websense®

2014

1 2 3 4 5 6 7 8

SECURITY PREDICTIONS

websense
TRITON®

websense®

2014 SECURITY PREDICTIONS

TABLE OF CONTENTS

INTRO

Every fall, Websense® Security Labs™ researchers predict the key threats your organization should prepare for in the coming year. They arrive at their predictions after carefully analyzing data from a number of sources. These include the core Websense technologies and security intelligence that informs our industry-leading security solutions, as well as trends in cyberthreats, technology, politics, economics and more.

The following eight predictions and recommendations indicate cybersecurity professionals are in for another bumpy ride in 2014. Some of the biggest challenges will come from areas where most security providers aren't even looking. You can use these insights to review current defenses, identify security gaps and prepare new safeguards.

1 ADVANCED MALWARE VOLUME WILL DECREASE.

It probably sounds surprising to hear this from a cybersecurity company, but according to the real-time telemetry feeds in Websense ThreatSeeker® Intelligence Cloud, the quantity of new malware is beginning to decline. Unfortunately, this isn't good news.

Cybercriminals will rely less on high-volume advanced malware because over time it runs a higher risk of detection. They will instead use lower volume, more targeted attacks to secure a foothold, steal user credentials and move unilaterally throughout infiltrated networks. Although the volume of attacks will decrease, the risk is even greater because of the increasingly stealthy nature of threats. In many cases, a single entry point into an organization's network is enough to build up to a complex data exfiltration attack.

Further, if cybercriminals steal user credentials, they can directly access cloud services and mobility infrastructure (e.g., VPN or RDP). This access would allow criminals to establish a presence by creating new domain-level user accounts, without resorting to massive malware distribution.

RECOMMENDATION

Organizations can't rely on anti-virus (AV), firewalls or other traditional security measures to save their networks. Security teams need a comprehensive security solution that not only detects malware activity, but goes a step further by detecting and protecting against anomalous activity. It's time to transform security thinking from "setting and forgetting" to using technology that can stop threats by analyzing irregular behavior and sleuthing through the data. Stopping the most advanced, targeted attacks requires amplified information collecting that investigates threat behavior in real time.

2 A MAJOR DATA-DESTRUCTION ATTACK WILL HAPPEN.

Most attackers historically used a network breach to steal information for profit. In 2014, organizations need to be concerned about nation-states and cybercriminals using a breach to destroy data. Ransomware — where cybercriminals hold corporate data hostage and demand a ransom be paid in exchange for its release — will play a part in this trend. In fact, the 2013 resurgence of CryptoLocker demonstrated how one small piece of malware, on a single computer, can hold an entire organization hostage by locking out network drives. This and other ransomware campaigns were just the tip of the iceberg. We expect this trend to move down market, affecting small- and medium-sized organizations.

The monetary gain for ransomware can prove to be extreme, hence the continued motivation to employ this attack strategy. Unfortunately there is no guarantee that the ransomed data will be returned. Many cybercriminals collect ransom without returning the data to its rightful owner.

RECOMMENDATION

Make sure your organization is protected from targeted attacks, properly backs up data and segments each network. This will eliminate attacker advantage if they gain access, destroy your data or attempt to hold your sensitive information hostage. In addition, deploy a comprehensive data loss prevention (DLP) solution to enable your team to track and monitor the movement of your most sensitive data.

3 ATTACKERS WILL BE MORE INTERESTED IN CLOUD DATA THAN YOUR NETWORK.

Cybercriminals will focus their attacks more on data stored in the cloud. This tactical shift follows the movement of critical business data to cloud-based solutions such as Google, Microsoft Office 365 and Confluence. They will find that penetrating the data-rich cloud can be easier and more profitable than getting through the “castle walls” of an on-premise enterprise network.

No doubt, attackers will still infiltrate enterprise networks to target users, steal information and compromise their systems. However, such attacks will serve as an intermediate step to gain access to third-party cloud services instead of an internal data store.

RECOMMENDATION

Implement a comprehensive DLP solution that can help you identify what data is in the cloud and where it resides. Understand who is accessing your data and ensure these individuals have hardened access controls and the proper security training. In addition, make sure that the database containing your most sensitive information has extra protection.

4

REDKIT, NEUTRINO AND OTHER EXPLOIT KITS WILL STRUGGLE FOR POWER IN THE WAKE OF THE BLACKHOLE AUTHOR ARREST.

The Blackhole exploit kit was arguably the most successful in history. Everything changed in October 2013 when "Paunch," the alleged hacker author behind the famous kit, was arrested in Russia. Websense Security Labs predicts that we will see a fight for market leadership between a number of new entrants and existing exploit kits in 2014. Similar to brick-and-mortar criminal rings, now that the kingpin is removed, others will rise in popularity and struggle for dominance.

Until the arrest of Paunch, Blackhole was used in the biggest percentage of exploit activity, and for good reason: its owner was adept at staying up-to-date with the most recent vulnerabilities. Blackhole had been followed in popularity by the Cool, Gong da and Redkit exploit kits. But the exploit kit market was disrupted almost immediately — within a month of Paunch's arrest, Blackhole had dropped from the top spot to number eight behind Redkit.

To fill the void, we anticipate Redkit and the Neutrino exploit kit will secure a strong foothold in the coming year. Neutrino has incorporated Microsoft Internet Explorer zero-days very quickly and has increasingly become a Blackhole replacement. We also anticipate seeing fragmented exploit kits appear more frequently than top kits. This fragmentation will increase the volume of exploit kits that information security professionals need to monitor.

RECOMMENDATION

Information security professionals need to stay updated on how the exploit kit market changes in 2014. Stay tuned to the Websense Security Labs blog for the latest news on exploit kit developments: **community.websense.com/blogs/securitylabs**.

5 JAVA WILL REMAIN HIGHLY EXPLOITABLE AND HIGHLY EXPLOITED — WITH EXPANDED REPERCUSSIONS.

Despite highly publicized and successful exploitations of Java vulnerabilities throughout 2013, most end points continue to run older versions of Java and therefore remain extremely exposed to exploitation.[1] The situation is not expected to change in 2014.

Pragmatism, not ignorance, is behind most decisions not to update Java. Patching is still an unfeasible option for many organizations, particularly those using business-critical applications that have not been updated to support more recent versions of the platform. And alternative approaches combining a variety of tactics are time-consuming for IT to design and implement.

In addition, we anticipate repercussions throughout the threat landscape. **These include:**

- With numerous proven Java exploits to choose from, cybercriminals will devote more time to finding new uses for tried-and-trusted attacks or to crafting other aspects of their advanced, multi-stage attacks.[2]
- Cybercriminals will look elsewhere for similarly exploitable opportunities. Our researchers are paying particular attention to Flash, web-kits and several other popular platforms that, like Java, are popular, readily exploited and inconsistently updated.
- Cybercriminals will reserve the use of zero-day Java exploits for targeting high-value networks with good Java patching practices.

RECOMMENDATION

To balance business needs with enterprise security requirements, the best practices are to blend tactics. Patch, uninstall Java when it isn't required, and implement the "alternative browser" approach. The alternative browser approach dedicates machines and browsers for the use of Java-based applications and all others are kept secure against Java vulnerabilities. In addition, deploy comprehensive and integrated cybersecurity solutions.

[1] Websense Security Labs blog, 9/5/13, "New Java and Flash Research Shows a Dangerous Update Gap," **http://wb-sn.com/16p9YPz**

[2] Learn more about The Seven Stages of Advanced Threats at **www.websense.com/sevenstages**.

6 ATTACKERS WILL INCREASINGLY LURE EXECUTIVES AND COMPROMISE ORGANIZATIONS VIA PROFESSIONAL SOCIAL NETWORKS.

During the first stage of the advanced threat kill chain, cybercriminals conduct reconnaissance to gather intelligence on their potential victims.[3] In 2014, attackers will increasingly use work-oriented social networks, such as LinkedIn, instead of personal social media (e.g., Facebook) when targeting professionals. The information gathered this way will be used to compromise networks.

We predict many of the cybercrime tactics that are successful when targeting personal social networking users will be applied in new, innovative ways within professional social networks. For example, in October 2013, Websense Security Labs researchers discovered a false LinkedIn profile that pinpointed targets for an upcoming phishing campaign.[4] A fake user named "Jessica Reinsch" contacted specific LinkedIn users chosen for their job title, company size and other information. Cybercriminals then lured these contacts to endorse the counterfeit account and visit their malicious website. This added creditability for the fake profile and provided attackers with insight into each target's professional network.

RECOMMENDATION

Networking is a powerful business tool. Unfortunately, it can provide cybercriminals access to a professional's social connections and a direct communication channel to deliver malware. To avoid becoming a victim of socially engineered cyberattacks, members of LinkedIn and other professional social networks need to be wary of those attempting to connect with them. Verify a legitimate relationship before adding connections and determine why this person wants to interact. In addition, as a best practice, educate your workforce about the reconnaissance stage of the advanced threat kill chain.[5]

[3] Learn more about the advanced threat kill chain at **www.websense.com/sevenstages**.

[4] Websense Security Labs blog, 10/31/13, "LinkedIn Lure Looking for Love-ly Profiles, Possibly More," **http://wb-sn.com/1b6yO8y**.

[5] See again at **www.websense.com/sevenstages**.

7 CYBERCRIMINALS WILL TARGET THE WEAKEST LINKS IN THE "DATA-EXCHANGE CHAIN."

Many high-value government and enterprise targets, after years of being hacked or attacked, have significantly improved their defensive strategies and capabilities. Cybercriminals will therefore increasingly go after the contractors, vendors and others that comprise the "data-exchange chain" with the larger, more valuable targets — for fewer of these partners have sufficient defenses. Any organization in the data-exchange chain is a potential target or can serve as a means of attacking the "big prize."

As transactions move from using physical currency to digital forms such as "electronic wallets," the number of organizations in the data-exchange chain will continue to grow. Cybercriminals could go after any organization in the chain that collects, processes, records, or bills any part of these transactions.

RECOMMENDATION

You need to understand the extent of your organization's data flow 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.

8

MISTAKES WILL BE MADE IN "OFFENSIVE" SECURITY DUE TO MISATTRIBUTION OF AN ATTACK'S SOURCE.

For several years, we've been hearing more about "offensive" security, where global governments and enterprises have been threatening retaliatory strikes against anyone caught attacking them or their interests. As in traditional warfare, tactical mistakes will increasingly happen in these cybertrenches.

Security teams might feel justified in mounting counter-cyberattacks in response to harmful incoming incidents, but the reality is that correctly attributing an attack's true source is exceptionally difficult even for the most experienced experts. Failure to accurately identify the perpetrator could trigger a retaliatory strike against the owner of a compromised website commandeered in the attack. As a result, the innocent organizations caught in the crossfire will suffer varying and potentially grave consequences.

Other repercussions are less clear but still potentially impactful. Attacks that hit undeserving targets might result in numerous lawsuits among affected parties, and the lack of legal precedent in this realm could delay or prevent timely resolution.

RECOMMENDATION

Never hack back, because offensive attacks do more harm than good. Instead, adopt a robust incident response and security triage program to collect as much forensic information as possible before passing it on to internal teams or trusted third parties. The more information you can gather at this stage, the better. In addition, improve your organization's attack-prevention defenses by adding real-time defenses that correlate with the advanced threat kill chain.[6]

[6] See again at **www.websense.com/sevenstages**.

ABOUT WEBSENSE

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. Tens of thousands of enterprises rely on Websense 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 Websense TRITON solutions.

Websense 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.

websense®

websense TRITON®