WEBROOT®

Top 5 Malware Trends for 2014 and How to Combat Them

In This Paper

- Malware will continue to evolve and attacks will become more sophisticated this year
- Increased use of mobile devices makes it more challenging to protect systems and data
- Companies need a security solution that protects PCs, tablets, and smartphones against malware and web threats

eSecurity Planet

Executive Brief

Introduction

In 2014, hackers and cyber thieves will continue to change their tactics, using new exploits to infect systems and steal data. This Executive Brief discusses the top five malware trends to keep an eye out for in 2014 and how Webroot SecureAnywhere can provide the endpoint protection that companies will need to be safe in 2014.

Dubbed by some as the year of the personal data breach, 2013 saw hacks and cyber thefts dominating the news capped off with major breaches at Target and Neiman Marcus.[i] Most of the breaches used varying modus operandi to install malware to compromise systems.

Unfortunately, this scenario is expected to continue in 2014. This year, hackers and cyber thieves are expected to evolve their techniques. This will make it ever-more challenging for companies to protect their systems and safeguard their data.

Simply put, in the coming year companies will need to deal with new types of attacks, while continuing to defend against older attacks that can still cause problems. To keep up with the changing methods that will be employed to steal information and commit fraud, companies need to be aware of the following malware trends for the coming year.

Trend 1: Web-based malware on the rise

A fairly large percentage of malware infections today are the result of what are known as drive-by-downloads. When users go to a compromised or rogue site, malware is automatically installed on their device.

Some of the techniques used to compromise sites include injection attacks that take advantage of flaws in SQL databases and libraries, and cross site scripting attacks. These types of attacks focus on compromising legitimate web sites. In many cases, when sites are compromised using these techniques, hackers target weaknesses in web browsers and their plug-ins with HTML or JavaScript exploit code. In 2014, hackers will continue to leverage newly found web server and application vulnerabilities to infect commercial web sites.

Increasingly, other forms of web-based malware attacks are being used. For example, early this year hackers infected[ii] a third-party advertising network that fed ads to Yahoo users. Clicking on the ads directed users to web sites poised to deliver malware.

To put the issue of web-based malware into perspective, consider that Google's malware detection component in Chrome, called Content Agnostic Malware Protection, detected more than 5 million malware downloads per month in 2013. In the coming year, hackers will continue to refine their techniques to direct users to rogue sites and to compromise legitimate sites.

Trend 2: Continued growth of botnets

Malware infected PCs and servers are often commandeered for use in massive botnets. In the past few years, such nets increasingly have been used to carry out click fraud[iii] (with the bots simulating clicks on web site ads, where the actions generate revenue on a per-click basis). Some botnets have been used for Bitcoin mining.[iv] And many botnets have been used to launch large-scale Distributed Denial of Service (DDoS) attacks.[v]

For years, botnets have been attractive to malicious individuals and groups because they deliver cheap processing power and provide a platform to launch spam and other attacks. In fact, botnets were used in a number of highly disruptive DDoS campaigns against U.S. banks over the past two years.[vi]

Despite some notable interruptions of some major botnets in 2013,[vii] industry experts expect hacker interest in botnets to rise in coming years. DDoS attacks against commercial entities have proven to be effective at disrupting business and bringing attention to causes espoused by hackavists.

Furthermore, as more devices become IP-enabled, and the Internet of Things approach to gadgets takes hold, there will be more devices that can be compromised and included in botnets for distributed attacks.

Trend 3: Increasingly sophisticated socially engineered phishing attacks

Phishing attacks have long been used by hackers to compromise systems through infected attachments or to direct users to rogue sites. Such sites either are poised to deliver malware or pose as legitimate sites in an attempt to steal passwords and other personally identifiable information to be used in identity theft and fraud.

Phishing attacks were on the rise in 2013[viii] and are expected to continue to grow in 2014. One of the more recent troubling trends with phishing is its increased sophistication through the use of social engineering techniques.

For example, social networks are now frequently mined for information to make phishing attacks more targeted. Determining the names of friends or coworkers on social sites lets hackers use that information in a more customized phishing email. In many cases, a message may imply the email came from a friend or the sender was directed to the recipient through a mutual acquaintance. Such email messages may cause even those savvy about security to let down their guard and open an attachment or click on a link.

Hackers also are now more likely to customize attacks to take advantage of news-based events. Whether involving the installation of the new Pope, a public meltdown of a celebrity, or a major disaster, hackers quickly pushed out tailored phishing email messages[ix] to entice people to click on links to get more information or, in the case of disasters, contribute to the relief efforts. Such attacks will likely continue in 2014.

"Hackers will continue to refine their techniques to direct users to rogue sites and to compromise legitimate sites."

One disturbing trend to keep an eye out for is the increased use of phishing in what is being called piggyback attacks. In such attacks, hackers leverage customer confusion after a major breach and, in what appears to be an effort to help the customer resolve problems or get

additional information, tries to get them to open an attachment or go to a rogue site. Last year, piggyback attacks were launched after major breaches at Target[x] and JPMorgan.[xi] Expect more of these attacks in 2014 whenever there is a major breach.

Trend 4: Source code leaks and targeted attacks that steal source code

Hackers frequently exploit newly found vulnerabilities, deploying malware aimed at the latest weaknesses as they are identified. In the past, this approach typically relied on someone in their normal course of business coming across the vulnerability.

But last year saw a rise in a more pro-active approach to finding vulnerabilities. Specifically, there were several highly publicized cases where thieves carried out targeted attacks to steal source code. One example was a major breach at Abode where hackers stole user passwords AND source code to Adobe Acrobat, ColdFusion, and other products.[xii]

Such source code leaks potentially can be very damaging. With the information about the actual code, hackers can find new vulnerabilities and exploit them.

Trend 5: Mobile SMS-forwarding malware increases

Malware targeted at mobile devices will increase in sophistication this year. This will make it harder to protect user identities and data, particularly as companies embrace "bring-your-own-device" (BYOD) policies.

One notably troubling mobile threat that is expected to bring new and bigger problems is SMS forwarding malware. As the name implies, such malware is capable of intercepting and forwarding SMS messages.

Unfortunately, cyber thieves are demonstrating great creativity when it comes to using this relatively new malicious method to commit crimes.

One approach, dubbed premium-rate fraud, compromises a mobile device and sends SMS messages to premium-rate services.[xiii] Such services are growing in popularity, allowing users to pay for items or contribute money to charitable causes by simply sending a text message. The fraud is typically carried out using a compromised app.

Another scheme takes a more traditional approach targeting users' credit cards and bank accounts. The technique takes advantage of the increased use of text messages to transmit authentication information. For example, many banks will ask online customers using public or new computers to verify themselves by entering an access code sent to their mobile phone. Hackers capturing this authentication information can use it to access online accounts.

This year, SMS-related techniques will simply expand the possibilities for malicious activities by hackers and cyber thieves.

Other trends to keep an eye out for

In addition to the five trends noted above, companies need to consider other issues that will likely have some impact this year.

For years, hackers targeted Windows PCs and servers. This year will see more threats aimed at other operating systems.

To that point, last year saw a hint of things to come. Hackers focused on Mac OS X systems with new variants of malware.[xiv] In one widely reported attack, cyber thieves brought ransomware to OS X systems.[xv] Infected systems would display what appeared to be a message from the FBI warning users they had viewed pages with prohibited content and their browser was locked. Users were instructed to pay $300 to unlock the computer and "avoid other legal consequences."

In 2013, there also was an increase in attacks aimed at Linux systems. Because Linux systems are widely used to run web sites, such attacks can have significant consequences.

Malware attacks on Mac OS X and Linux systems are expected to increase in 2014.

"In 2014, companies will need an integrated security solution that protects against malware and web threats, across PCs, tablets, and smartphones."

The other trend to keep an eye on is the advent of more targeted malware aimed at mobile devices. The number of malicious mobile apps jumped 614 percent last year,[xvi] demonstrating the exponentially higher cyber criminal interest in exploiting mobile devices. The increased reliance on mobile devices for business by users and their increased acceptance by businesses via BYOD policies will make mobile device malware a topic of concern going forward.

Teaming with a technology partner

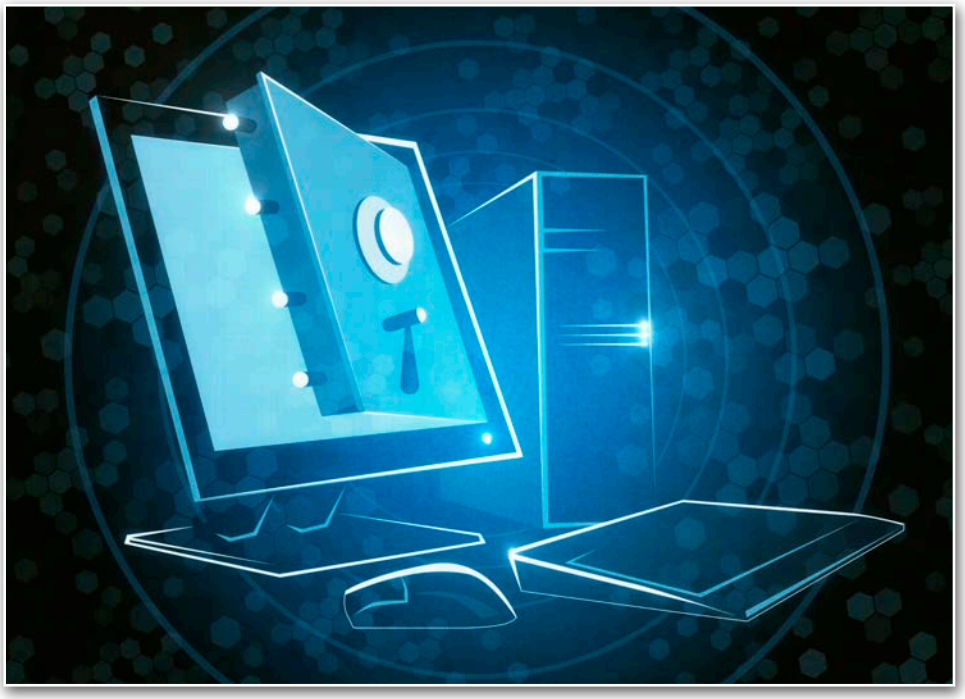
Guarding against such varied threats can be quite challenging. Companies need a variety of security solutions. In many cases, they select point products that are hard to manage and do not provide the needed synergies between various solutions to deliver the high level of protection required today.

An alternative is to team with a company that provides an integrated security solution that protects against malware and web threats, across PCs, tablets, and smartphones. One such vendor is Webroot®.

The Webroot SecureAnywhere™ user protection solution offers flexible protection for PCs, smartphones, tablets, and servers. A key differentiator with SecureAnywhere is that its endpoint protection solution provides instantaneous protection and fast scans without the hassle of time-consuming patches and signature updates.

To address the security challenges of today's increasingly mobile workforce, Webroot SecureAnywhere offers support for a diverse set of mobile platforms. Specifically, the mobile protection solution provides antivirus help to reduce the threat of malware, enables secure web browsing, is capable of blocking calls and SMS threats, and offers lost device protection.

Complementing these solutions, Webroot SecureAnywhere web security service provides flexible and unobtrusive web gateway security that stops online threats before they reach users. The service offers URL filtering, virus and spyware protection, heuristic anti-phishing protection, and web application and content control, as well as blocks malicious JavaScript and Shellcode.



In total, the Webroot SecureAnywhere solutions can help companies combat the changing and new threats that are expected to persist and emerge this year.

For more information on how to protect against ever-evolving malware threats, visit: http://www.webroot.com.

---

[i] http://mashable.com/2014/01/11/neiman-marcus-credit-card-security-breach/

[ii] http://www.pcworld.com/article/2086700/yahoo-malvertising-attack-linked-to-larger-malware-scheme.html

[iii] http://www.esecurityplanet.com/network-security/microsoft-battles-zeroaccess-botnet.html

[iv] http://www.bbc.co.uk/news/technology-25653664

[v] http://www.informationweek.com/7-infosec-predictions-for-2014-good-bad-and-ugly/d/d-id/1113299

[vi] http://www.informationweek.com/attacks/us-bank-hack-attack-techniques-identified/d/d-id/1108089?

[vii] http://threatpost.com/microsoft-zeroaccess-botnet-has-been-abandoned/103273

[viii] http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf

[ix] http://www.networkworld.com/slideshow/91577/9-classic-hacking-phishing-and-social-engineering-lies.html#slide7

[x] http://www.bankinfosecurity.com/target-issues-phishing-warning-a-6319/op-1

[xi] http://securitywatch.pcmag.com/none/319566-phishing-attack-preys-on-jpmorgan-data-breach-fears

[xii] http://www.crn.com/news/security/240162259/adobe-addressing-massive-data-breach-source-code-leak.htm

[xiii] http://www.webpronews.com/new-android-malware-steals-your-money-via-sms-2012-08

[xiv] http://www.forbes.com/sites/timworstall/2013/02/20/yes-apple-really-does-have-a-serious-problem-with-computer-viruses-and-malware/

[xv] http://blog.malwarebytes.org/fraud-scam/2013/07/fbi-ransomware-now-targeting-apples-mac-os-x-users/

[xvi] http://www.computerworld.com/s/article/9240772/Mobile_malware_mainly_aimed_at_Android_devices_jumps_614_in_a_year