SOPHOS
Security made simple.

Trends to Watch in 2014

By SophosLabs

Major technology developments over the last year—and a series of revelations about the National Security Agency that shook the international security community—made 2013 an interesting year for trend watchers. In highlighting the past year's security events, we've considered some emerging trends we are likely to see in the coming year.

1. Attacks on corporate and personal data in the cloud

As businesses increasingly rely on various cloud services for managing their customer data, internal project plans and financial assets, we expect to see an emergence of attacks targeting endpoints, mobile devices and credentials as means to gaining access to corporate or personal clouds.

It's hard to predict what form future attacks will take—but we can imagine ransomware taking hostage not just your local documents, but any type of cloud-hosted data. These attacks may not require data encryption and could take the form of blackmail—threats of going public with your confidential data.

Strong password and cloud data access policies are more important than ever. Your security is only as good as your weakest point, in many cases your Windows endpoint and your users' awareness.

2. APTs meet financially motivated malware

We expect the success of advanced persistent threats (APTs) in carrying out attacks for the purposes of industrial espionage will inspire old-school financial malware gangs to adopt their techniques. In fact, we're already seeing exploit techniques borrowed from APT groups being used for malware distribution.

As security vendors make progress with improving layers of defense, OS security and user awareness, cybercriminals are forced to make bigger financial gains from a smaller number victims. New attacks initiated by traditional malware actors may in the future include components and delivery mechanisms purposely built or customized for a narrower target audience. The line marking the difference between APT and traditional malware will continue to blur in 2014.

3. Android malware, increasingly complex, seeks out new targets

In 2013 we saw exponential growth in Android malware, not only in terms of the number of unique families and samples, but also the number of devices affected globally.

While we expect that new security features in the Android platform will make a positive change in infection rates over time, their adoption will be slow, leaving most users exposed to simple social engineering attacks. Cybercriminals will continue to explore new avenues for Android malware monetization. Although their options on this platform are more limited than Windows, mobile devices are an attractive launching pad for attacks aimed at social networks and cloud platforms.

Mitigate this risk by enforcing a BYOD (bring your own device) policy that prevents side-loading of mobile apps from unknown sources and mandates anti-malware protection.

4. Malware diversifies and specializes

The diversity in financially-motivated malware reflects differences between various geographic and economic regions. We already see it through country-specific social engineering techniques, malware monetization options and attack purposes. Malware diversity by targeted audience will likely continue to grow in 2014, especially to differentiate between consumer and business users. We can also expect more specialized attacks in relation to the varying degrees of cyber-defense levels and target value.

5. Personal data danger from mobile apps and social networks

Mobile security in general will continue to be a hot topic in 2014. The continuing adoption of emerging apps for personal and business communication widens the attack surface, particularly for socially engineered scams and data exfiltration attempts. Your address book and your social connections graph is a treasure for cyber-crooks of all sorts, so be mindful of who you entrust to access it and why. Mobile and web applications control for business users will help mitigate this risk.

6. Penetrating defenses

In the never-ending fight between the cybercriminals and security vendors, we expect to see new weapons aimed at the latest cyber-defense mechanisms. Reputation services, cloud security databases, whitelisting and sandboxing layers will be attacked in new and sinister ways. We'll see more malware signed with stolen digital signatures, attempts to poison security data and telemetry analytics, new sandbox detection and bypass techniques, and increased use of legitimate tools for malicious purposes.

7. 64-bit malware

With growing adoption of 64-bit operating systems on PCs, we're expecting a growth of malware that is unable to run on 32-bit PCs.

8. Exploit kits continue to be a primary threat for Windows

Although Microsoft has made technological advances in the Windows operating system that raise the bar for exploit developers, the company is not yet winning the war.

With Windows XP reaching end-of-life after 12 years, it will become a huge target for attackers. Will Windows 7 enjoy such widespread dominance for as many years? How long before we see the majority of endpoints migrating to more recent versions of Windows with improved security features?

Threat delivery that requires user interaction (social engineering) will also continue to be a major infection vector. But malware authors will have to refine their techniques to convince victims to execute the payload, as people become smarter about distinguishing malicious from benign. Mass malware authors will have to make their lures more targeted and more convincing.

9. Undermining hardware, infrastructure and software at the core

The revelations throughout 2013 of government agency spying and backdoors (not only by governments, but also commercial organizations) showed the world that broad-scale compromise of the core infrastructure we all operate on is not only possible, but happening. We'll need to re-evaluate technologies and trusted parties.

The discoveries so far likely only scratch the surface and we can expect to see many more of these stories in 2014. Most enterprises won't have the resources or skills to go digging for backdoors. But it would be wise to closely monitor the work of security researchers and media outlets for new revelations.

10. Hacking everything

We have continued to diversify the devices in our environments, and those devices hold sensitive business data. The security ecosystem simply is not as well developed around such devices as the traditional PC environment.

For those wishing to harm us, embedded devices in our homes, offices and even cities represent interesting attack targets. And new electronic currencies and payment techniques make far more than just the credit card worth considering.

While we don't expect attacks against the "Internet of Things" to become widespread in 2014, we do predict an increase in reported vulnerabilities and proof-of-concept exploits.

Download the Security Threat Report 2014 at

sophos.com/threatreport

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

© Copyright 2013. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

1091-11.13DD.na.simple

SOPHOS