QUARTERLY REPORT PANDALABS

JULY-SEPTEMBER 2013

PANDA SECURITY

01| Introduction

The third quarter of 2013 was one of the most active ever with regard to malware creation. In fact, the number of new malware samples in circulation in just the first nine months of 2013 has already met the 2012 figure for the entire year

One of the highlights of the quarter was the appearance of **CryptoLocker**, a new ransomware threat that hijacks users' documents and demands a ransom for them.

The report takes a look at the activities of the hacking collective "Syrian Electronic Army", whose members managed to hack the personal email accounts of a number of White House employees.

In the mobile arena, we analyze some of the attacks launched on the iPhone, such as the one that allows attackers to infect Apple devices through a malicious charger. Meanwhile, Android continues to be the primary target for cyber-attacks, despite claims by some Google top executives that Android is the most secure platform on the market.

Finally, we discuss some of the major stories concerning cyber-war and cyber-espionage, focusing our attention on the latest revelations concerning the NSA and the cyber-espionage operations conducted by this U.S. intelligence agency.

02| Malware Figures in Q3 2013

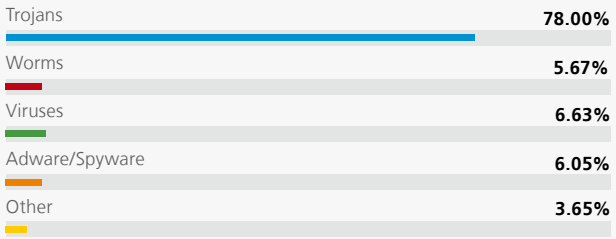
Malware creation hit a new record high in the third quarter of 2013, as shown by the fact that PandaLabs cataloged nearly 10 million new malware strains from July to September. In fact, the number of new malware samples in circulation in just the first nine months of 2013 has already met the 2012 figure for the entire year.

Trojans were once again the most popular type of malware, accounting for 76.85 percent of all new threats created. This figure is very similar to the previous quarter.

New malware strains in Q3 2013, by type

Trojans	**76.85%**
Worms	**13.12%**
Viruses	**9.23%**
Adware /Spyware	**0.57%**
Other	**0.23%**

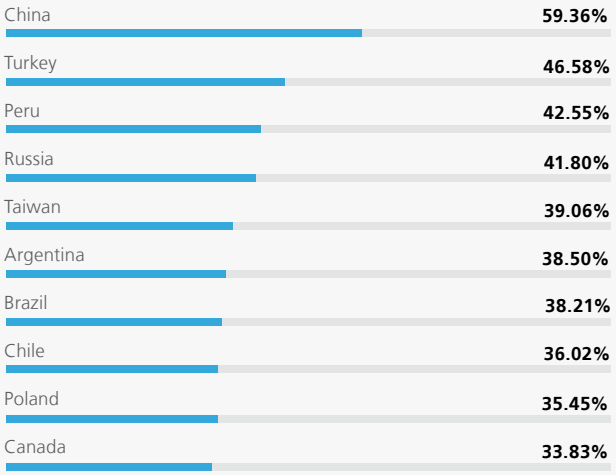
Malware infections by type in Q3 2013



Trojans occupied the first position, and continued to be the weapon of choice for malware writers. It is worth noting the slight increase in the number of adware and spyware infections, although, at 6.05 percent, they are still well below Trojans (78 percent of all infections).

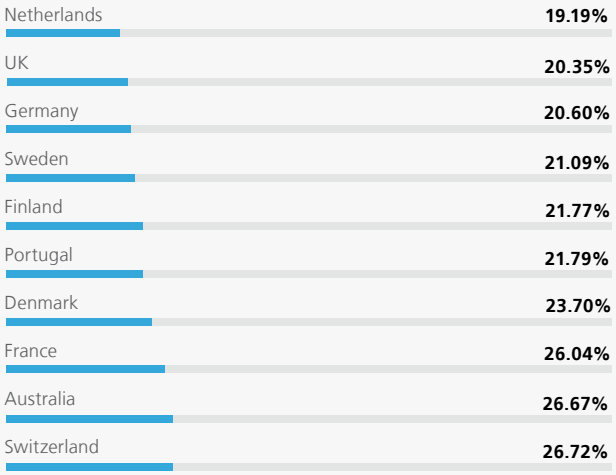
We will now look at how infections were distributed geographically. **In the third quarter of 2013, the global infection ratio was 31.88 percent,** almost a full point lower than in the second quarter. As for the data for individual countries, China once again topped the table (59.36 percent of infected computers), followed by Turkey (46.58 percent) and Peru (42.55 percent).

Most malware-infected countries



In this "Top 10", although there are countries from many regions, there is a strong presence of Latin American countries. **China set a new record high with a malware infection rate well beyond 50 percent.**

Least malware-infected countries



Europe continued to have the lowest infection rates. Netherlands (19.19 percent), UK (20.35 percent) and Germany (20.60 percent) were the countries with the fewest infections. **The only non-European country in the Top Ten was Australia, in ninth place with 26.67 percent.** Other countries outside this Top 10 but with infection rates below the average were: Japan (26.84 percent), Hungary (27.56 percent), Venezuela (27.82 percent), Colombia (29.14 percent), Belgium (29.14 percent), Italy (30.16 percent), USA (30.58 percent), Mexico (31.49 percent) and Spain (31.74 percent).

03| The Quarter at a Glance

Cyber-criminals often try to exploit newsworthy events or notable dates to try to spread malware to new victims.

CYBER-CRIME

This quarter, the hacking collective **Syrian Electronic Army** continued launching cyber-attacks against different institutions worldwide. In July, they used phishing techniques to hack into the personal Gmail accounts of at least three **White House** social media staffers. Then, they used the compromised accounts to send phishing emails to other White House accounts.

In August, The **Washington Post** reported being victims of a hacking attack, with readers of certain articles being redirected to the site of the Syrian Electronic Army.

> Hacking group **Syrian Electronic Army** was particularly active this quarter, with victims including The New York Times, Twitter and even some White House employees

A few weeks later it was The **New York Times** and social networking site **Twitter** that fell victim to the hacking group. In this case the criminals didn't use a hacking attack, but a technique called DNS cache poisoning that redirected users who typed the Web address of these two organizations to another site. However, users who tried to access these Web pages using their IP addresses, could do so without problems.

DNS cache poisoning attacks are nothing new, although they have become more common in recent months. Several large

websites hosted in Malaysia fell victim to this type of attack, including the local websites of companies such as Google, Microsoft or Kaspersky.

DNS cache poisoning attacks have been on the rise over the last few months

The **"Police Virus"** showed no sign of receding and continued wreaking havoc among users through new variants. One of them was especially noteworthy for the high 'fine' it demanded from users ($/€300 instead of the usual $/€100).

The Technological Investigation Brigade of Spain's National Police arrested in Madrid two Ukrainian men accused of money laundering for one of the gangs behind the Police Virus attacks. The materials seized from these cyber-criminals included bitcoins, making this the second time only that a law enforcement agency seizes this popular online virtual currency.

In any event, the highlight of the quarter was the appearance of **CryptoLocker.** This is a new Trojan that uses ransomware techniques, hijacking users' documents and asking them to pay a ransom for them.

CryptoLocker is a new family of malware that hijacks users' documents and demands a ransom for them

Even though this type of attack is nothing new, this new ransonware has some unique characteristics that have made it a success for its creators:

- Instead of encrypting every file it finds, it focuses on those most valuable to users: photos, videos, text documents, etc.
- It not only encrypts files on the computer's hard disk, but also on every network drive the infected user has access to.
- It uses asymmetric encryption, which makes decryption impossible without having access to the actual key used by the cyber-criminal to encrypt the files. Neither is it possible to decrypt the files using any kind of forensic tools.
- The message displayed asking users to make the payment includes a countdown timer, pressing the victim into making a decision: pay the ransom or lose access to their files forever.

In the fight against cyber-crime, the European Parliament passed a bill imposing harder sentences on cyber-criminal activities. For example, simply creating or using a botnet may be punished with a minimum of three years in prison, excluding other crimes that may have been committed using the botnet.

SOCIAL NETWORKS

In the social media arena, Facebook announced it had finished migrating its users to safe browsing, with all active users of the most popular social networking site now accessing it over HTTPS. This means that all traffic between users' devices and Facebook is now encrypted to prevent data theft.

Facebook users now connect to the social media site via HTTPS

MOBILE PHONE MALWARE

Despite **Android** continues its reign as the most popular smartphone platform and has become a regular presence in this section, this time we must refer to its fiercest competitor: iOS, Apple's operating system for smartphones (iPhone) and tablets (iPad). In July, a group of researchers from Georgia Tech Information Security Center (GTISC) revealed how they were able to hack into an iPhone using a malicious charger.

Fake chargers can infect iPhone devices with malware

In September, **Apple** launched the new iOS 7 which, in addition to an all-new design and all-new features, included fixes to 80 different vulnerabilities, including the fake USB charger flaw. However, just a few hours after its release, new security flaws had been reported in iOS 7. One of them, for example, allowed attackers to bypass iOS 7's lock screen.

Android continued suffering most attacks, despite the words from Google's Android security chief Adrian Ludwig, who reported that "less than an estimated 0.001% of app installations on Android are able to evade the system's multi-layered defenses and cause harm to users." Statistics may indicate otherwise, but there is no denying that Android is the mobile platform most targeted by cyber-criminals.

Android continues to be most targeted by hackers

Android is in the crosshairs of cyber-criminals for a simple reason: it is extremely popular. That's why hackers keep looking for new ways to attack the platform and infect users. This quarter we saw a new form of attack that involves modifying a legitimate APK file (Android app installer) to install any type of malicious code in an undetected way.

CYBER-WAR

The cyber-war arena has been dominated by yet more news regarding the U.S. National Security Agency, aka **NSA**. At the beginning of 2013, Edward Snowden, who worked for the NSA as a system administrator, ended his contract with the agency

taking with him a significant amount of documentation he later disclosed to various media publications. This revealed the existence of a clandestine program called PRISM and operated by the NSA, which allowed the agency to obtain user data from major U.S. companies such as Microsoft, Google, Apple, Facebook, etc.

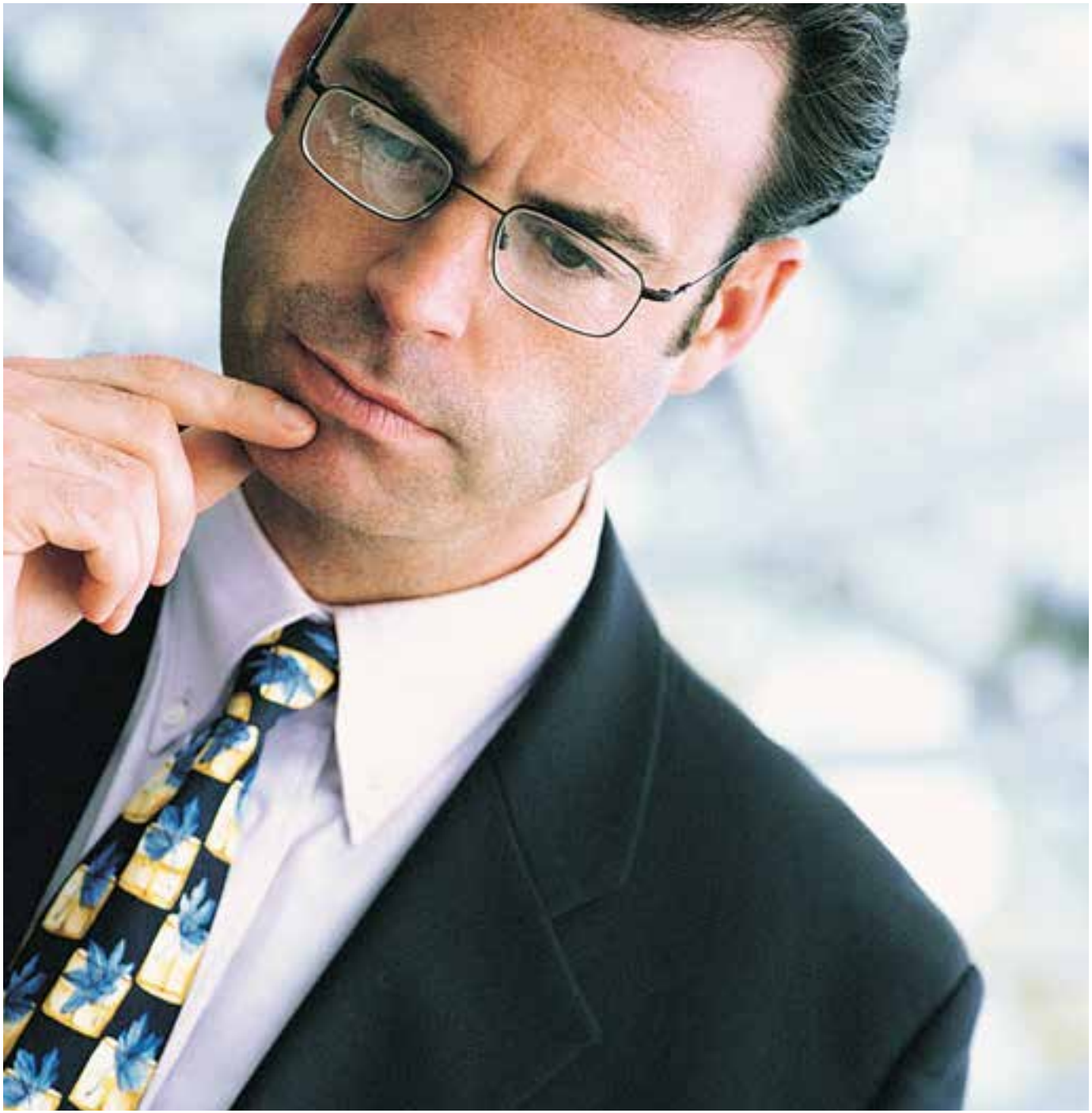
New documents obtained from Edward Snowden tied the **NSA** to major cyber-espionage operations

Despite the first news about the case were truly scandalous, these were quickly followed by new findings that limited the scope of the leaked documentation. For example, the NSA could not access citizens' call or email information without warrants. In any event, recent revelations have confirmed the seriousness of the violations.

After the repercussions of the NSA spying scandal, major communication companies have asked the U.S. government for greater transparency in surveillance programs. More specifically, they are asking the government to allow them to make public the data request received from the NSA, as well as additional information in relation to these requests.

The **NSA** inserted a backdoor in a popular pseudo-random number generator endorsed by important official institutions

According to some of the news articles appeared during the last three months, the NSA put a backdoor in Dual EC_DRBG, a pseudo-random number generator algorithm certified by the most important international bodies. In fact, some days after this information, computer security company RSA issued an advisory telling its customers to stop using the algorithm, which was included by default in two of its products.



04| Conclusion

The third quarter of 2013 closed with malware creation at record levels, as shown by the fact that malware figures for the first nine months have already reached the 2012 numbers for the entire year.

DNS cache poisoning attacks have been on the rise and may become one of the prevalent trends for the next few months.

Regarding cyber-espionage, the United States has taken the spotlight off China due to the espionage scandal uncovered by Edward Snowden, and everything seems to indicate that there will be more revelations about other NSA surveillance programs to indiscriminately spy on users, companies and governments around the world.

05| About PandaLabs

PandaLabs is Panda Security's anti-malware laboratory, and represents the company's nerve center for malware treatment.

PandaLabs creates continually and in real-time the counter-measures necessary to protect Panda Security clients from all kind of malicious code on a global level.

PandaLabs is in this way responsible for carrying out detailed scans of all kinds of malware, with the aim of improving the protection offered to Panda Security clients, as well as keeping the general public informed.

Likewise, PandaLabs maintains a constant state of vigilance, closely observing the various trends and developments taking place in the field of malware and security. Its aim is to warn and provide alerts on imminent dangers and threats, as well as to forecast future events.

For further information about the last threats discovered, consult the PandaLabs blog at:
http://pandalabs.pandasecurity.com/

06| Follow us on the web

facebook
https://www.facebook.com/PandaUSA

twitter
https://twitter.com/#!/Panda_Security

google+
http://www.gplus.to/pandasecurity

youtube
http://www.youtube.com/pandasecurity1

linkedin
http://www.linkedin.com/company/panda-security