Stepping up the battle against advanced threats

Achieve more stable, effective and manageable endpoint security with Stateful Application Control

Contents

1 Introduction

1 Targeting end users

2 Three lost battles

3 Helping eliminate vulnerabilities: Patching and secure code development

7 The importance of application control

10 Protecting enterprise credentials

10 Conclusion

11 For more information

11 About IBM Security solutions

Introduction

The primary approaches used to fight cybercrime over the past several years simply have not been effective. Despite losing some of these security battles, today's organizations can still win the war. However, a new approach is needed. IBM Security Trusteer solutions offer a new cybercrime-prevention approach that provides exceptional protection against spear phishing, drive-by downloads and advanced, information-stealing malware. IBM solutions can help organizations to prevent targeted attacks, with no increased management load for IT staff or disruption to end users.

Targeting end users

Cybercriminals use a variety of tricks and social-engineering tactics to try and fool employees, compromise their machines and corporate accounts, and gain a foothold in the enterprise network. The most common techniques used today are phishing and watering hole attacks.

Phishing and spear phishing

In a phishing attack, cybercriminals send users a message in an attempt to lure them to perform an action that will result in a malware infection, credentials theft or both. The message can be in the form of an email, instant message, Facebook post or Twitter message, for example. Depending on their type, messages can contain either a weaponized document or a link to a malicious website. In a spear-phishing attack, the attacker uses the same tools, but this time, the attacker personalizes the message and targets specific users. This is because a personalized message is often more convincing and trusted by users.

These messages may contain **weaponized attachments**, such as Microsoft Word, Microsoft Excel or Adobe PDF files that contain hidden malicious code. When the user opens the weaponized document and the application renders the content, the hidden code executes and exploits a vulnerability to download malware onto the user's device.

Or, the message may include links to malicious sites that can lead users to:

- **Phishing sites:** These sites are designed to steal user credentials (usernames and passwords) and try to mimic the look and feel of legitimate websites, such as online banking, e-commerce websites and even Google applications. When a user accesses a phishing website and tries to log in, these credentials are sent to the attacker, who can use them to log into the user's account and steal information, funds or both.
- **Exploit sites:** These sites contain a hidden malicious applet or code that exploits a browser (or browser plug-in) vulnerability to silently download malware to the user's device. The user does not need to initiate the download and, in most cases, is unaware of the download taking place. This is called a *drive-by download*.

Watering hole attacks

In a watering hole attack, cybercriminals compromise a legitimate website that is routinely accessed by a specific type or group of users. The compromised website becomes an exploit site and infects its visitors with malware. In a recent watering hole attack, a mobile application development site was compromised to serve up malware to the site visitors. As a result, developers from companies such as Facebook, Apple and Microsoft were infected with a remote-access Trojan (RAT) virus. Although the perception may be that watering hole attacks cast a wider net, they are still highly targeted in nature.

Three lost battles

Over the years, organizations have used various tools and techniques to help block cyber attacks and prevent attackers from gaining access to enterprise networks. Today, it is clear that three of these techniques were not effective.

User education: Explaining the do's and don'ts

Education and awareness programs are continuously developed to train employees to recognize common phishing and spear-phishing attack tactics, and in the proper use of external content. The belief is that with proper education, organizations can reduce the risk of successful phishing attacks occurring through human error.

Despite the time and resources that organizations have put into training users, user education alone has failed to mitigate the risk. Training programs that explain the dangers of opening untrusted external content and clicking on suspicious links have not prevented users from doing so on a daily basis. Users still open untrusted content and click on suspicious links because phishing schemes can be very convincing. Attackers use information gained through social engineering to personalize spear-phishing messages and convince targeted users that the messages are legitimate.

In June 2013 the FBI issued a warning about the rise of spear-phishing attacks, saying, “Often, the emails contain accurate information about victims obtained via a previous intrusion or from data posted on social networking sites, blogs or other websites. This information adds a veneer of legitimacy to the message, increasing the chances the victims will open the email and respond as directed.”[1]

Recently, an attacker used fake Twitter messages and shortened URLs to spread malware among Twitter users. In this case, the malware gained access to the users’ Twitter accounts and created malicious tweets containing URLs. Followers of those accounts received a tweet from the trusted source, with a link that led them to an exploit site and infected their endpoints with malware. Because the malware compromised trusted Twitter accounts and used shortened URLs to mask the real ones, it was very difficult for users to identify these messages and links as malicious.[2]

Additionally, user education cannot protect users against the fairly recent phenomenon of watering hole attacks. Compromising websites that employees need in order to perform their jobs is devious, as organizations cannot block users from visiting these sites. It is practically impossible to train employees to avoid watering hole websites, as no one knows which sites have been compromised, and banning employees from accessing trusted sites required for their work is counterproductive.

The bottom line: as long as employees depend on online information, spear-phishing and watering hole attacks will remain threats that can lead to the theft of credentials and malware infections.

Helping eliminate vulnerabilities: Patching and secure code development

Vulnerabilities in endpoint applications introduce significant risk to organizations, as cybercriminals can exploit them to silently download malware onto user devices.

Timely patch application is critical to help prevent the exploitation of known endpoint application vulnerabilities. However, failure to keep up with software patches is one of the most common challenges identified by security and IT professionals. New patches are released daily, making it difficult for even the most experienced system administrators to help ensure proper deployment in a timely manner.

Some of the major attacks of the past few years have targeted known vulnerabilities for which patches existed. One example is a targeted attack on users in Vietnam, India, China, Taiwan and possibly other countries.[3] In this attack, weaponized Word documents were sent to victims via spear-phishing emails. The weaponized documents contained an exploit targeting known vulnerabilities in installations of Microsoft Office. In fact, a Microsoft patch for these vulnerabilities was provided in 2012. Despite being relatively old, these Word vulnerabilities continue to be exploited in targeted attacks. In this case, the exploit was used to download KeyBoy, a malicious back-door program that steals credentials stored in Internet Explorer and Mozilla Firefox and installs a key-logger to steal credentials entered into Google Chrome. This back-door program also allows attackers to obtain detailed information about the compromised devices, browse their directories, and download or upload files from and to them. In addition, the malware can be used to open a Windows command shell on the infected devices that, in turn, can be used remotely to execute Windows commands.

While the timely patching of application vulnerabilities is important, it is clearly not enough. The increasing frequency and sophistication of zero-day attacks has highlighted the need for more proactive measures. Zero-day vulnerabilities—software vulnerabilities unknown to the vendor—are a top concern of security administrators, since no patches exist. Attackers who are aware of these vulnerabilities can quickly develop zero-day exploits—pieces of code that exploit unknown vulnerabilities to silently download malware onto user devices—and embed the exploit in a website or email attachment. Users who access the malicious website or open the weaponized document cannot prevent, or even see, the exploitation of the vulnerability—which results in malware infection. As long as the vulnerability is not patched, users will continue to be infected with malware.

A recent example of a targeted attack—the infamous "Poison Ivy" attack—exploited a zero-day vulnerability to infect users in more than 37 countries.[4] The attackers used a watering hole attack that compromised a US Department of Labor website that is regularly visited by government employees and contractors in the nuclear research sector, as well as by civilians in the defense, security and aerospace industries. Visitors to the website were redirected to another site where malicious code targeted those using Internet Explorer. The code exploited a zero-day vulnerability in the browser to download the virus to the victims' endpoints. The attackers may have used the virus to collect sensitive military information on behalf of a nation-state. Microsoft was not able to provide a patch for this vulnerability until a month after the attack was discovered.

Secure coding practices

Increased awareness of the risk introduced by application vulnerabilities, specifically zero-day vulnerabilities, has accelerated the introduction of secure coding and programming initiatives. Secure coding guidelines—developed by organizations such as the SANS Institute, OWASP and CERT[5]—promote the concept of creating secure applications by design. These guidelines support solution architects and developers in their efforts to conceive, develop, acquire, operate and maintain hardened applications, while also significantly reducing software vulnerabilities.

Secure coding has been getting significant attention over the last few years, and many organizations have introduced training programs designed to educate developers about the importance of secure coding and best practices they should follow. However, these important initiatives have not completely eliminated vulnerabilities. In fact, in 2012, the number of publicly reported software vulnerabilities jumped by 26 percent, the biggest increase in five years.[6] While this does not mean that secure coding initiatives have failed, it does suggest there is still more work to be done.

Today's security professionals must assume that vulnerabilities exist in Internet-facing software installed on user endpoints and that these vulnerabilities can be exploited to silently download malware and infect their machines. Waiting for a patch is simply not enough.

Malware detection: Blacklisting and behavior analysis

Around the world, security experts agree: even when anti-virus applications work perfectly, they can still fail to block sophisticated malware attacks. Anti-virus solutions, which first appeared in the late 1980s, use several blacklisting methods to identify viruses and other malware:

- **Signature-based detection** compares the contents of a file to a dictionary of known virus/malware signatures.
- **Heuristic-based detection** compares the heuristics of a file to a dictionary of known malware heuristics.
- **Behavior-based detection** compares the behaviors of the file in a virtual sandbox test environment to known malware behaviors.

Most anti-virus solutions are host-based, scanning the host file system for known malicious files. However, due to the performance impact on user endpoints, some anti-virus and malware detection vendors have moved the detection process to network appliances—but the detection methods remain unchanged.

While many users still trust that malware detection solutions will protect their enterprise endpoints and personal devices against advanced threats, in the current threat landscape, malware detection solutions fall short. A recent breach at the New York Times demonstrates that blacklisting detection methods used by anti-virus vendors may not be able to prevent all attackers from gaining entry into corporate networks. In 2012, Chinese hackers persistently attacked the newspaper's network for more than four months, infiltrated computer systems, and stole reporter and employee credentials. The attackers infected user endpoints with malware and stole the corporate passwords of every Times employee to gain access to the personal devices of 53 employees, most of them outside the newsroom. What is more, out of the 45 different pieces of malware planted on systems over the course of the attack, only one was spotted by anti-virus software. The other 44 were only found during a post-breach investigation, months later.[7]

Today's hackers are creating new malware faster than anti-virus vendors can blacklist them. AV-Test, a research institute that tests anti-virus products, says it registers more than 200,000 new kinds of viruses every day.[8] In addition, attackers use polymorphic code to continuously mutate malware and evade anti-virus detection.

Anti-virus vendors have introduced behavior-based detection methods to better identify new, unknown malicious files and battle polymorphic code evasion techniques. This approach emulates unknown, untrusted file execution in a sandbox environment—typically on a network appliance—and, based on the file behavior, determines if the file is malicious or benign. Naturally, attackers have responded with techniques to evade these detection solutions, as well. For example, some have designed malware that "sleeps" for hours or days, or waits for a mouse-click, thus avoiding detection in synthetic sandbox environments. Once the malware gets to the user endpoint, where mouse-click events are abundant, it will compromise the endpoint.

Another method for detecting malware is by monitoring outbound traffic for data exfiltration. These types of solutions look for communication with known command-and-control servers or network behavior profiles that indicate malicious communication. However, attackers have also devised evasion techniques to bypass these solutions, including using legitimate sites—such as social networks or Google Docs—as proxies to hide malicious traffic and use of custom communication protocols. Malware authors also incorporate peer-to-peer (P2P) communication so there is no one set of addresses that can be blocked.

Simply put, malware detection rules can be bypassed. Every time a new detection method is developed, hackers study the blacklisting rules and develop new evasion techniques. It is clear that anti-virus software cannot prevail alone against today's advanced malware. Despite this, many organizations continue to buy and implement anti-virus solutions in order to adhere to compliance regulations—such as the Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI-DSS), the Gramm-Bleach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA)—which explicitly require implementation of anti-virus solutions.

The importance of application control

Application control: Harder to evade, but difficult to deploy and maintain

Application control technologies help ensure that only approved applications and their associated executable files are permitted to run on endpoints. The most well-known application control approach is based on file whitelisting. File whitelisting is the opposite of the blacklisting approach used by anti-virus applications, essentially using a list of approved or certified files instead of a list of known malicious files. It is more difficult for malware to bypass this control because whitelisting does not use detection rules. That said, file whitelisting solutions introduce a different challenge—the setup and maintenance of the whitelist. The whitelist must contain every file and application that any user in the organization might use.

Consider the fact that the average endpoint contains 20,000 executable files, and that the whitelist must include every update, every patch and every executable required for internally developed applications. As a result, whitelist maintenance quickly becomes complex and difficult to manage. For example, one widely used whitelisting solution uses a database that contains more than 700 million distinct files, and is constantly updated by the company and by more than 300 partner software vendors.[9] Another vendor uses a database that contains more than eight billion records with hundreds of thousands of new files added every week.[10] Due to this complexity, large organizations struggle to implement and maintain enterprise-wide deployments, especially for dynamic, Internet-facing endpoints, which can leave user endpoints vulnerable to malware infections.

A different application control approach isolates application tasks by executing the tasks in a virtual environment. When an isolated application is compromised, the threat remains inside the virtual environment and does not infect the underlying host. This can be a very strong security control, but it also introduces many challenges. Primarily, end user applications are not designed to run in isolation. On the contrary, they are designed to interoperate. Think about the simple copy-paste capability that allows users to copy content from one application, such as a browser, and paste it into another application, such as a Word document. Applications are also designed to interact with the underlying host, such as when saving files to the file system, printing files and so on. These functions require the definition of special policies and the installation of special drivers to enable basic business workflow without impacting user productivity. This can become very challenging in large enterprise environments that consist of a variety of users, endpoint platforms and applications, and where any changes can potentially harm legacy applications.

Stateful Application Control: Next-generation advanced malware protection

Since user education, vulnerability elimination, malware detection and application control approaches cannot provide complete protection against advanced malware, a new approach is needed. Organizations require a solution that is not dependent on the end user, patch availability or malware-detection methods; one that is easy to implement and maintain across all enterprise endpoints.

IBM® Security Trusteer Apex Advanced Malware Protection applies a new approach to advanced malware protection—Stateful Application Control. By analyzing *what* the application is doing and *why* it is doing it, the software can automatically and accurately determine if an application action is legitimate or malicious. Using this approach,Trusteer Apex Advanced Malware Protection is able to block vulnerability exploitation and silent malware downloads. It also blocks malware communication and data exfiltration that enables attackers to gain footholds in the network. The Stateful Application Control behind Trusteer Apex Advanced Malware Protection enables automated enterprise malware protection that optimizes security while simplifying deployment and significantly reducing management overhead.

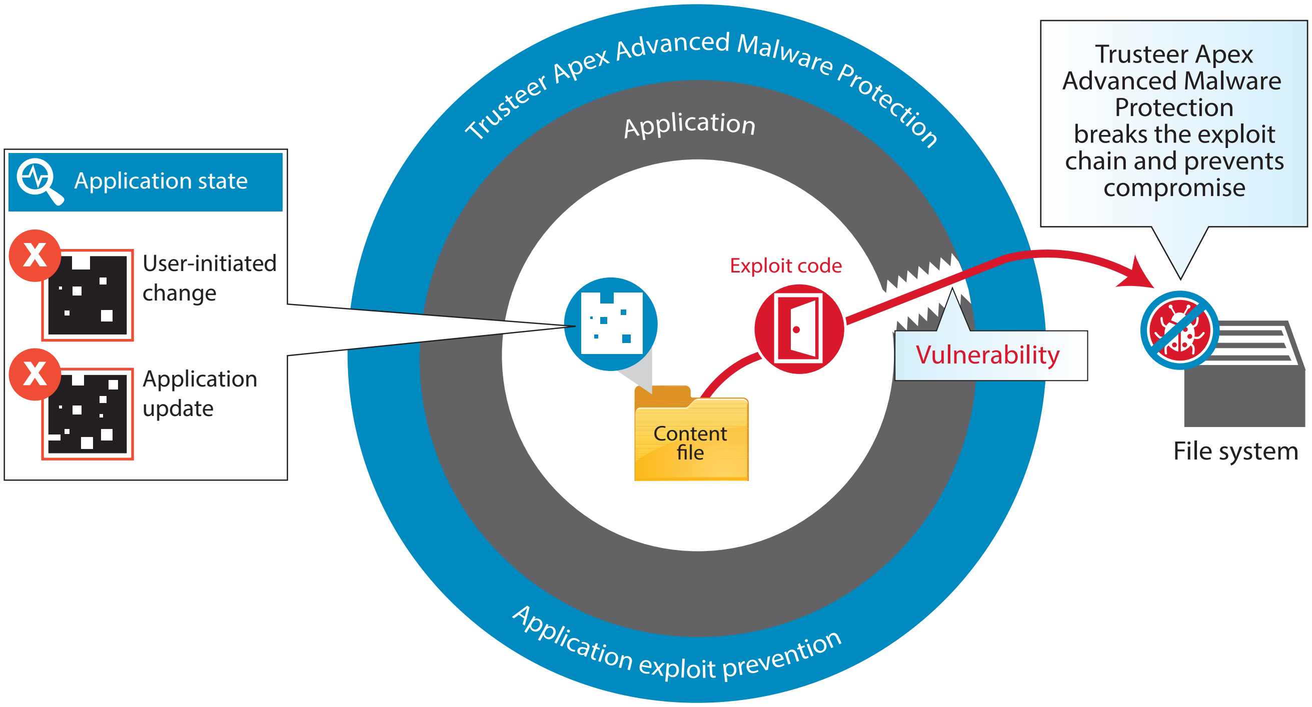
Trusteer Apex Advanced Malware Protection
Application
Application state
User-initiated change
Application update
Exploit code
Vulnerability
Content file
Trusteer Apex Advanced Malware Protection breaks the exploit chain and prevents compromise
File system
Application exploit prevention

Figure 1: Stop application actions with unknown state

Unlike other security controls, Stateful Application Control does not try to identify malicious files or control their execution. Instead, it stops the silent download of malware via vulnerability exploitation by validating the state of the application during sensitive functions. For example, when an application downloads a file for a legitimate reason—such as when the user selects the Save As option from the application menu—a specific application state is created—that is, the state of the memory and kernel-level processes. By analyzing the application states during normal operations, Stateful Application Control maps the legitimate application states of targeted applications—such as web browsers or Adobe Acrobat, Adobe Flash, Java or Microsoft Office—when these applications write to the file system. These mapped application states provide the context of the action, enabling an accurate determination of why the file was downloaded.

Stateful Application Control uses the mapped application states to validate operations; when the application downloads a file, the control verifies that a known, legitimate application state was created and, if so, it allows the action to continue. But if the application downloads a file as a result of an exploit, an unknown application state is created—one that does not match any of the mapped application states. In that case, the file is stopped so that it can do no harm.

One of the main advantages of Stateful Application Control is that it can help stop the exploitation process for a wide range of vulnerabilities. It does not matter if the vulnerability is known or unknown (zero-day), what kind of malware it is trying to download to the endpoint, the malware's source or its destination. As soon as an unknown application state is created, the exploitation process is stopped and the downloaded file is stopped. This makes Stateful Application Control very difficult to evade.

Stateful Application Control allows for more stable, effective and manageable endpoint security than traditional application control approaches because it is focused on exploitable applications for which the legitimate application states are few and relatively static. This reduces the maintenance required compared to other application control approaches that must inspect and manage a multitude of files.

The key to implementing Stateful Application Control is making it highly manageable so that it requires no end user intervention and limited IT staff involvement. This can only be accomplished through a sizeable network of endpoints that enables new, legitimate application states to be detected and immediately pushed out to all protected endpoints via the cloud.

Stateful Application Control enables the following capabilities:

- **Application exploit prevention:** Trusteer Apex Advanced Malware Protection blocks malicious code embedded in web pages and business documents from exploiting zero-day or unpatched vulnerabilities in client applications and installing malware on the endpoint.
- **Data exfiltration prevention**: Trusteer Apex Advanced Malware Protection restricts untrusted files from executing sensitive operations that are potentially malicious, such as tampering with application processes to hide communication traffic to a command-and-control center. Untrusted files are sent to Trusteer Apex Advanced Malware Protection for further analysis.
- **Ease of deployment and automated management**: Trusteer Apex Advanced Malware Protection can be deployed within days across tens of thousands of endpoints, both managed and unmanaged, and is specifically designed to support large and complex environments. No learning period is required, and no initial or ongoing configuration is necessary.

Protecting enterprise credentials

The beginning of this white paper explained that attackers often target corporate employee credentials. Compromised credentials allow attackers to gain fraudulent access to corporate networks and resources. Attackers can gain corporate credentials by stealing them off user endpoints, using key-loggers or by stealing credentials on the Internet. They do this via phishing sites, such as a fake Google Apps login page, or by stealing the user database of public websites. Since many employees reuse their corporate credentials on consumer websites and social networks, the site's user database can provide attackers with valuable credentials, which can result in data breaches that significantly impact the corporate business.

To help secure enterprise credentials against key-logger and phishing attacks, and to help prevent exposure through public site user databases, Trusteer Apex Advanced Malware Protection added the following protections:

- Obfuscating keystrokes on the endpoint, preventing key-loggers from capturing the actual keystrokes.
- Validating that corporate credentials are used online only to log in to approved enterprise web applications; this can help prevent users from submitting their credentials on phishing sites, as well as help prevent employees from reusing their corporate credentials on public consumer websites and social networks.

Conclusion

The endpoint has become the path of least resistance for cybercriminals and hackers to get footholds into enterprise networks. Advanced information-stealing malware is the main tool that enables advanced persistent threats to affect organizations. Traditional methods such as user education, vulnerability patching and malware detection have failed to fully protect organizations against the current threat landscape. Attackers continuously develop sophisticated new tactics and evasion techniques to bypass the latest protection methods, requiring the security industry to seek a different approach to malware protection.

Trusteer Apex Advanced Malware Protection leverages Stateful Application Control, a new technology that provides effective protection against advanced malware by helping stop vulnerability exploitation and silent malware downloads. Because it does not rely on users' judgment, patch availability or malware-detection rules, it is effective even against unknown, zero-day threats.

Trusteer Apex Advanced Malware Protection includes a data exfiltration prevention layer that prevents malware from communicating with command-and-control servers and exfiltrating data. It also includes specific features to help protect enterprise credentials against theft and exposure.

Delivered as a lightweight software agent, Trusteer Apex Advanced Malware Protection is easily deployed on both managed and unmanaged endpoints. It transparently runs on the endpoint, protecting against advanced malware without impacting the endpoint performance or user experience. Automated processes, enabled by Stateful Application Control technology, help significantly reduce ongoing maintenance for Trusteer Apex Advanced Malware Protection. The IBM research lab delivers automated updates directly to the agents, wherever they are. Centralized management and reporting enable Trusteer Apex Advanced Malware Protection to provide a simple and cost-effective solution to a growing problem.

Security professionals who are concerned about the escalating frequency and sophistication of threats targeting employee endpoints now have a solution that accurately protects endpoints against advanced threats, yet is easy to deploy and manage in dynamic user environments.

Why IBM?

IBM Security solutions are trusted by organizations worldwide for fraud prevention and identity and access management. The 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 IBM Security Trusteer advanced threat protection and Trusteer Apex Advanced Malware Protection, 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 13 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

[1] Federal Bureau of Investigation (FBI), “Cyber Criminals Continue to Use Spear-Phishing Attacks to Compromise Computer Networks,” June 25, 2013. http://www.fbi.gov/scams-safety/e-scams

[2] Dana Tamir, “Twitter Malware: Spreading More Than Just Ideas,” http://www.trusteer.com/blog/twitter-malware-spreading-more-than-just-ideas, April 22, 2013

[3] Lucian Constantin, “New backdoor ‘KeyBoy’ malware hits Asia with targeted attacks,” ComputerWorld, June 10, 2013. http://www.computerworld.com/s/article/9239940/New_backdoor_KeyBoy_malware_hits_Asia_with_targeted_attacks

[4] Ben Weitzenkorn, “Internet Explorer Zero-Day Attack Targets Nuclear Researchers,” TechNewsDaily, May 6, 2013. http://news.yahoo.com/internet-explorer-zero-day-attack-targets-nuclear-researchers-214704437.html

[5] The trade name SANS derives from sysadmin, audit, networking and security. OWASP is the Open Web Application Security Project. CERT is not an acronym; it is a name and registered service mark of Carnegie Mellon University.

[6] Robert Lemos, “Lessons Learned From a Decade of Vulnerabilities,” Dark Reading, February 19, 2013. http://www.darkreading.com/vulnerability/lessons-learned-from-a-decade-of-vulnera/240148896

[7] Nicole Perlroth, “Hackers in China Attacked The Times for Last 4 Months,” The New York Times, January 30, 2013. http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

[8] The AV-TEST Institute, “Malware Statistics,” October 21, 2013. http://www.av-test.org/en/statistics/malware/

[9] Kaspersky Lab, “Kaspersky Lab Dynamic Whitelist technology gets ‘Approved Whitelisting Service’ certificate from AV-TEST,” April 25, 2013. http://www.kaspersky.com/about/news/product/2013/Kaspersky_Lab_Dynamic_Whitelist_technology_gets_Approved_Whitelisting_Service_certificate_from_AV_TEST

[10] Help Net Security, “RSA and Bit9 team to accelerate cyber forensics investigations,” August 9, 2012. http://www.net-security.org/secworld.php?id=13399

Trusteer was acquired by IBM in August of 2013.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
August 2014

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.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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.

♲ Please Recycle