

Sophos Security Threat Report 2013

June 2013

Every year, Sophos Ltd., a major security firm based in the U.K., publishes a threat report that highlights the security threats of the past year and the threats that seem likely in the coming year. In this article, we summarize the findings of the Sophos Security Threat Report 2013.¹

IT security is evolving from a device-centric view to a user-centric view, bringing many new security challenges. Users are fully embracing the power to access data from anywhere. The rapid adoption of bring-your-own-devices (BYOD) is accelerating this trend and is providing new malware attack vectors.

Another trend is the transformation of endpoint devices from homogeneous Windows systems to an environment of diverse systems. Predominant among exploits of such devices is Android malware, a serious and growing threat.

The web remains the dominant source for malware. Social engineering and targeting vulnerabilities in browsers and applications represent the primary attack vectors launched from the web.

A modern security policy must focus on all areas of vulnerability – enforcement of BYOD use policies, data encryption, secure access to corporate networks, content filtering, patch management, and threat and malware protection.

New Platforms and Changing Threats

In 2012, attackers continued to target thousands of badly configured websites and databases to expose passwords and deliver malware. They are now extending their reach to social networks and cloud platforms.

On the positive side, law enforcement authorities achieved significant victories against malware networks and cybercriminals. Those that facilitate cybercrime via botnets and online toolkits can be held as liable as the cybercriminals themselves.

Social Media

Throughout 2012, hundreds of millions of users flocked to social networks; and so did the cybercriminals. Included in the attacks were Facebook, Twitter, and Pinterest. For instance, Twitter direct messages (DMs) from reportedly online friends claimed that a person had been captured on video that had been posted on Facebook. Following the directions to see the video, that person was infected with a backdoor Trojan, opening up his system to malware infection.

¹ [Security Threat Report 2013](http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx), Sophos Ltd.; 2013.
<http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx>

With one billion users, Facebook remains the top target for attackers. Innovations such as Facebook showing a person photos of his friends and asking that person to identify them – something that hackers can't do – may prove helpful.

Cloud Services

Cloud security drew attention in 2012 when Dropbox admitted that user names and passwords stolen from other websites had been used to sign into some of its accounts. Evidently, Dropbox employees had used the same user names and passwords for all of their accounts. When the attackers discovered that these could be used to access Dropbox accounts, Dropbox security was breached.

This followed a 2011 Dropbox security lapse when it accidentally removed all password protection from its accounts for nearly four hours. Dropbox now provides optional two-factor authentication, in which a secret password sent to the user upon logon must be entered in order to access the account.

Dropbox's difficulties have called greater attention to cloud security in general. With cloud security beyond the control of an organization, how should it approach security and compliance? The following steps can help protect data stored in the cloud:

- Use URL filtering to control access to public-cloud storage websites, thus preventing users from browsing to sites that the company has declared off-limits.
- Use application controls to block or allow access to particular applications, either for the entire company or for specific groups.
- Automatically encrypt data before it is uploaded to the cloud from any managed endpoint.

Blackhole: Today's Malware Market Leader

Blackhole is now the world's most notorious malware exploit kit. An exploit kit is a prepackaged software tool that can be used to infect servers with undetected malware. Its authors benefit by delivering payloads for others. Nearly 30% of the threats detected by Sophos have been Blackhole-related.

Blackhole is distributed using a Software-as-a-Service (SaaS) rental model. Rental rates are specified (in Russian) in the kit's accompanying read-me file.

Blackhole works in four stages:

1. Hackers add malicious Java script to legitimate web sites that generate links to the hackers' Blackhole site. When someone visits the legitimate site, their browsers pull down the exploit kit from the Blackhole site.
2. The exploit code first determines the path through which the browser arrived at the Blackhole server. This is used to pay the affiliates who generated the traffic in the first place. It then determines which operating system the browser is using.
3. At this point, Blackhole delivers the payload it's been directed to send. It can actively check the antivirus protection in the browser's system and can erect defenses against it so that the payload remains undetected.
4. Blackhole tracks which exploits worked with which browsers and operating systems. In this way, it can tune future attacks.

Java Attacks Reach Critical Mass

Major new vulnerabilities in Java encouraged many organizations to get rid of Java in their browsers. Oracle quickly released emergency patches, but other vulnerabilities were rapidly found and attacked. The Department of Homeland Security has released an alert recommending that companies disable Java in their browsers.²

Major Organizations Still Leave Users' Passwords Vulnerable

2012 saw many massive password breaches:

- 6.5 million LinkedIn passwords were posted to the Internet.
- eHarmony reported that 1.5 million of its passwords were uploaded to the web.
- Formspring found that 420,000 of its passwords had been posted online.
- Yahoo Voices admitted that 500,000 of its passwords had been stolen.
- The IEEE (Institute of Electrical and Electronic Engineers) left a log file of nearly 100,000 passwords in a world-readable directory.

Password vulnerabilities should be a rarity. At the very least, passwords should be salted and encrypted.

Android: Today's Biggest Target

Androids represent more than a 50% share of the smartphone market. Targets this large are difficult for attackers to resist, especially since the Android source code is open.

Fake Apps

The most common method of attack against Android phones is the installation of fake apps that secretly send expensive messages to premium SMS services.

Another example of a malicious app is the distribution of infected Angry Birds games. This is a Trojan that plays like the real game but gains root access to install malicious code. At this point, it can communicate with a remote website to download and install additional malware.

Eavesdropping

Another class of Android malware eavesdrops on incoming SMS text messages and sends them to another SMS server. This type of attack can compromise two-stage authentication, in which a secret code is sent to a user's mobile phone for him to use when he logs on to a secured service. The secret code can be sent to another site that is maliciously attempting to log on. This can be used, for instance, to access bank accounts for the purpose of stealing funds.

Rooted Devices

It is possible for Android users to "root" their devices so that they have administrative control over their phones. This allows them, for instance, to remove unwanted software and add-ons included by the service provider and to replace them with alternatives of their choice.

However, rooting bypasses the built-in Android security model and invites malware to gain privileges and to avoid detection and removal.

² Department of Homeland Security says, "Disable Java," *Availability Digest*, January 2013.
http://www.availabilitydigest.com/public_articles/0801/disable-java.pdf

Diverse Platforms and Technologies Widen Opportunities for Attack

It used to be that almost everyone ran Windows. Security focused on Windows. Those days are now gone. Far more development currently takes place for the web and mobile platforms. Some examples of 2012 security breaches include:

- Cross-site scripting (XSS) holes in online stores certified as safe by VeriSign, Visa, or MasterCard allowed criminals to steal authentication credentials and customer billing information, thereby putting the customers at risk for identity theft.
- Users received “order verification” emails containing links to legitimate WordPress blogs that had been infected to download malware.
- Hackers have been demonstrating attacks against everything from transit-fare cards to near-field communication-enabled (NFC) smartphones.
- *Ransomware* is a particularly vicious attack. The attacker locks the PC or encrypts its files and demands that payment of a few hundred dollars be made via a cashier’s check or international money order.

OSX and the Mac: More Users, Emerging Risks

Most malware developers have found it to be more profitable to attack Windows and Android than the smaller community of Apple devices. However, the presence of Apple Macs in the workplace is growing; and they are becoming a more attractive target.

Attackers seem to be following their Windows successes in attacking Mac PCs. One way to anticipate the future of Mac malware is to see what is happening now to Windows users.

In 2012, Java vulnerabilities allowed many Macs to be infected. Apple has now by default disabled Java in its operating systems.

Morcut/Crisis

OSX/Morcut-A (aka Crisis) was discovered in 2012. It is designed for spying and monitors virtually every way a user communicates. It is contained in a Java Archive file (JAR) digitally signed by VeriSign. If installed by a user, Morcut runs without administrative authentication. It opens a Mac backdoor to accept malware that steals user data.

Morcut represents a serious threat to corporate security and compliance. It can initiate targeted attacks against individuals in pivotal organizational roles.

Windows Malware Hiding on Macs

Much of the malware found on Macs is Windows malware. Though this is often dismissed by Mac users as not being a threat, this is only true if they are using OSX operating systems. However, if they are running Windows on their Macs, they are exposed to much of this malware.

Authorities Make High-Profile Malware Arrests and Takedowns

2012 saw a marked increase in the success of law enforcement authorities around the world in apprehending cybercriminals.

- Following their 2011 arrests of the notorious LulzSec hackers, U.S. authorities gained extensive cooperation from one of its key members, Hector Xavier Monsegur (Sabu). He reportedly worked months under cover, building cases against those behind hacking attacks on the CIA, Pentagon, the U.S. Senate, and many other prominent organizations. He helped nab Jake Davis in the Shetland Islands, where Davis reportedly held 750,000 stolen passwords.
- U.S. authorities extradited Russian cybercriminal Vladimir Zdrovenin. He is charged with installing key loggers to capture credit-card numbers, which were then used to purchase goods from online stores.
- The mastermind of Bredolab, Georgy Avanesov, was sentenced to four years in jail in Armenia. Bredolab was a botnet that had captured 30 million computers. Avanesov reportedly made 100,000 euros a month renting his botnet to cybercriminals who wanted to spew email and spread malware.
- The FBI arrested 24 cybercriminals from the U.S., U.K., Bosnia, Bulgaria, Norway, and Germany for credit-card fraud.
- Tokyo police arrested six men in connection with an Android app that stole personal data and then demanded a fee to not distribute the data.
- The U.K. obtained stiff sentences for three citizens of Baltic states after their convictions for stealing from online bank accounts in the U.K., the Netherlands, and New Zealand.
- Authorities took down the command and control computers of the huge Grum botnet that was responsible for an estimated 17% of the world's spam.

Growth of Dangerous Targeted Attacks

2012 saw an increase in state-sponsored attacks. The Flame attack infected systems around the world for surveillance purposes.³ The Shamoon Trojan caused significant damage throughout the Middle East's energy sector. It infected some 30,000 computers and took Saudi Arabia's national oil company and Qatar's natural gas firm offline. DDoS (Distributed Denial of Service) attacks were directed against many large U.S. banks.⁴

By their very nature, state-sponsored cyberattacks are difficult to track and prove. More actors appear to be developing the capabilities to launch such attacks. Whatever their source, these attacks have breached some nation's most advanced computer defenses and exposed the vulnerability of their infrastructures.

Polymorphic and Targeted Attacks: The Long Tail

A *polymorphic* virus is able to mutate while keeping its original algorithm intact. The code changes each time it runs, but the functions of the code do not change. This makes a virus very difficult to detect via signatures (code snippets).

The phrase "long tail" is often used in statistics to describe events that do not fall within the conventional statistical distribution but rather occur in ones and twos at the "tail end." Polymorphic malware changes form for every infection. Sophos reports that 75% of the malware reported to it is seen in only one organization. This level of polymorphism is unprecedented.

³ First Stuxnet – Now the Flame Virus, *Availability Digest*, June 2012.

http://www.availabilitydigest.com/public_articles/0706/flame_virus.pdf

⁴ Islamic Hacktivists Attack U.S. Banks, *Availability Digest*, October 2012.

http://www.availabilitydigest.com/public_articles/0710/bank_attacks.pdf

Polymorphic attacks were classically found in Windows systems. However, in 2012, it appeared for the first time in Android malware. These attacks are often used to target specific classes of users, such as financial decision makers. By limiting the scope of the attacks, the cybercriminal minimizes the spread of his virus and minimizes its chance of detection.

Summary

Sophos provides full security protection across an entire enterprise, from fixed and mobile endpoints to applications and data. It focuses on eliminating complexity from security procedures.

The Sophos Security Threat Report 2013 contains much more information than is discussed in this relatively brief summary. Refer to that report to gain additional information and insight into the topics discussed herein.