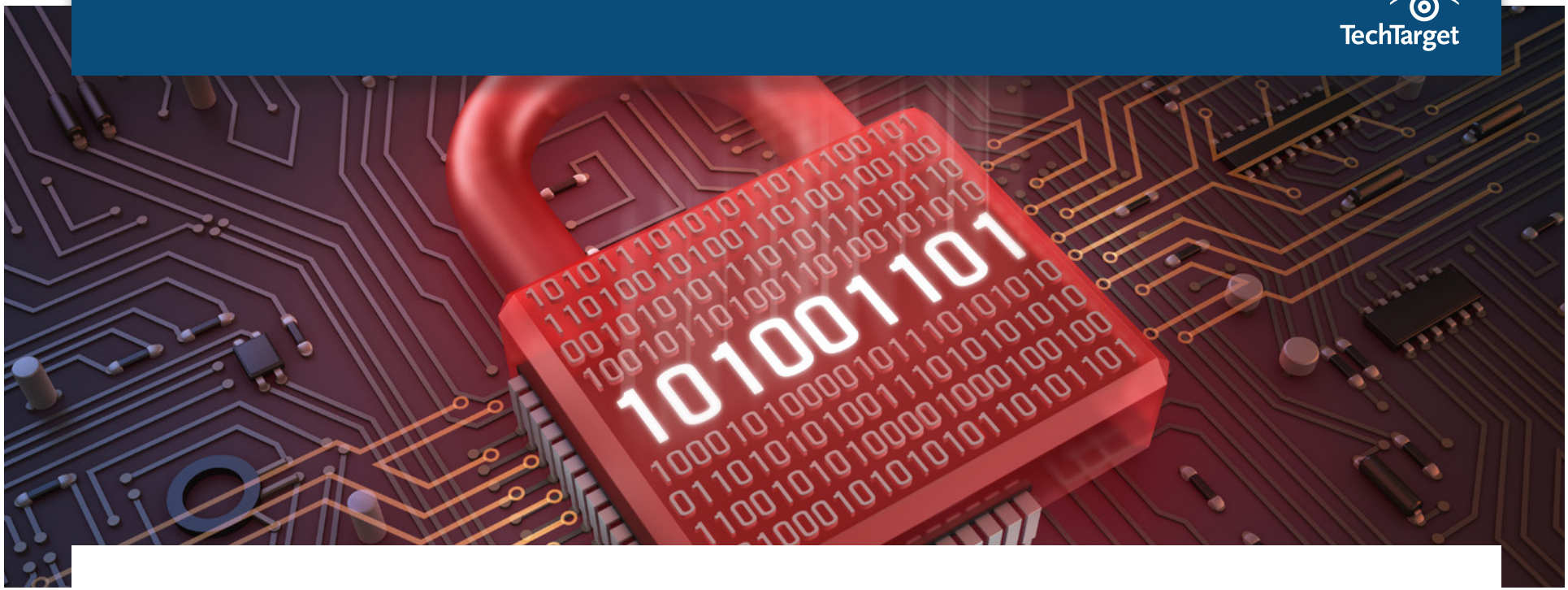

Fighting Crimeware

As malware gets mightier, here's what you must know to keep out these modern-day thieves.

Fighting Cybercrime in the 21st Century

Forget the Colt .45 that Bonnie and Clyde favored. Malware is the weapon of the 21st-century robber. Whether it's aimed against enterprise systems or end users, the target of crimeware is always the same: sensitive financial information that unlocks access to bank accounts and other financial resources.

In recent months advanced malware has become even more sophisticated, so in this three-part guide our experts shine a light on several specific threats and what InfoSec professionals can do about them. We open with Rob Shapland's chapter, which both outlines the latest developments in crimeware and offers advice on investigating break-ins. Formal investigations of malware breaches are not the norm, he says, but they should be. Even though the crime's been committed, the nature of malware today means your systems may remain infected. At the very least, IT professionals must understand what's wrong in order to know what training and tweaks must be done to reduce chances of another attack.

In the second chapter, Nick Lewis explores RAM-scraping malware—the weapon used in last year's Target breach. He closes with a chapter on the latest tactics hackers are using to evade detection, like automation and social engineering, and how to counter them.

Hackers won't quit, and malware is only going to get more pervasive and persistent. You need to keep current on the new threats and the latest defenses. An attack on your financial resources is not a matter of *if* but *when*, since—to steal the words of bank robber Willie Sutton—"that's where the money is." ■

Brenda L. Horrigan, Ph.D.
Associate Managing Editor
Security Media Group

Crimeware: What It's After and How to Fight Back

CRIMEWARE HAS ADVANCED significantly in the last few years. In fact, the 2015 Verizon Data Breach Investigations Report (DBIR) describes crimeware, which constituted 25% of malware incidents, as "representing malware infections within organizations that are not associated with more specialized classification patterns."

SHOW ME THE MONEY

Sensitive financial information is a key target for attackers because it allows direct access to bank accounts to transfer funds to attacker-controlled accounts. While attackers have realized that targeting point-of-sale terminals is highly effective, targeting individual end users is also very lucrative. Crimeware is primarily financially motivated, and aims to directly access bank accounts or steal money using a number of techniques. These include tracking requests to banking sites and surreptitiously redirecting the user to a malicious site in order to steal credentials via command-and-control servers, installing ransomware (such as TeslaCrypt) to force users to pay to access their data, and stealing passwords stored on computers in order to access financial systems. Command-and-control crimeware is the most popular variant, but a change this year has shown attackers moving more toward distributed denial-of-service (DDoS) as an attack vector. This allows the attacker to demand ransom from the victim in order to restore service.

A recent example of crimeware is the Dyre variant, which uses the redirection technique to steal credentials for banking sites. The software will wait until the user tries to access a banking website before redirecting their browser to a clone of the site, which is hosted on an attacker-controlled domain. When the victim enters their credentials into the cloned website, they are sent to command-and-control

servers for processing. The delivery method of the crimeware is usually via an attachment in a phishing email. Dyre is an example of increasing sophistication in how crimeware operates, as it uses a randomly generated address to contact the server, evading detection methods that check for blacklisted URLs to block access.

DON'T FORGET TO INVESTIGATE

The Verizon report shows that crimeware incidents are less likely to be formally investigated than other types of incident. However, these incidents should undergo the same formal investigation procedures as other incidents. Although in some cases this isn't always feasible (opportunistic attacks on home users, for example), when crimeware is introduced onto an organization's systems, thorough investigation needs to be conducted as it can still be used as a method of extracting sensitive corporate data, even if this was not its original goal.

Crimeware is also often distributed as part of an exploit kit (such as Angler or Nuclear), and therefore the discovery of certain crimeware strains may be an indicator of further infections. As an organization you need to understand how these infections occur in order to identify the weak point in your defenses. The most likely infection point is through email phishing, which means that staff training and email filters need to be improved. Without investigating the individual cases your system will remain vulnerable.

Most mature security programs are capable of detecting crimeware intrusions, but do not have the manpower or willingness to spend the required money to investigate each incident. Most crimeware still involves intrusions that aim to contact command-and-control servers; however, a recent trend in DDoS-style attacks via crimeware is emerging that could even be termed *crimeware as a service*, where specific malware can be designed and delivered. To mitigate the threat, a defense in depth strategy is needed. Strong technical controls, combined with an ongoing staff-awareness program, can help prevent most infections. Investment in monitoring systems and a willingness to investigate incidents can help an organization find how an infection occurred, with the goal of preventing it next time. —*Rob Shapland*

How Enterprises Can Defend Against RAM Scrapers

RAM SCRAPING OR memory-scraping malware has advanced significantly since it first became widely known via the 2010 Verizon Data Breach Investigations Report. Since the 2013 attack on Target, in which attackers used a RAM scraper to capture credit card numbers, there has been renewed interest in the topic. While the technical aspect of malware using RAM scraping has changed little since 2010, the overall sophistication of the attacks has increased tremendously.

TIMES, THEY HAVE A CHANGED

First, a little background on RAM-scraping malware: While the Payment Card Industry Data Security Standard (PCI DSS) requires end-to-end encryption of all payment data—including credit card numbers, cardholder names and expiration dates—there is a period of time during the authorization process when the data is stored unencrypted in RAM on point-of-sale (POS) terminals. RAM-scraping malware was designed to infiltrate these POS terminals and scan the system's RAM, searching for the unencrypted data. Once found, RAM-scraping malware harvests the data and transmits it to attackers.

As it inevitably goes, new malware attacks and variations of malware are constantly emerging to bypass common enterprise security protections, such as firewalls and anti-malware—this is as true now as it was in 2010. And in terms of RAM-scraping malware, access to the POS terminal and network is still required, so those standard protections will still need to be bypassed in an attack.

While these facts remain the same, to me the major thing that sticks out is how sophisticated and automated the overall attacks have become. The increased usage of encrypted connections has forced attackers to target any place where

credit card numbers are transported unencrypted, and these days that's often only at the POS where the initial card data capture occurs.

Many of the strategies to protect an enterprise from RAM scraping malware are the same today as they were in 2010.

Kartoxa a new strain of the BlackPOS malware, was reportedly used in the recent Target data breach. This malware monitors for any swipe of a credit card and records it to a file. Note that nothing about this is different from any other RAM-scraping malware. This attack in particular merely used more developed steps to better hide the communications and more sophisticated malware to make detection far more difficult. According to security journalist Brian Krebs, the attackers used a third-party vendor's account to get a foothold in the Target network and exploited the segmentation used by Target to separate the internal network from the PCI network. Using BlackPOS malware, the attacker was able to automate the copying of captured data via a Windows file share on a compromised internal Target server to extract the data. Using this Windows file share helped the attacker hide in plain sight. The compromised server was infected with some unknown malware and used to store the data until it was sent via FTP to servers outside of the Target network, as was mentioned by Dell SecureWorks' investigation. Using FTP also likely helped the malware hide from detection.

PROTECT AGAINST RAM SCRAPING

Many of the strategies to protect an enterprise from RAM-scraping malware are the same today as they were in 2010. Tools and techniques including patching, antimalware, firewalls, not running as administrator and network monitoring are all still vital—and all required by the PCI DSS. In January 2014, the U.S. Computer Emergency Readiness Team even released Technical Alert TA14-002A, which reiterated that these protections are critical.

Other basic steps—such as limiting usage

to only the POS software on the cash register, whitelisting or restricting access of the account used for the POS system—can also boost security. A host-based intrusion-detection system (HIDS) that monitors suspicious access to RAM or system devices can send an alert, notifying administrators to further investigate a system or block the access outright if needed. The HIDS or an embedded firewall can also provide an additional layer of protection by allowing only authorized connections. End-to-end encryption from a device connected to the POS to the payment processor can also be used to limit the transport of unencrypted credit card numbers and protect the credit card encryption from malware on the POS system; a chip and PIN will help limit the scope.

In addition to monitoring for suspicious connections, it is critical to also monitor for non-SSL encrypted traffic to detect malicious communication. Point-of-sale malware is often installed remotely, and attackers often use a remote connection to exfiltrate data as well, creating opportunities for detection. However, note that malware authors are moving toward using standard HTTPS for communications, so they won't stick out as much when analyzed. However, botnet communications might not look like normal, browser-based HTTPS communications and could generate an alert from a network anomaly-based detection system to investigate. Detecting a system with more outbound communications or any Internet-bound connection in a properly firewalled network could also generate an alert. Aggressive firewall configurations can also be set to allow the POS system to talk only to the cash registers and vice versa. A dedicated connection with the payment processor could be used in addition to strong firewall rules.

Besides monitoring for suspicious connections, it is critical to also monitor for non-SSL encrypted traffic.

While some enterprises may claim they need to collect credit card numbers to track consumer shopping habits, it is important to note that this can still be done by using a token in

the place of the credit card number. Though this could still pose an issue for enterprises storing credit card numbers for uniqueness, companies could mass-convert existing credit card numbers to new tokens using the same algorithm or processing as their payment processor. Despite the fact that mass-converting 40 million credit cards to tokens would be very resource-intensive, know that it would certainly be less costly than a data breach of millions of credit card numbers.

RESOLVE TO EVOLVE

Recent developments in both the sophistication and automation of RAM-scraping malware are indicative of the constant evolution of malware. It is critical that enterprises continually improve their defenses by implementing some of the aforementioned best practices. These will not only thwart potential attacks, but also ensure sensitive corporate and consumer data is protected as effectively as possible.

—Nick Lewis

Outwitting Advanced Evasion Techniques

AS LONG AS there are targets to exploit and money to be made, malware will continue to be used, and improved.

To remain relevant and receive a paycheck, malware authors will adopt advanced evasion techniques and include new features to meet their customers' requests so the attacks using the malware can be more effective and profitable. There are many instances of malware becoming more sophisticated over the past months, including Zeus transitioning from 32-bit to 64-bit and the advancement of the iBanking malware to target Android devices.

In addition to new features in malware, there is a relatively new idea around "living off the land," where attackers use built-in or legitimate tools to prevent their attacks from being detected by antimalware software. The Poweliks malware is the most recent example of this happening.

MALWARE ADVANCEMENTS

The TROJ_POWELIKS.A or Poweliks is fileless malware designed to download other malware that will control the compromised system. Poweliks requires a separate initial infection vector to compromise the local system and install the malware, which, it has been reported, is a malicious Word file. After the initial infection, the malware is installed and stored in the registry as an encoded dynamic link library (DLL) that is extracted and injected into legitimate dllhost.exe processes running on a system, which will then execute it.

While storing a DLL in the registry isn't a common method of installing malware on an endpoint, it does make it more difficult to detect the malware, because not all antimalware tools check the registry. However, for tools that do check the registry, finding a registry key with a significant amount of data would certainly be something to alert on. The Poweliks

malware also runs PowerShell commands to complete the attack. PowerShell commands could have been used to avoid detection by living off the land, since PowerShell is installed on most systems and has the advanced functionality for interacting with the operating system that is necessary to complete the attack.

Other malware has also continued to make advancements so it can remain profitable for malware authors. The mature Zeus malware continues to incorporate new features; the most recently reported functionality added to it was an improved social-engineering attack where the malware spoofed a browser warning message to get the user to install the malware. Similarly, the iBanking.Android has added new functionality where it uses fake security software to get the user to install the malware. It then steals SMS messages used in two-factor authentication.

DETECTING MALWARE

Detection of advanced malware can be done many different ways. Multistage malware, such as Poweliks, and multistage attacks could give enterprises more time to detect the malware because each step takes time; however, each step might not necessarily need to be detected because the individual steps themselves might not be malicious.

In the example of Poweliks, its multistage aspect may be difficult to detect when each individual stage happens, but correlating all of the stages and actions can help detect and mitigate malicious activity.

For example, while PowerShell scripts are useful for system administrators or power users, few end users develop and use them. Detecting malicious PowerShell commands is difficult because there are many legitimate enterprise uses of PowerShell functions. However, for PowerShell scripts used by end users, system admins could require the script to be signed before execution; this would help block any malware from executing malicious scripts. While this policy would not stop a dedicated attacker, it could raise the bar enough to frustrate them and prevent an attack.

Though detecting the PowerShell aspect of the Poweliks malware may be difficult, detecting its command-and-control infrastructure

and network connections could be easier. TrendMicro's blog post mentions a specific IP that can be used as an indicator of compromise so an enterprise could monitor its network for any connections to the IP and investigate each connection. Monitoring for anomalous network connections could also help identify a compromised system that requires additional investigation. This could include looking at NetFlow logs to see which systems are the top talkers to external IPs or systems with a significant number of failed authentication attempts.

The newly modified Zeus malware and iBanking.Android malware can be identified through steps similar to those used to identify Poweliks, as they rely on security awareness. The Zeus variant can be detected by monitoring the network for connections to the command-and-control IP; iBanking.Android can be detected by using a mobile antimalware tool that scans the system looking for malicious files.

Note that detection is only one part of effectively controlling malware in the enterprise. Rigorous response to incidents involving malware is critical for minimizing the effects from a compromised system.

NO SURPRISES HERE

It should be no surprise that malware will continue to advance and automate some of its most effective manual attack techniques. As enterprise malware defense measures become more sophisticated, malware will inevitably find new methods to circumvent them. This will require constant attention from enterprises in order to control and mitigate potential attacks.

Enterprise security controls and technologies will need to be vetted constantly to ensure they are effective against current attacks. Changing security programs and controls when new attacks or vulnerabilities are discovered is essential to remaining ahead of the curve.

It is also critical for an enterprise to not only evaluate how it manages its systems, but also assess the management of its systems to decide whether certain functionality—such as PowerShell scripts—could potentially introduce new risks into its environment and will require additional policies to prevent vulnerabilities from being exploited.

—Nick Lewis

NICK LEWIS, *CISSP, is the information security officer at Saint Louis University. Lewis received his master of science degree in information assurance from Norwich University in 2005, and in telecommunications from Michigan State University in 2002. Prior to joining Saint Louis University in 2011, Lewis worked at the University of Michigan and at Boston Children's Hospital, the primary pediatric teaching hospital of Harvard Medical School, as well as for Internet2 and Michigan State University.*

ROB SHAPLAND *is a senior penetration tester at First Base Technologies where he specializes in Web application security. He has used his skills to test the websites of companies ranging from large corporations to small businesses, using a wide variety of Web technologies.*

TechTarget

Fighting Crimeware
is a SearchSecurity.com e-publication.

Robert Richardson | *Editorial Director*

Kara Gattine | *Executive Managing Editor*

Brenda L. Horrigan | *Associate Managing Editor*

Kathleen Richards | *Features Editor*

Sharon Shea | *Assistant Editor*

Robert Wright | *Site Editor*

Jacquelyn Howard | *Senior Director, Editorial Production*

Joe Hebert | *Production Editor*

Linda Koury | *Director of Online Design*

Neva Maniscalco | *Graphic Designer*

Doug Olender | *Senior Vice President/Group Publisher*
dolender@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

COVER ART: FOTOLIA