 2013.

WGW03046-USEN-01