websense

THREAT INTELLIGENCE

DATE: MARCH 2014	ORIGINATOR: WEBSENSE SECURITY LABS

SUBJECT:

WEBSENSE® 2014 THREAT REPORT

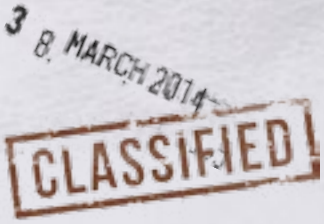
DATE	ACTION	INITIAL
03 JAN 2014	[redacted]	[redacted]
11 JAN 2014	[redacted]	[redacted]
06 FEB 2014	[redacted]	[redacted]
18 FEB 2014	[redacted]	[redacted]
01 MAR 2014	[redacted]	[redacted]
18 MAR 2014	operation kill chain	[redacted]

FOR YOUR EYES ONLY

DA1 FROM MARCH 2014

websense TRITON

CONTENTS



Executive Summary 4

The State of Cybersecurity 6

The New Normal
An Increasingly Complex Attack Ecosystem
Understanding Motivation is Crucial

Mapping the Seven-Stage Kill Chain to the Attack Ecosystem 8

Stage 1: Recon
Description
Motivation
Execution
Recommended Countermeasures

Stage 2: Lure 10
Description
Motivation
Execution
Recommended Countermeasures

Stage 3: Redirect 13
Description
Motivation
Execution
Recommended Countermeasures

Stage 4: Exploit Kit 15
Description
Motivation
Execution
Recommended Countermeasures

Stage 5: Dropper File 17
Description
Motivation
Execution
Recommended Countermeasures

Stage 6: Call Home 19
Description
Motivation
Execution
Recommended Countermeasures

Stage 7: Data Theft 20
Description
Motivation
Execution
Recommended Countermeasures

A Unified Approach to Kill Chain Defenses 22

Conclusion 22

EXECUTIVE SUMMARY

2013 was another eventful year in cybersecurity. From the egregious insider data leak at the world's most technologically advanced security agency, to the major shifts in exploit kit activity triggered by the arrest of Blackhole exploit kit creator Paunch, to the attacks on point-of-sale (POS) systems at Target and Neiman Marcus, the security community was kept busy. New threats emerged every month, using more advanced techniques than before or introducing altogether new methods. Even a high school football team got in on the act, resorting to cybercrime to gain a competitive advantage over an opponent.[1]

The overall success of last year's threats is proof that "advanced attacks" and "targeted attacks" are now the norm, not the exception. The data and numerous examples within this report make it clear — of the more than 4.1 billion live attacks that Websense technology prevented in 2013, nearly all exhibited techniques to bypass traditional defenses, compromise systems, and persist throughout infected networks in pursuit of confidential data.

Though data theft was a common goal of many attacks, attacker motivation varied greatly. Financial gain remained a highly motivating factor, yet some attackers attempted to compromise data for reasons other than making money — to destroy a company's data and impair its competitive advantage, for example, or to disrupt civic infrastructure or steal state secrets.

Attack techniques also ranged far and wide. Some, such as the "royal baby" attacks leveraging the interest in the birth of Prince George, went after wide swaths of users. Others revealed a continuing trend toward highly targeted campaigns, such as the Tibetan website watering hole attacks that focused solely on financial institutions in the Middle East and sent as few as 10 emails from a vendor's compromised email server.[2]

To better understand how an attacker translates motivations into methods, one must understand the apparatus that they create in order to launch and re-launch their campaigns. To this end, the "kill chain" — that set of activities executed by threat actors to penetrate organizations, expand their footprint within these compromised networks, and steal valuable data – is a useful model. The kill chain can be segmented into seven discernible stages to help organizations determine the most effective defense strategies. These seven stages are:

- Recon
- Lure
- Redirect
- Exploit Kit
- Dropper File
- Call Home
- Data Theft

[1]http://msn.foxsports.com/collegefootball/story/louisiana-high-school-cheating-scandal-charges-destrehan-high-used-hudl-website-illegally-scouted-south-lafourche-103113

[2]http://community.websense.com/blogs/securitylabs/archive/2013/08/15/tibetan-compromise.aspx

It's crucial to understand that attacks are using sophisticated techniques to bypass defenses at any or all of the seven stages, and that the further an attack progresses along the threat lifecycle the greater the risk of data theft. Further, rapidly evolving attacks make it more difficult for point security solutions that provide protection across only one or two stages. Effective security in 2014 and beyond requires integrated solutions that protect not only at each individual stage, but also across the entire kill chain.

The Websense® 2014 Threat Report explains the threat landscape through the lens of this seven-stage model to help you:

- Understand the threat lifecycle, current criminal attack apparatus and techniques, and attacker motivations as a foundation for understanding risk and reviewing your security posture.
- Gain deep insight into each stage of the attack lifecycle for crucial clues to understand how cybercriminals conduct their attacks, adapt them and gradually, persistently attempt to get closer to your critical data.
- Recognize that durable protection from the simplest to the most complex new threats ultimately rests in identifying and preventing live attacks at all seven stages, effectively disrupting a criminal's attack apparatus for both current and future attempts to steal your data.

We produced this report with data gathered through the Websense ThreatSeeker® Intelligence Cloud — a global network uniting customers, partners and more than 900 million endpoints to provide visibility into 3-5 billion requests each day, across Windows, Mac, Linux and mobile systems.

THE STATE OF CYBERSECURITY

THE NEW NORMAL

Advanced attacks, including the subset of targeted attacks, are now not only the de facto style of attack, they're happening with increasing frequency. The evidence is provided by the ThreatSeeker Intelligence Cloud, which identifies and responds to changes in the global threat landscape at a "heartbeat" of 2.3 state changes per second.

Frequently, these attacks can be simple attempts to get past an organization's defenses. However, it's important to note that simplicity can be deceptive, for it often hides a complex process that an attacker used to reach that stage. Indeed, a highly sophisticated attacker in pursuit of a high-value target typically will continue to subtly evolve an attack across all seven stages of the kill chain until it hits pay dirt.

In the realm of targeted attacks, cybercriminals are increasingly aiming attacks at:

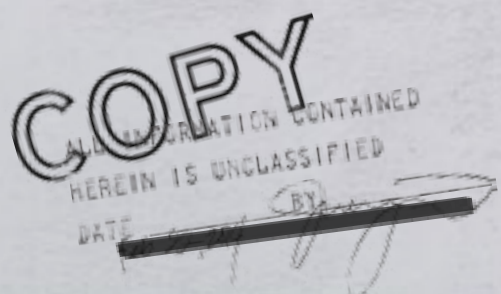
- Specific populations (users within a particular political boundary)
- Geographic regions (users within a particular geographic boundary)
- Groups (users with shared roles or linkages: business functions, shared social habits, user communities)
- A single individual (a user chosen for strategic value)

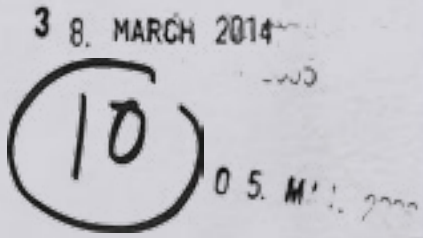
AN INCREASINGLY COMPLEX ATTACK ECOSYSTEM

Any apparent simplicity of an attack can also be deceptive in another sense. The entire attack ecosystem — the extraordinarily diverse body of all the actors, their motivations and the techniques they use to achieve their ends — actually has many moving parts, and these continue to grow in number, complexity and sophistication.

Within this attack ecosystem, a particular attack's apparatus is constantly being developed, enhanced and reused throughout the entire threat lifecycle. As described earlier, this apparatus comprises the necessary components to execute an attack. Examining a common attack apparatus can illustrate the underlying complexity. For example, assembling a big bot network requires:

- An address book of contacts or a collection of compromised servers (to act as watering holes).
- An email or web-based delivery mechanism.
- Socially engineered content for lure activation.





- Redirection servers and domains to mask destination.
- Hosted malicious content servers and domains for exploits and malware.
- Command-and-control (C&C) servers and domains for lateral movement within a targeted network, and further penetration.
- Data exfiltration repositories.

Components such as these are frequently reused in subsequent attacks, with attackers updating parts of — or even the entire — apparatus to account for improvements in security made following the last wave of attacks.

As the attack ecosystem grows in scope, it's getting increasingly difficult to attribute the source of an attack. Many experts and organizations claim to be able to pinpoint the source of an attack, but it is rarely that easy or straightforward. As exemplified in the Zeus attack, the reusing of attack components, compromising of websites and using numerous redirections can all serve to thwart identification of sources (see Figures 1, 2).[3]

Originally designed as a financial threat, the Zeus malware was repurposed in 2013 for other vertical market objectives, from widely distributed attack sources.

Figure 1 & 2

ZEUS TOP 10 BY GEOGRAPHIC LOCATION	
1.	US
2.	UK
3.	INDIA
4.	CANADA
5.	BRASIL
6.	AUSTRALIA
7.	MEXICO
8.	ITALY
9.	FRANCE
10.	TURKEY

ZEUS TOP 10 BY MARKET VERTICAL	
1.	SERVICES
2.	MANUFACTURING
3.	FINANCE
4.	GOVERNMENT
5.	COMMUNICATIONS
6.	EDUCATION
7.	RETAIL
8.	HEALTHCARE
9.	TRANSPORTATION
10.	UTILITIES

[3]http://community.websense.com/blogs/securitylabs/archive/2013/09/09/malicious-emails-target-financial-institutions-in-asia.aspx

UNDERSTANDING MOTIVATION IS CRUCIAL

Understanding cybercriminal motivation at every stage of the kill chain is necessary for comprehending the complex cyberthreat landscape and knowing how to properly defend against advanced attacks.

Opportunities for financial gain abound in the black market hacker economy. Stolen credentials, compromised systems, compromised web servers and pages, new vulnerabilities — all these command a price and can equip other actors for data exfiltration. It's important to note here just how many actors there are in this market. (We define "actor" as anybody trying to do something malicious at any time and at any stage of the threat lifecycle.) As in any economy, there are those actors who enable others by providing one or two key services or technologies (e.g., exploit kits) that other attackers can capitalize on.

In addition, ransomware — malware that enables cybercriminals to hold data hostage — plays upon organizations' fear of data destruction, which potentially has as much value as outright data loss.

Not all opportunities for financial gain require the use of all seven stages in an attack. An "insider attack," for example, transpires solely within the confines of Stage 7 (Data Theft). Another example is a phishing lure that links to a web page that requests user credentials, a hallmark of Stage 2 (Lure).

Further, many sophisticated attacks are aimed at data, not dollar signs. Sometimes an attacker seeks control of infrastructure. Other times an attack goes after state secrets. Occasionally all an attacker wants to do is embarrass an organization simply by breaching its defenses.

The next section explains how cybercriminal motivation changes at each of the seven stages, and shows the value of understanding the stages both individually and holistically.

MAPPING THE SEVEN-STAGE KILL CHAIN TO THE ATTACK ECOSYSTEM

In this section, we review the entire attack ecosystem, including sample attack apparatus, through the lens of the seven-stage kill chain.

STAGE 1: RECON

DESCRIPTION

Recon can be a straightforward or relatively sophisticated process, where technique is determined by intent. One approach to recon takes place outside of an attack, where cybercriminals research their intended victims using personal, professional and social media websites and other public-facing content. Another approach occurs within an actual, multi-stage attack.

MOTIVATION

In the former approach, attackers are looking for information to help them create seemingly trustworthy "lures" (see Stage 2: Lure) that lead to compromised websites under their control. In the latter approach, a cybercriminal attempts to infiltrate an organization's network and exfiltrate user credentials or other personally identifiable information (PII) for use in additional attacks, or for sale on the black market for other cybercriminals to use in their attacks.

EXECUTION

In broadest terms, you can think of the seven-stage attack model as a data-gathering recon exercise for fueling an entire new threat lifecycle, ensuring that the attack apparatus continues unabated. Operating under this modus operandi, and armed with insights gleaned from previous attacks, cybercriminals are able to craft more advanced and targeted attacks.

Recon is becoming more complex. In addition to identifying the target(s), finding the weakest link (i.e., users) through social media, and sending a phishing lure that culminates with an exploited system, cybercriminals are now using entire campaigns as a reconnaissance exercise. A case could be made that Mevade malware is such a campaign. The complexity of the attack, which installed reverse proxies and created anonymity through the free Tor software, implies a sense of persistence that allows the resulting malware to stay hidden and ready for use at any given moment.

Persistence also allows the infection to move laterally, another form of recon that takes inventory of additional information such as databases, critical systems, source code and document repositories. With this information, cybercriminals can create new data theft campaigns against these targets.

RECOMMENDED COUNTERMEASURES

The attack apparatus is usually far less sophisticated at the earlier stages. That's especially the case with recon, where cybercriminals, because they don't yet know exactly who to target, cast a wide net using less-sophisticated techniques aimed at snaring less-

sophisticated users. Therefore, user education is an important and effective defense at this stage. Instruct employees, "If you see something unusual, say something."

The secret to fighting the later, more dangerous stages of the attack model is to catch the early warning signs that recon can reveal at the apparatus level. Paying attention to all security events and performing due diligence can expose the true intent of even the most seemingly basic events. Recognizing that attackers will achieve some level of success at every stage, aggressively monitoring such early-stage activity can help you determine whether a multi-stage attack might be forming.

NOTES: DATE: MARCH 2014

TARGET BREACH: LESSONS LEARNED

It's well known that at the heart of the Target Corp. breach was a novel variant of malware known as a point-of-sale RAM scraper (POSRAM). It's important to understand, however, that a critical catalyst for the success of that breach happened far in advance of the news-making attack. It occurred when a third party, a Target partner, was compromised and a key set of credentials were stolen. To the third party the attack was direct, but the much larger impact was the leaked data that formed the backbone for the subsequent reconnaissance of the much bigger target (i.e., Target Corp.).[4]

PROPERTY OF WEBSENSE SECURITY LABS

You also need to understand the extent of your organization's data flow across all partnerships and vendor relationships and ensure it is protected at every stop along the way. Examine what security measures your partners are taking and ask questions based on the nature of your relationship and the business function they perform. In addition, develop criteria for email, web, data, and cloud security measures that you expect your vendors and partners to have in place.

STAGE 2: LURE

DESCRIPTION

Using information collected in the recon stage, on the black market or via other attacks, cybercriminals create socially engineered web pages and email lures that can cause users to act in ways that seem in their self-interest but in reality lead them astray.

MOTIVATION

In either situation, lures are designed to encourage users to enter credentials or other PII, which cybercriminals can then use in later attack stages or different attacks altogether, or sell on the black market.

[4]Download an infographic of the POSRAM attack at http://www.websense.com/assets/pdf/Infographic-Security-Labs-2014.pdf.

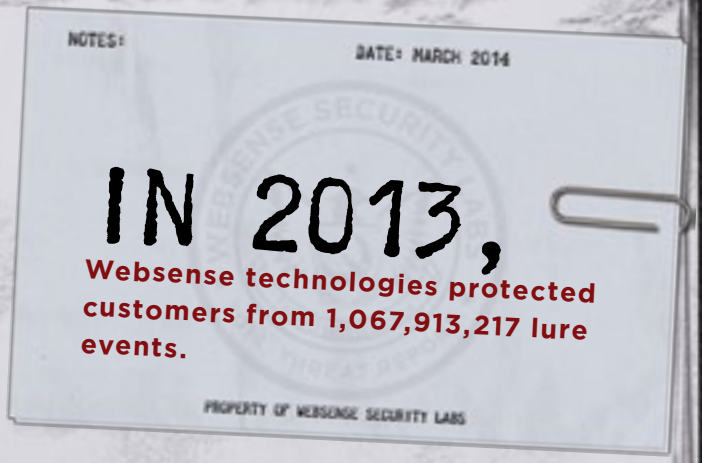
EXECUTION

Lures are dangled via email, social media posts, mobile devices or other content that appear to come from trustworthy sources. Some lures use recent disasters, social drama or celebrity deaths to draw on human curiosity, a relatively primitive form of social engineering. Others are personalized according to the information gleaned through social media profiles.

Typically, lures are only as complicated as they need to be to bypass organizational defenses. The goal of the attack, and the value of the target, determines the level of complexity, as well as the degree to which the attack is targeted. Even though recon is often undertaken precisely to provide targeting information, how targeted an attack is, is often a matter of degree; initially, an attack may target broadly to find an entry point into a system, after which a more fine-tuned attack can be made.

A watering hole attack is an example of a "silent" lure, where an attacker compromises a high-traffic site and relies upon its existing, legitimate content to entice users to act. The scope of such attacks in 2013 was broad, ranging from the massive audience of the NBC.com[5] attack to the highly targeted Tibetan website attacks.[6] By compromising well-known sites, cybercriminals take advantage of the sense of security users feel when they visit familiar sites; in essence, they're attacking unsuspecting users along the cyber paths they travel every day.

Socially engineered phishing emails continue to become more advanced. A good example is a Fox-News-themed campaign that began with highly convincing phishing messages containing information on current events. Going beyond the typical use of a single URL, the email contained numerous links about a variety of subjects, including the activity in Syria, immigration reform and the war on terror.



Overall, in 2013 85 percent of malicious links used in web or email attacks were located on compromised legitimate websites, and 3.3 percent of all spam contained malicious links and other malicious content. The latter figure might not seem like a lot, but given the extremely high volume of spam that businesses encounter, it represents a significant email risk.

RECOMMENDED COUNTERMEASURES

User education is a typical first line of defense against lures, but as with other traditional defenses its efficacy is diminishing in today's advanced threat landscape. Sure, some users might still need to be told not to act on garden-variety Nigerian 419 and other grammatically challenged email scams, for example. However, lures are proliferating in channels beyond

[5]http://community.websense.com/blogs/securitylabs/archive/2013/02/22/nbc-com-compromise.aspx
[6]http://community.websense.com/blogs/securitylabs/archive/2013/08/15/tibetan-compromise.aspx

email (e.g., social media and web), and the sophistication of the underlying technologies and techniques are outstripping the savviness of even the most informed users.

Identifying the luring techniques that cybercriminals employ remains a crucial component of a comprehensive security strategy. Knowing who the attackers are, how they're conducting their attacks and what they're after, can help you strengthen your infrastructure accordingly. But though it's important to interrupt the attacker's ability to gain that first foothold into your network, it's perhaps even more important to gain visibility into the attempts. Lures are social, in that they rely upon words to propagate. Users are social, in that they act on and share content that is usually predictable, such as topical news. Over time attack patterns emerge, and organizations can use these as potential indicators of future attacks.

GEOGRAPHIC DISTRIBUTION OF GLOBAL LURES

Web and email lures during 2013 were globally dispersed, and attackers had a worldwide luring infrastructure to customize their attacks according to the regions of focus.

STAGE 3: REDIRECT

DESCRIPTION

In their lures, cybercriminals may use links that point users to safe-looking or hidden web pages that then "redirect" users to sites containing exploit kits, exploit code, obfuscated scripts or other malicious content.

MOTIVATION

Cybercriminals use redirects not only to obscure their identity, but also to hide the attack apparatus from those who could create defenses.

EXECUTION

Cybercriminals continue masking their true intent with redirection. From a simple URL redirect sent via a phishing email to a silent redirect on a compromised website, the intent is the same: to quietly direct the target along the threat lifecycle to the malicious payload. To traditional static detection methods, the destination appears legitimate. In reality, a compromised page with a dynamic redirection chain behind it can turn even the most innocent-seeming sites into attacker-controlled playgrounds.

An attack on Yahoo at the start of 2014 serves as a good example of the havoc redirects can cause and the unexpected tactics they can use. Numerous redirects lead Yahoo users to an exploit kit that exploited Java vulnerabilities and installed malware including ZeuS, Andromeda and Dorkbot/Ngrbot. At the attack's height, upward of 27,000 infections were recorded per hour, and by the time Yahoo addressed the issue perhaps millions of visitors to the popular search engine had been affected. And these weren't your typical, garden-variety HTTP 302 redirects. A compromised ad server was the apparent culprit, seamlessly delivering the attack to users accustomed to Yahoo ads pointing them to legitimate outside destinations. In other words, Yahoo users were caught unawares because they expected to be redirected — just not to illegitimate sites.

The use of redirects implies a sizable investment of time and effort into building and setting up the attack apparatus. Major components are compromised websites that are used as seemingly legitimate destinations, while the final destination is usually a malicious server. Redirects are often easily hidden amidst normal web browsing behavior, where web pages make numerous legitimate server requests.

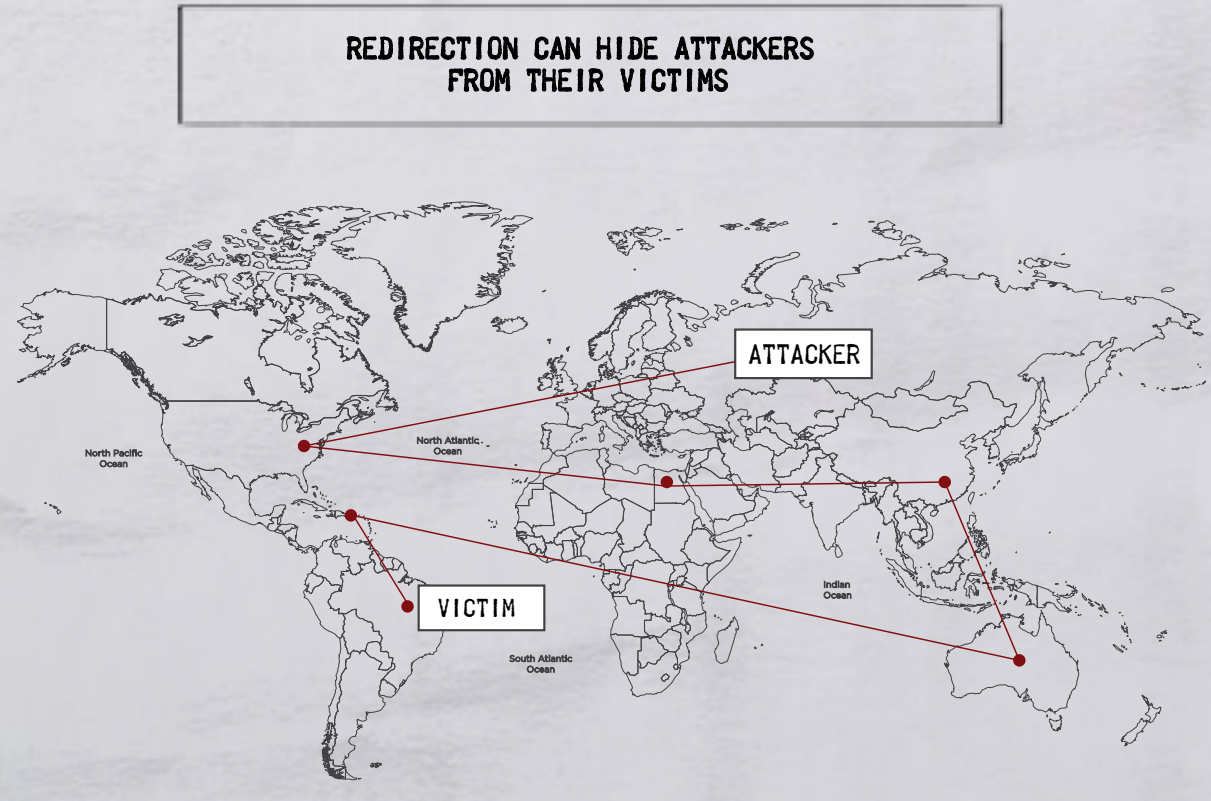
Redirection has become more advanced. The depth of redirection can be astonishing — upward of 10, 20 or more "bounces" can be employed to evade the cybercriminal's true intent. An Israeli website compromise was an example of *fragmented* redirects. Starting with a basic HTML file, the redirects continued to an Adobe Flash file, followed by two more HTML files that ultimately delivered Internet Explorer exploit CVE-2012-4969 — a total of

four redirects, none of which, by themselves, provided any malicious markers. Taken as a whole, however, the various redirects are assembled for delivery of the malicious payload to the user.

RECOMMENDED COUNTERMEASURES

Defenses with real-time awareness of both web page reputation and redirect destination are critical for defending against this stage of attacks, because traditional, basic URL filtering defenses, based on outdated signatures, are ineffective. This last point can't be overstated — from a security perspective, trusting a static representation of the web as a set of URLs you scanned in the past doesn't express the true breadth and millisecond-by-millisecond dynamism of the web and the threat landscape contained within. You can't expect signatures to be accurate.

No matter how many redirects might exist in an attack, it only takes stopping one of them to stop the entire attack. And the ability to do so presents a serious setback for cybercriminals, and not just those behind any single attack. Setting up a redirect network is no small task, so these networks are often sold and shared on the black market and reused frequently. Whenever a network is effectively broken, the cybercriminals that rely upon it are sent back to the drawing board.



The average number of redirects we saw used per attack in 2013 was four. The maximum number we saw used in a fully documented attack was 20.

TOP 10 INITIAL REDIRECT HOSTS

To disguise the malicious nature of the final location, initial redirect destinations are often hidden within compromised, legitimate sites.

1. WEB AND EMAIL SPAM
2. SEX
3. HACKING
4. ILLEGAL OR QUESTIONABLE
5. BUSINESS AND ECONOMY
6. INFORMATION TECHNOLOGY
7. SHOPPING
8. TRAVEL
9. ENTERTAINMENT
10. ADVERTISEMENT

NOTES:

DATE: MARCH 2014

IN 2013,

Websense technologies protected customers from 1,815,242,594 redirect events.

PROPERTY OF WEBSENSE SECURITY LABS

STAGE 4: EXPLOIT KIT

DESCRIPTION

Once a user has clicked on a link to a compromised website, software known as an exploit kit scans the victim's system to find known and zero-day vulnerabilities.

MOTIVATION

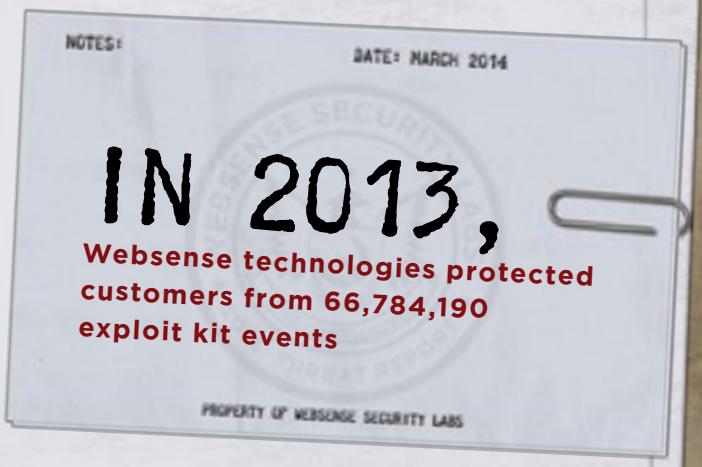
Cybercriminals seek weaknesses that can become open doors for delivering malware, key loggers or other advanced tools that enable them to further infiltrate networks and steal data or compromise systems. They also seek to bypass static defenses by adapting their exploits and keeping ahead of the latest security updates.

EXECUTION

Exploit kits remain a common delivery mechanism for compromising a target. Their increasing complexity and speed at which they evolve to include new vulnerabilities make detection difficult. At particular risk for use in the delivery of later stages of the attack lifecycle are browsers, custom apps and anything else that uses the (likely out-of-date)

Java Runtime Environment (JRE) with its extensively documented known and zero-day vulnerabilities.[7]

For most of 2013, Blackhole represented the largest volume of exploit activity. Its success was at least partially attributable to the speed at which it incorporated new exploits, often within one week of discovery. But the arrest of Blackhole creator Paunch forced the criminal underground to move on, trying a variety of exploit kits (e.g., Magnitude and Neutrino) looking for a suitable replacement (Figure 3).[8]



Within a week of Paunch's arrest, Websense researchers noted a dramatic increase in the variety of techniques used by the cybercriminal community. Malicious email links that previously redirected to Blackhole exploit kits, for example, began pointing to the Magnitude exploit kit. Further, for a short time direct email attachments were the predominant attack mechanism. Cybercriminals thus have proven that the loss of Blackhole will not deter them from their goals.

Java vulnerabilities, and the lack of updates, makes the challenge of exploiting targets that much easier. Twice in 2013 Websense researched Java implementations of advanced threats.[9] In both cases, the results were alarming.

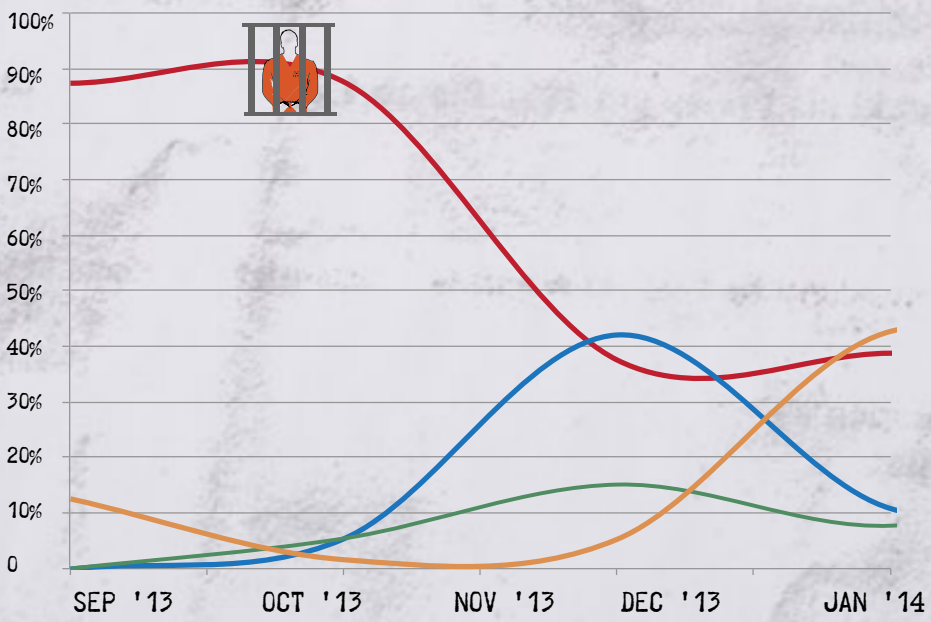
- One month after the release of a new version of Java, adoption was only 7 percent.
- In another report 31 percent of systems were using a version of Java outdated by 1 year or more.

This lack of Java updating creates a fertile environment for cybercriminals where, with the latest unfixed exploit, upward of 94 percent of Java-enabled browsers are susceptible.

RECOMMENDED COUNTERMEASURES

Most bypasses of traditional defenses occur after a handful of commercially available, mass-market exploit kits are used to modify the existing apparatus; note that it only takes an incremental change to render these traditional defenses ineffective. It's therefore critical to understand how variations of those exploit kits are made creates opportunities to programmatically intercept all variations of those kits.

[7] http://www.websense.com/content/whitepaper-java-exploits-top-security-risk.aspx
[8] http://community.websense.com/blogs/securitylabs/archive/2013/12/17/exploit-kits-lacking-paunch.aspx
[9] http://www.websense.com/content/whitepaper-java-exploits-top-security-risk.aspx



Exploit kits struggle for dominance in the void left by Blackhole after the arrest of Paunch in October.

Figure 3

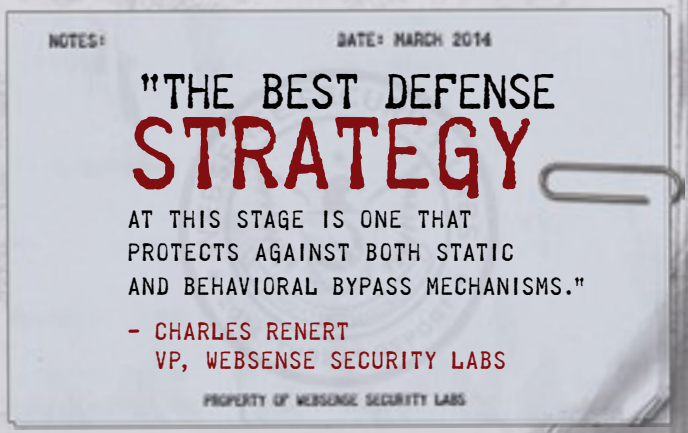
STAGE 5: DROPPER FILE

DESCRIPTION

The dropper file is the object that, once delivered and installed on a system or endpoint, enables the attacker to persist and advance an attack.

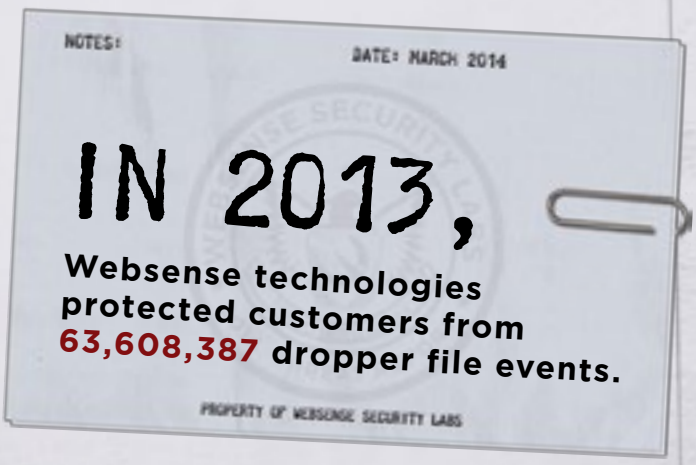
MOTIVATION

This is the point of the attack where the attacker attempts to gain control of a system or endpoint. The dropper file may contain software that executes on the victim's system to begin the process of fulfilling the goals of the attack by establishing a line of communication between the compromised system or endpoint and the attacker. Dropper files often establish a means for persistence on a compromised system, becoming a "window" into that system and providing a way for the attacker to move laterally.



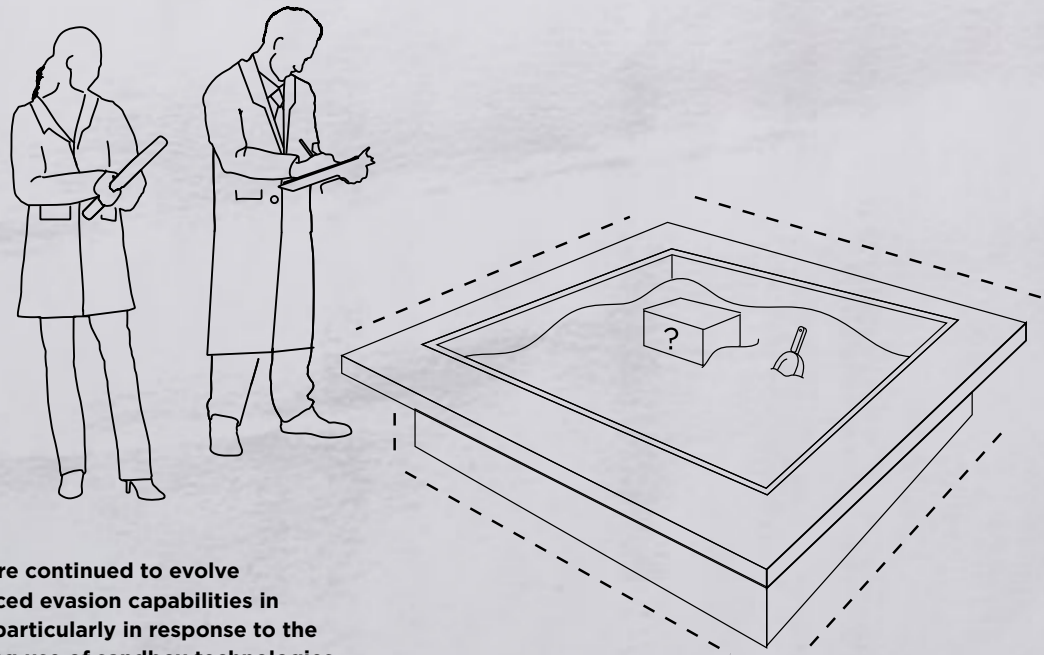
EXECUTION

By far the most pervasive (and effective) bypass technique for dropper files is to make trivial alterations to their compiled code to defeat the signatures of traditional anti-virus products. Beyond that, malware that checks for certain non-standard conditions and apps that don't perfectly match those installed by analyzers (even different versions of the same app or even .DLL) are among the attack strategies cybercriminals employ to get past behavioral defenses. Dropper files establish a direct connection between the attacker and the infected system. They employ two kinds of defense bypass mechanisms: static and behavioral.



Rapid variations enable dropper files to easily evade detection by static, signature-based defenses such as anti-virus, whose signatures often are not updated in time. Given the increasing use of file sandboxing, there has been a sharp rise in behavioral evasion techniques, including:

- Use-time delays before exhibiting malicious behavior.
- Testing for human interaction, to ensure the environment is not completely automated or simulated.
- Probing for indicators of a virtual environment.



Malware continued to evolve advanced evasion capabilities in 2013, particularly in response to the growing use of sandbox technologies.

Each technique has its strengths and weaknesses. Cybercriminals continue to evolve their methods to identify sandboxes without giving away their intent, minimize "false positive" sandbox identifications and still achieve their objectives.

In addition, the use of ransomware such as Cryptolocker is on the rise. With ransomware, no data exfiltration is required for an attacker to profit; the goal is not stealing data but preventing users' from accessing their data until paying a ransom. Therefore, a ransomware attack does not require all seven stages to succeed.

RECOMMENDED COUNTERMEASURES

Because traditional static defenses on their own are inadequate to address security at this stage, and due to the increase in sandbox evasion techniques, the best, most proactive defense strategy is a combination of activities. These can include real-time defenses that enable the identification of current behavior markers, delivery mechanisms, and content around the object (who signed it, origin domain, reputation, etc.).

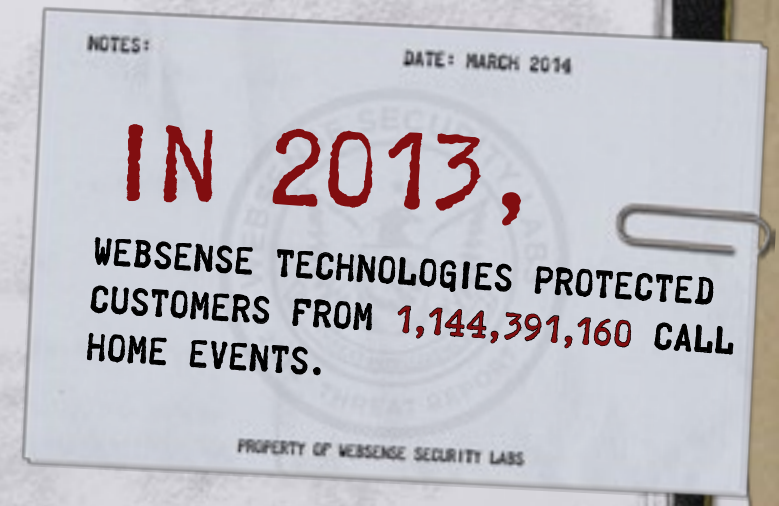
STAGE 6: CALL HOME

DESCRIPTION

Once the dropper file infects the target system, it "calls home" to a C&C server to download additional programs, tools or instructions.

MOTIVATION

Cybercriminals can have a variety of motivations — such as sending spam, moving laterally through a network to conduct recon, pulling off a distributed denial-of-service (DDOS) attack, or stealing data — and these motivations can change at any stage of an attack. The C&C apparatus enables a shift from one to another. It also can serve multiple attacks at once, enabling its simultaneous reuse among a number of attackers.



EXECUTION

Cybercriminals attempt to evade C&C detection in numerous ways. For example, the Mevade attack installed a full-weight proxy that enabled cybercriminals to tunnel through NAT environments and initiate a backdoor into the target network. There is also evidence that Mevade (and its close cousin Sefnit) further enhances this backdoor through the use of Tor to provide almost complete anonymity for the attackers.

In C&C the use of SSL is very uncommon due to the overhead of certificates, making custom encryption by far the tool of choice for hiding the communications between attacker and victim.

We're also seeing more redirection take place within outbound C&C communications, where cybercriminals avoid detection by moving data through "legitimate" locations. Many of these locations were unknowingly used as redirect "hops" to hide the final destination. By using dynamic DNS from a known security provider, the malicious intent behind the redirects is more difficult to ascertain.

COMMAND-AND-CONTROL MECHANISMS WORK

WHEN ORGANIZATIONS EITHER DO NOT OR CANNOT INSPECT THE INCREASINGLY RELIED UPON SSL/TLS CHANNEL.

For more advanced attacks, the initial C&C is often simple beacon back to the command center.

RECOMMENDED COUNTERMEASURES

To combat C&C communications, it's important to scan outbound communications, monitor both SSL/TLS and non-SSL/TLS traffic, and have destination-aware defenses — all features lacking in traditional security products. Such defenses are especially crucial given that, according to an internal Websense study of our customers' traffic, 30 — 40 percent of enterprise traffic is SSL/TLS, and 40 percent of the most popular sites (e.g., Facebook, Google, Twitter, Yahoo) use SSL/TLS.

STAGE 7: DATA THEFT

DESCRIPTION

The end-game of most modern cyber attacks, the theft or destruction of data completes the kill chain.

MOTIVATION

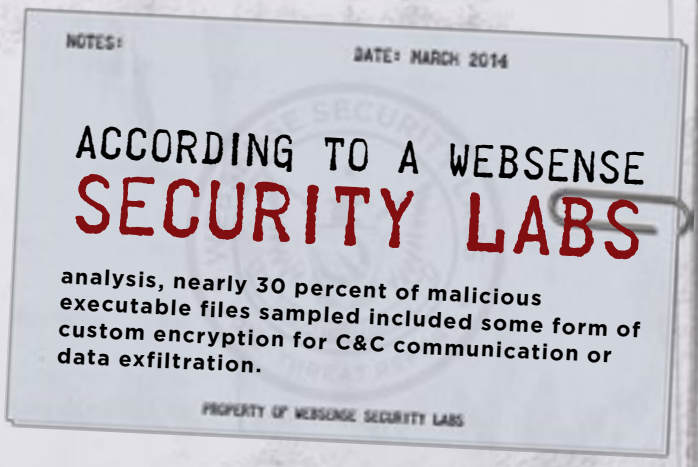
Cybercriminals steal intellectual property, personally identifiable information or other valuable data for financial gain, for use in other attacks or sometimes to destroy.

EXECUTION

There are far fewer events in the data theft stage than at any other stage, yet these events have the biggest potential consequences. Most frequently, successful data theft happens

in a singular event — that's all it takes. Yet data theft can also occur in a slow trickle of data exfiltration events ("data drip") over time. In any case, this stage is your last opportunity to prevent.

As with C&C, encryption is commonly used at this stage. However, unlike C&C, the use of SSL is more common than custom encryption, especially in data exfiltration events where attackers use third-party sites to warehouse their data to avoid attribution (e.g., Dropbox, social networking sites).



Data theft is often the product of much preliminary recon, staging and compromise activities. These culminate in the exfiltration of data in up to three ways:

- Via "in-the-clear" text, which appears as legitimate, high-volume data traffic and is easily scanned by defenses.
- Via SSL/TLS, which is an increasingly common mechanism for data transmission and is much more expensive to scan.
- Via custom-encrypted files that are sent over legitimate data channels that are effectively impossible to scan.

Data can be exfiltrated from a variety of channels, depending on what's enabled. The most common are HTTP and HTTPS, but there are others. For example, in 2013's Target Corp. breach, data appeared to have been stolen via FTP.

Drip data exfiltration is increasing as a technique for bypassing data security defenses. To prevent the triggering of data-security thresholds through the exfiltration of a large amount of data at one time, in a drip data loss scenario data is released in smaller bites, appearing to a data security solution as normal business traffic. By remaining beneath a particular threshold, the data loss can continue for an indefinite period of time.

RECOMMENDED COUNTERMEASURES

The relative low volume of data theft events make them the most challenging to detect, but the potential havoc they wreak make them the most critical to detect. Your best defense against

data theft is to have defenses at each of the other six stages in the attack lifecycle. Yet even at this final stage, there are contextual markers that can help you determine your organization's risk and how to remediate a current data security event and those in the future.

Traditional data loss prevention (DLP) solutions that address compliance and regulatory issues are important, but these do not address attempts at active data exfiltration. The best techniques for catching these attempts exist in a full data theft prevention (DTP) solution, and include: scanning outbound content for proprietary material; scanning images with OCR technology; and using "data drip protection" technology that can identify slow data exfiltration.

Other important layers for DTP includes scanning all clear text and SSL/TLS events for your data, and blocking all non-standard encryption methods.

A UNIFIED APPROACH TO KILL CHAIN DEFENSES

At each of the seven stages, we've covered Recommended Countermeasures to take, and these are important. Each stage carries rich context pertaining to the attack apparatus — geographic origin, authorship, techniques and more — and it's worthwhile and vital to take advantage of this information.

However, it's insufficient to focus solely on any one stage or point solution. Instead, it's crucial to consider the seven stages as a whole, and to cover your entire infrastructure with a convergence of web, email and mobile security. Recognizing the rich contextual information inherent in each stage, you can imagine how much this valuable intelligence is present in a solution that comprises all seven stages of the kill chain and the attack model.

There is an additional point to consider that underscores the importance of a comprehensive approach. While each stage of the attack model represents an opportunity for your organization to respond to threats, they also provide attackers a chance to bypass your defenses. If your defenses are non-existent at one stage because you've focused your defenses on one or more of the other stages, your organization remains vulnerable.

By evaluating the full range of threat activity, you can look forward and backward throughout the threat lifecycle, evaluating each stage for threats and responding accordingly. These techniques are also valuable at generating threat intelligence and awareness for future attacks.

CONCLUSION

Almost all of today's cyber attacks have raised the cybersecurity bar through a complex set of infrastructure and tools cybercriminals use to rapidly launch new attacks and thereby evade traditional controls. The best defense is to understand malicious techniques and likewise raise the bar on your defenses.

A good starting point is to view the threat landscape though the lens of the seven-stage kill chain. This segmentation provides a structure not only for understanding how the attack apparatus works, but also for organizing your defenses at each stage — and across all stages.

In addition, knowing what motivates an attacker — seeing an attack through the attacker's eyes — provides crucial insight for grasping criminal behavior and anticipating next moves.

It's also important to understand the true nature of attacks. Most are not highly targeted advanced persistent threats (APTs), because criminals often lack the skills or resources to create a brand new attack apparatus and threat techniques at every stage. Instead, most leverage proven techniques from the past success to engineer future threats, aiming for only the bare minimum capabilities to bypass simple countermeasures.

Therein lies the opportunity — if you block every stage of an attack today, you'll have a fair shot at interrupting the next attack, too.

Websense, Inc. is a global leader in protecting organizations from the latest cyber attacks and data theft. Websense® TRITON® comprehensive security solutions unify web security, email security, mobile security and data loss prevention (DLP) at the lowest total cost of ownership. More than 11,000 enterprises rely on TRITON security intelligence to stop advanced persistent threats, targeted attacks and evolving malware. Websense prevents data breaches, intellectual property theft and enforces security compliance and best practices. A global network of channel partners distributes scalable, unified appliance- and cloud-based TRITON solutions.

TRITON stops more threats; visit **www.websense.com/proveit** to see proof. To access the latest Websense security insights and connect through social media, please visit www.websense.com/smc. For more information, visit www.websense.com and www.websense.com/triton.

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

websense®
www.websense.com

websense
TRITON®

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

websense®
www.websense.com

websense
TRITON®