Report

McAfee
An Intel Company

McAfee® Labs 2014 Threats Predictions

Table of Contents

1: Mobile malware will be the driver of growth in both technical innovation and the volume of attacks in the overall malware "market" in 2014.

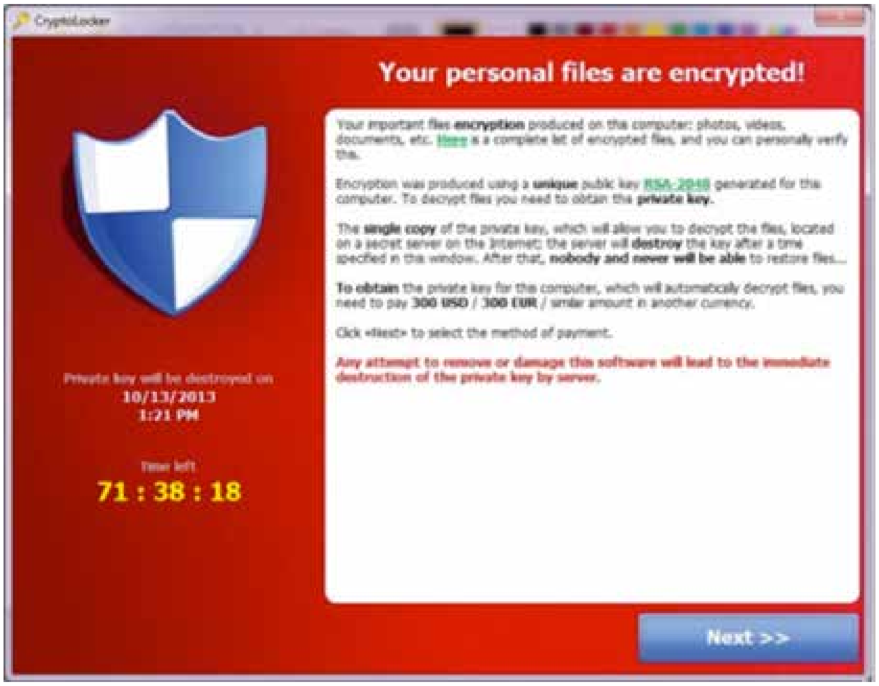
In 2013 the rate of growth in the appearance of new mobile malware, which almost exclusively targets the Android platform, was far greater than the growth rate of new malware targeting PCs. In the last two quarters reported, new PC malware growth was nearly flat, while appearances of new Android samples grew by 33%.

While McAfee Labs expects this trend to continue in 2014, it's not just the growth rate in new mobile attacks that will make news. We also expect to see entirely new types of attacks targeting Android. It is highly likely we will see the first real ransomware attacks aimed at mobile devices that will encrypt key data on the device and hold it for ransom. The information will be released only if the victim delivers either conventional currency or a virtual currency—such as Bitcoin—to the perpetrator. Other new tactics we expect to see in the mobile realm include attacks on vulnerabilities in the near-field communications features now found on many devices and attacks that will corrupt valid apps to expropriate data without being detected.

Attacks on mobile devices will also target enterprise infrastructure. These attacks will be enabled by the now ubiquitous bring-your-own-device phenomenon coupled with the relative immaturity of mobile security technology. Users who unwittingly download malware will in turn introduce malware inside the corporate perimeter that is designed to exfiltrate confidential data. BYOD is not going away, so enterprises must put in place comprehensive device-management policies and solutions to avoid becoming victims.

2: Virtual currencies will fuel increasingly malicious ransomware attacks around the world.

Ransomware attacks that encrypt data on victims' devices have been with us for some time. However, such attacks have historically been vulnerable to law enforcement actions taken against the payment processors used by the perpetrators.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 38 : 18

CryptoLocker dialog box.

Although growth in the use of virtual currencies benefits and promotes economic activity, it has also provided cybercriminals with the perfect unregulated and anonymous payment infrastructure they need to collect money from their victims. We expect attacks such as CryptoLocker to proliferate for as long as such attacks remain (very) profitable. We also expect to see new ransomware attacks aimed at enterprises that will purport to encrypt key corporate data assets.

The good news for individuals and enterprises alike is that though the ransomware payload is unique, the distribution mechanisms (spam, drive-by downloads, and infected apps) are not. Consumers and enterprises that keep their antimalware (both endpoint and network) systems current will be relatively safe from this threat. An effective backup system, be it personal or enterprise deployed, will also isolate victims from most of the negative consequences of ransomware.

3: In the spy vs. spy world of cybercrime and cyberwarfare, criminal gangs and state actors will deploy new stealth attacks that will be harder than ever to identify and stop.

As information security solutions have become increasingly more sophisticated so have the efforts of the cybercriminal community to circumvent those defenses. Attacks that include advanced evasion techniques represent the newest front in the enterprise data security war. A popular evasion technique that will see broad adoption by cybercriminals in 2014 is the use of sandbox-aware attacks that do not fully deploy unless they believe they are running directly on an unprotected device.

Other popular attack technologies that will be further developed and deployed in 2014 include return-oriented programming attacks that cause legitimate applications to behave in malicious ways, self-deleting malware the covers its tracks after subverting a target, and advanced attacks on dedicated industrial control systems that have the potential to damage public and private infrastructure.

Politically motivated attacks will continue to increase, especially around the 2014 Sochi Winter Olympics (in February) and the FIFA World Cup in Brazil (June-July). Hacktivists will also take advantage of these events to promote their ideas.

Enterprise IT organizations will need to respond to this new set of tactics to ensure their defenses are not completely dependent upon security measures that can be readily defeated by global cybercriminal gangs.

4: "Social attacks" will be ubiquitous by the end of 2014.

Social platform attacks are those that leverage the large user bases of Facebook, Twitter, LinkedIn, Instagram, etc. Many of these attacks will mimic the tactics of legacy malware such as Koobface and simply use the social platforms as a delivery mechanism. In 2014, however, we also expect to see attacks that employ the unique features of the social platforms to deliver data about user contacts, location, or business activities that can be used to target advertising or perpetrate virtual or real-world crimes.

One of the most common platform attacks simply steals users' authentication credentials, which are then used to extract personal data from unsuspecting "friends" and colleagues. The Pony botnet,[1] which stole more than two million passwords from users of Facebook, Google, Yahoo, and others, is likely just the tip of the iceberg. Facebook itself estimates that 50–100 million of its Monthly Active User (MAU) accounts are duplicates and that up to 14 million of its registered MAUs are considered "undesirable." According to a recent Stratecast study, 22% of social media users have experienced a security-related incident.[2]

Both public and private enterprises will also leverage social platforms to conduct "reconnaissance attacks" against their competitors and rivals, either directly or through third parties. High-profile leaders in both the public and private sectors were targeted by such attacks in 2013. We can expect the frequency and breadth of these attacks to expand in 2014.

The other form of social attacks we expect to see in volume in 2014 will be "false flag" attacks that dupe users into revealing personal information or authentication credentials. One of the most popular attacks will present an "urgent" request to reset the user's password. It will instead steal the username and password credentials and then use the unsuspecting user's account to collect personal information about the user and contacts.

Preventing both the social platform and false flag attacks will require increased vigilance by individuals and enterprise policies and solutions to ensure employee use of the social media platforms does not result in material data breaches.

5: New PC and server attacks will target vulnerabilities above and below the operating system.

While many cybercriminal syndicates will turn their attention to mobile devices, others will continue to target PC and server platforms. The new attacks we'll see in 2014 will, however, not simply attack the operating system, but will also exploit vulnerabilities both above and below the OS.

Many of the new PC attacks in 2014 will exploit vulnerabilities in HTML5, which allows websites to come alive with interaction, personalization, and rich capabilities for programmers. However, HTML5 also exposes a number of new attack surfaces. Using HTML5, researchers have already shown how to monitor a user's browser history to better target ads. As many HTML5-based applications are designed for mobile devices, we expect to see attacks that will breach the browser sandbox and give attackers direct access to the device and its services. Many enterprises will also build HTML5-based corporate applications. To prevent exfiltration of the data used by these apps, security will need to be built into these new systems from Day One.

Cybercriminals will increasingly target vulnerabilities below the operating system in the storage stack and even the BIOS. In the corporate environment mitigating these low-level attacks will require deploying hardware-assisted security measures that also operate below the operating system level.

6: The evolving threat landscape will dictate adoption of big data security analytics to meet detection and performance requirements.

Historically most information security solutions have depended upon identifying malicious payloads (blacklisting) or tracking known valid applications (whitelisting). The current challenge facing information security practitioners involves identifying and appropriately processing "gray" payloads. Doing so involves applying multiple security technologies in concert with robust threat-reputation services.

Threat-reputation services have already proven their value in detecting malware, malicious websites, spam, and network attacks. In 2014 security vendors will add new threat-reputation services and analytics tools that will enable them and their users to identify stealth and advanced persistent threats faster and more accurately than can be done today. Big Data analytics will allow security practitioners to identify the sophisticated advance evasion technique attacks and advanced persistent threats that can disrupt mission critical business processes.

7: Deployment of cloud-based corporate applications will create new attack surfaces that will be exploited by cybercriminals.

Willie Sutton, who is said to have robbed 100 banks in the early 20th century, is credited with remarking that he robbed banks because "that's where the money is."[3] Cybercriminal gangs of the 21st century will target cloud-based applications and data repositories because that's where the data is, or will be soon enough. This could be through business applications that have not been assessed by IT against corporate security policies. According to a recent report, more than 80% of business users use cloud applications without the knowledge or support of corporate IT.[4]

Although cloud-based applications certainly have compelling functional and economic benefits, they also expose an entirely new family of attack surfaces to perpetrators such as the ubiquitous hypervisors found in all data centers, the multitenant communications infrastructure implicit in cloud services, and management infrastructure used to provision and monitor large-scale cloud services. The issue for enterprise security practitioners is that when a corporate application moves to the cloud, the organization loses visibility of and control over the security profile.

This loss of direct control of the enterprise security perimeter puts tremendous pressure on security leaders and administrators to make sure that the cloud provider's user agreement and operating procedures ensure security measures are both in place and constantly upgraded to meet the evolving threats landscape. Large enterprises may have sufficient leverage to require cloud providers to put security measures in place that are consistent with the enterprise's security posture. Smaller consumers of cloud-based services, however, will not and will need to carefully review the provider's often ambiguous user agreement as it relates to security and data ownership. New cloud services may also expose new attack surfaces until the services reach a level of maturity that includes the instrumentation and countermeasures required to ensure the security of the data they must protect.

About the Authors

This report was prepared and written by Christoph Alme, Cedric Cochin, Geoffrey Cooper, Benjamin Cruz, Toralv Dirro, Paula Greve, Aditya Kapoor, Klaus Majewski, Doug McLean, Igor Muttik, Yukihiro Okutomi, François Paget, Craig Schmugar, Jimmy Shah, Ryan Sherstobitoff, Rick Simon, Dan Sommer, Bing Sun, Ramnath Venugopalan, Adam Wosotowsky, and Chong Xu.

About McAfee Labs

McAfee Labs is the world's leading source for threat research, threat intelligence, and cybersecurity thought leadership. The McAfee Labs team of 500 researchers collects threat data from millions of sensors across key threat vectors—file, web, message, and network. It then performs cross-vector threat correlation analysis and delivers real-time threat intelligence to tightly integrated McAfee endpoint and network security products through its cloud-based McAfee Global Threat Intelligence service. McAfee Labs also develops core threat detection technologies—such as DeepSAFE, application profiling, and graylist management—that are incorporated into the broadest security-product portfolio in the industry.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com

[1] http://blogs.mcafee.com/consumer/pony-botnet-steals-2-million-passwords

[2] Stratecast, "*The Hidden Truth Behind Shadow IT.*" November 2013. http://www.mcafee.com/us/resources/reports/rp-six-trends-security.pdf

[3] Sutton himself claimed he never made the famous statement for which he is credited, instead explaining that he robbed banks because "he enjoyed it."

[4] Stratecast, "*The Hidden Truth Behind Shadow IT.*" November 2013. http://www.mcafee.com/us/resources/reports/rp-six-trends-security.pdf

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com