Quarterly Report PandaLabs

April - June **2011**

01| Introduction

The title of Guns N' Roses hit "Welcome to the Jungle" perfectly sums up the events that have taken place in the computer security world during Q2 2011. The number of attacks suffered by businesses and large organizations has set alarm bells ringing as systems and companies that until now were considered 'hack-proof' have fallen victim to cyber-crime.

Even though the number one culprit behind these attacks is and will always be the criminal that carries them out, it is true that the companies or institutions that are supposed to store and protect users' information but leave the door open or implement inadequate security measures are guilty of gross negligence.

However, not all attacks have been fully financially motivated; we have also witnessed cyber-espionage incidents as that on the International Monetary Fund (IMF) and sheer vandalism by the Anonymous group and its spin-off, the hacker group "LulzSec", which have affected private companies and governmental institutions like the US Senate or even the CIA.

02| Q2 at a glance

Cyber-activism, cyber-war, cyber-crime… These words are on everyone's lips these days. In fact, they have had specific sections dedicated to them in our latest quarterly reports. Normally it is quite easy to classify attacks and security incidents according to their goal: It is quite clear that to sabotage a nuclear facility in Iran is an act of cyber-war, or to steal personal data from a company is a cyber-crime. Also, cyber-activism as such is not something bad, despite the bad name given to it by the illegal or unethical activities committed in its name.

However, this quarter we have seen how the dividing line between hacktivism and criminality is getting more and more blurry, with the consequences this might have.

From 'hacktivism' to 'stupidism'

It seems that the only way the Anonymous group has to protest is by committing illegal acts. However, if the members of the group were smart enough, they would realize that their constant breaking of the law undermines the legitimacy of their protests. Over the last few months they have launched attacks on Sony and the websites of the U.S. Chamber of Commerce, Spain's national police force, several governmental institutions, etc.

Moreover, they claim that their activities are 'peaceful protests', despite their actions are purposefully enacted to cause economic loss and completely illegal. They say they represent everyone's 'best interest' but are not brave enough to appear publicly, hiding instead behind their pseudonyms.

Well, if you hadn't already had enough of Anonymous, a new hacker collective called LulzSec has emerged, whose claimed main motivation is simply 'to have fun by causing mayhem'. In my opinion, if you took the most irresponsible and brainless members of Anonymous and put them all together, they would be considered the most refined gentlemen compared to LulzSec.

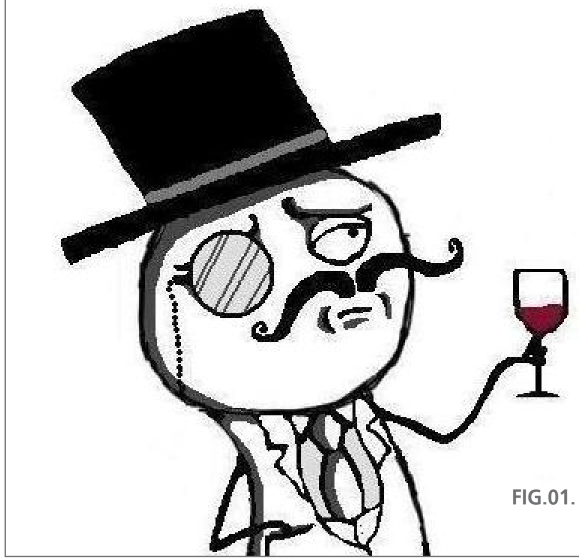
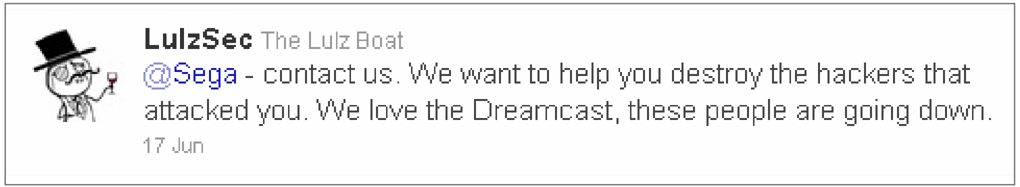


FIG.01. *LULZSEC'S TWITTER PROFILE PICTURE.*

LulzSec specializes in stealing and posting information from companies with poor security (PBS, Fox, etc.) as well as carrying out denial of service attacks (against the CIA website, for example). And if all this was not enough, they have also released a full list of user data they had previously stolen such as email addresses, passwords, etc. which has led to account hijacking and other forms of identity theft.

At the end of June, LulzSec teamed up with Anonymous for "Operation: Anti-Security", encouraging supporters to hack into, steal and publish classified government information from any source.

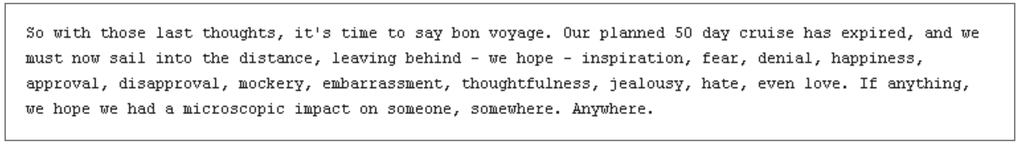
However, Lulzsec's lack of coherence is exemplified by the following story: Back in June, hackers stole the personal data of some 1.29 million customers of the Japanese game maker Sega. Lulzsec was initially linked to the attack, but soon afterwards they released a statement claiming they had nothing to do with it and offering to help Sega find the actual culprit. It seems pretty clear that Lulzsec thinks it is perfectly OK to commit a crime as long as they are the perpetrators, otherwise it is clearly wrong and the "competitor" must be destroyed.



LulzSec The Lulz Boat
@Sega - contact us. We want to help you destroy the hackers that attacked you. We love the Dreamcast, these people are going down.
17 Jun

FIG.02. *LULZSEC'S TWITTER MESSAGE TO SEGA.*

LulzSec continued its hacking escapades, which reached their climax with "Operation Chinga la Migra" in which they stole and released a torrent of information belonging to Arizona law enforcement. The information included hundreds of classified documents and all kinds of personal data about hundreds of Arizona border patrol officials.

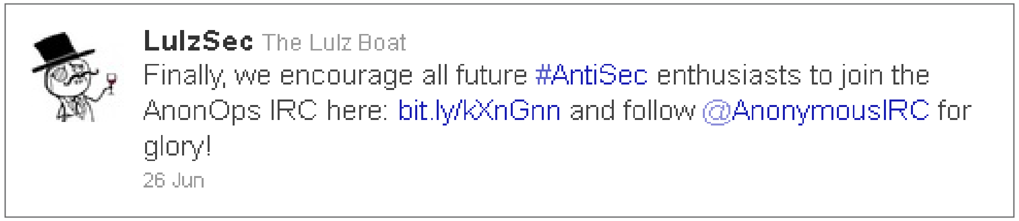


So with those last thoughts, it's time to say bon voyage. Our planned 50 day cruise has expired, and we must now sail into the distance, leaving behind - we hope - inspiration, fear, denial, happiness, approval, disapproval, mockery, embarrassment, thoughtfulness, jealousy, hate, even love. If anything, we hope we had a microscopic impact on someone, somewhere. Anywhere.

FIG.03. *LAST PRESS RELEASED FROM LULZSEC.*

Meanwhile, a growing assemblage of rival hackers had been working to unmask LulzSec members. It is believed that the information gathered by these groups helped in the arrest of Ryan Cleary, 19, in Britain. Cleary ran one of the IRC servers used by LulzSec.

On June 26, LulzSec released a statement on Twitter announcing the end of their activities. Nevertheless, they urged hackers to carry on with operation Anti-Security (#Antisec) and join the Anonymous IRC channel.



LulzSec The Lulz Boat
Finally, we encourage all future #AntiSec enthusiasts to join the AnonOps IRC here: bit.ly/kXnGnn and follow @AnonymousIRC for glory!
26 Jun

FIG.04. *LULZSEC LAST WISH: SUPPORTING ANONYMOUS.*

But not everything is going to be bad news: a number of suspected members of the Anonymous group were arrested during the second quarter of 2011: three in Spain and 32 in Turkey.

A disastrous quarter

Besides the deplorable events involving Anonymous and LulzSec, this has certainly been one of the most negative quarters ever judging from the number of cyber-attacks launched. RSA, the security division of EMC Corporation, announced in mid-March that they had suffered a breach on their network systems that had exposed proprietary information about their two-factor hardware-based authentication system "SecurID".

FIG.05. *SECURID TWO-FACTOR HARDWARE-BASED AUTHENTICATION SYSTEM.*

In May, Lockheed Martin, the largest provider of IT services to the U.S. government and military, suffered a network intrusion stemming from data stolen pertaining to RSA. It seems that the cyber-thieves managed to compromise the algorithm used by RSA to generate security keys. RSA will have to replace the SecurID tokens of more than 40 million customers around the world, including some of the world's biggest companies.

The Norwegian military stated in May 19 that it had been the victim of a serious cyber-attack that took place at the end of March. The attack happened when 100 senior military personnel received an email in Norwegian with an attachment. The attached file was in reality a Trojan designed to steal information. At least one person opened the attachment, but the attack was a failure and no data was lost.

In June, the International Monetary Fund said it had been targeted by a sophisticated cyber-attack for months, even though the organization has made no public statement about the motivation behind it. The nature of the information stored by the institution would seem to indicate that this was a targeted attack, however, we cannot rule out the possibility that it was just a common case of cyber-crime.

The website of the European Space Agency was also hacked into and a lot of information was stolen and made public. This data included user names, FTP accounts and even FTP login details stored… in plain text files!

Also in May Citigroup revealed that information for more than 360,000 U.S. credit card accounts had been compromised by a website hack. The worst thing about this attack is the fact that the data thieves did not even have to hack a server, but were able to penetrate the bank's defenses and leapfrog between the accounts of different Citi customers simply by inserting various numbers into a string of text located in the browser's address bar.

The Japanese video game firm Sega also fell victim to a cyber-attack. The company confirmed that information for 1.3 millions of its customers was stolen from its database. Names, birth dates, email addresses and even encrypted passwords for Sega Pass online network were taken. The fact that the passwords were encrypted should minimize the impact of the hacking incident, but only if strong encryption was used, which is not always the case.

Sonygate

Perhaps the most infamous attack occurred this quarter was the one suffered by Sony. Everything started with the theft of data from their PlayStation Network (PSN), affecting 77 million users worldwide. Not only was this the biggest data theft ever, but the situation was also particularly badly handled by the company. They hid the problem for days, and when they finally made it public they simply said that there was evidence that some user data could have been compromised, even though they knew perfectly well that the situation was far more serious than that.

To make things worse, the stolen data was especially sensible, including users' names, billing addresses, email addresses, PSN IDs, passwords (apparently unencrypted), birthdates, purchase history, credit card numbers (from approximately 10% of users), credit card expiry dates, etc.

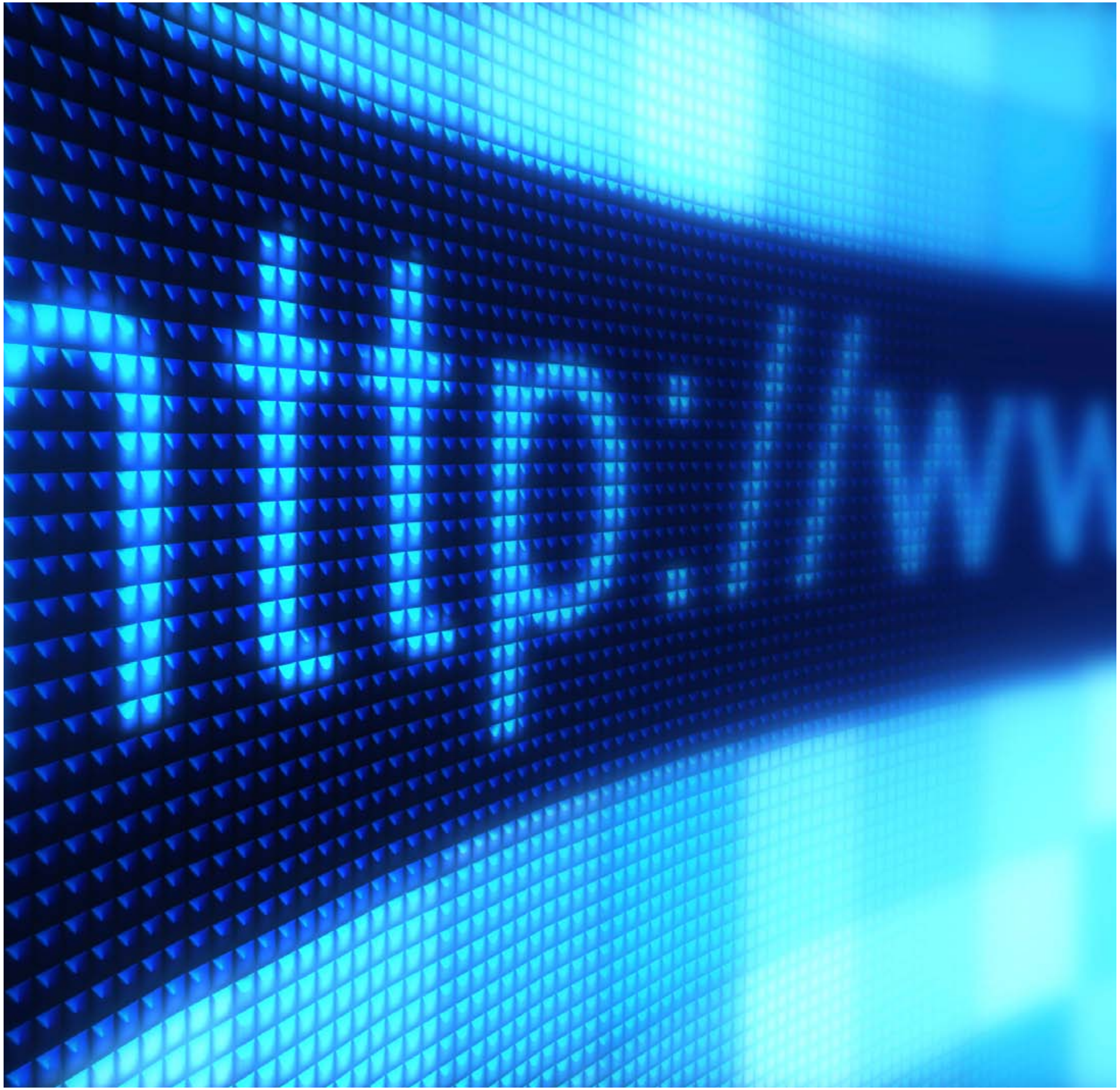
If this was not sufficient, Sony Online Entertainment was subject to another attack a few days later, a data theft that affected another 24 million users.

Malware

In addition to all the attacks we have covered so far, this second quarter has seen a surge of "traditional" online attacks aimed at home users. There haven't been any major changes with regard to past trends although we have seen the first large-scale attack on Mac using rogueware or fake antivirus software. Despite thousands of users being affected by the fake antivirus program (called MacDefender), Apple very much tried to bury their head in the sand, denying that any attack ever took place. A few days later, however, they acknowledged it and released a "security update" to protect against the malware. But mere hours after the update, cyber-criminals had already released new variants of the malware, like MacShield, that easily bypassed Apple's security patch. This was rather logical if you consider the fact that it was based on 20-year-old technologies, fully obsolete and totally useless unless combined with modern techniques like behavior analysis.

There haven't been any major or ground-breaking changes in the cell phone sector, that is, the number of attacks on Google's Android platforms has continued to rise. They are still no way near to the fake antivirus attacks launched on Apple, but if things don't change this might become a major problem in the near future.

Finally, if there is one thing that social networks prove it is that users are very much capable of making the same mistakes over and over again. Malware campaigns fooling Facebook users into believing they will discover who is secretly viewing their profile are still hugely successful and infect thousands of computer users around the world.



03| Quarterly figures

In this section we'll take a look at the Q2 malware statistics. Overall, malware keeps spreading massively as shown by the staggering 42 new malware strains created every minute. There are no major changes in the type of malware being developed, as Trojans are still the most predominant malware family (68.34% of all samples in circulation). The reason for this is, as previously explained, the fact that Trojans are the ideal tool for cyber-crooks to steal user data, providing the largest financial return to threat creators.

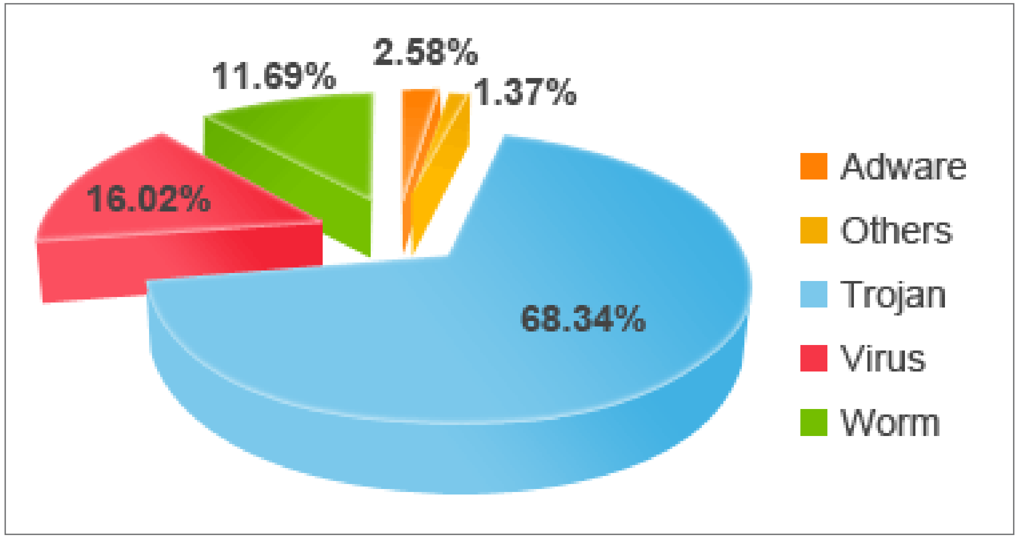


FIG.06. *NEW MALWARE SAMPLES DETECTED AT PANDALABS.*

Trojans are followed by traditional viruses (16.02%). Even though viruses may seem like a thing of the past, their recent revival stems from the appearance of a few but highly active families with new variants aimed at infecting a large number of users. But… why are these new strains so active if malware writers are mostly interested in stealing information? The reason is simple: These new viruses have Trojan features and are capable of stealing user information, like Sality or Viking.

Worms occupied the third position, followed by adware (a category that includes fake antivirus programs or rogueware). Rogueware is a form of computer malware that deceives or misleads users into paying for the fake or simulated removal of malware, or that installs other malware. Back in 2009 we conducted a study that revealed that cyber-thieves could make over 400 million dollars every year selling fake antivirus software.

In any event, these figures reflect the number and type of malware strains created, but not the distribution of malware infections. The following graph shows the types of malware that have infected systems in Q2 2011 according to the data gathered by our free antivirus scanner Panda ActiveScan:

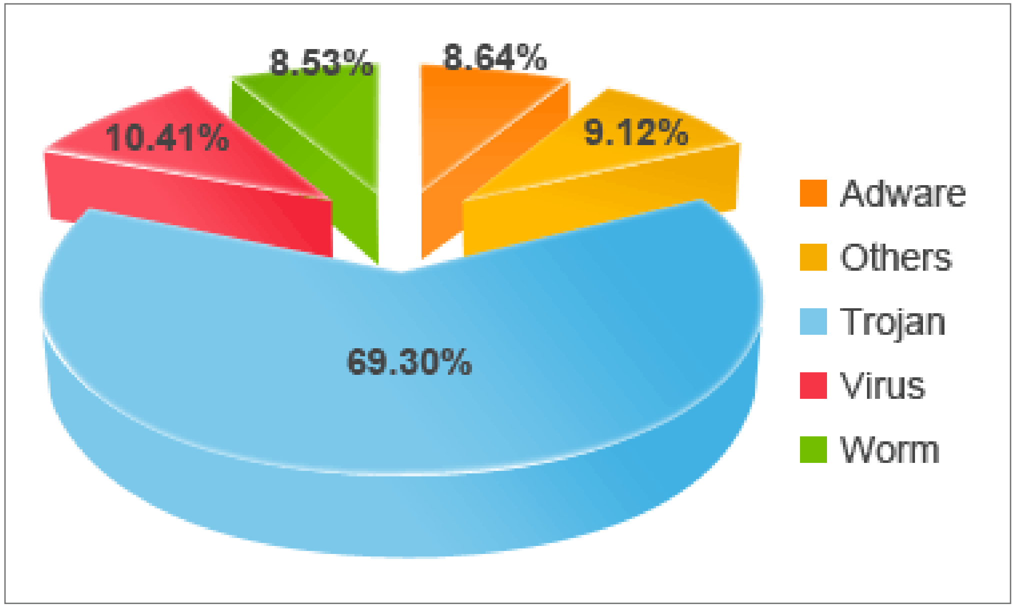


FIG.07. *INFECTIONS PER TYPE OF MALWARE.*

As seen in the graphs, there are major differences between the malware specimens created in the second quarter of 2011 and the infection distribution. In principle, logic would dictate that viruses and worms should account for a larger percentage of infections as they share a trait not found in other malware species: they can replicate themselves and therefore can spread much more than Trojans or rogueware. But then, why is that not the case? Well, basically because infections are caused by cyber-crooks and it all depends on what their objectives are and what profit they can get out of their creations. And so, we see that Trojans are causing most infections by far, whereas viruses and worms see their 'market share' shrinking compared to the other malware strains collected by PandaLabs during this period.

However, if there is one malware category that really catches our attention, that is adware, as only 2.58% of the new malware specimens account for 8.64% of all infections. This shows the interest and the amount of work put in by cyber-crooks to 'promote' these tools. From a pure cost-benefit perspective this is quite easy to understand, as all they have to do is spread their fake antivirus software and wait for users to start sending them their money.

As can be seen from the graph below, the Top 10 most prevalent malware account for 52.03% of all infections. However, this can be a bit misleading as many of the entries on the Top 10 list are generic detections (detected by Collective Intelligence) that include several malware families. The details are as follows:

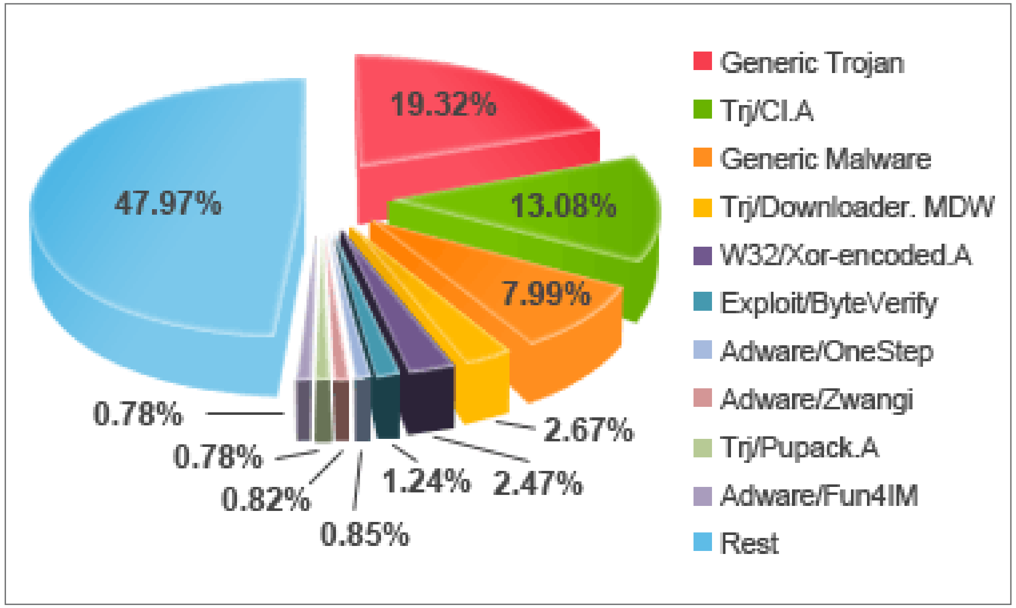


FIG.08. *MALWARE FAMILIES.*

Now we'll take a look at the infection rankings by country according to Panda ActiveScan. This data may be a bit controversial as some people claim that ActiveScan (an on-demand online virus scanner) is only used by people who suspect their computer is already infected with a virus and are looking for a second opinion. Even though this is true, it is not the only aspect to bear in mind. For example, the vast majority of ActiveScan users already have an up-to-date antivirus installed on their computers, which reduces the number of infections detected compared to unprotected PCs.

The graph below shows the 20 countries with the highest rates of malware infection in Q2 2011:

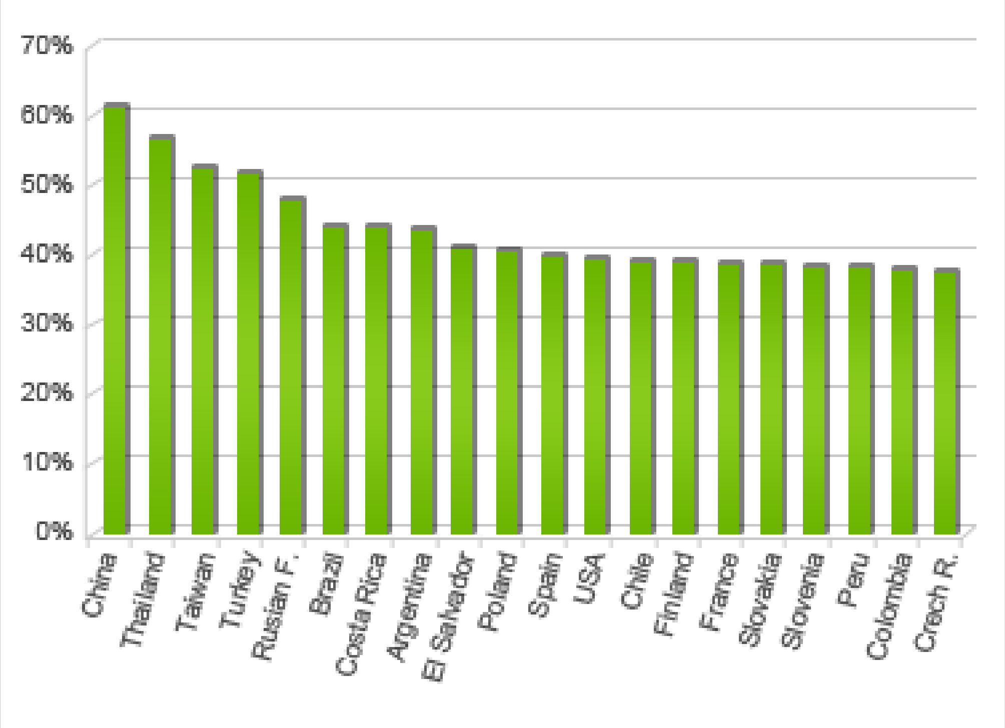


FIG.09. *INFECTION RATE PER COUNTRY – TOP 20.*

As you can see, the top three spots are occupied by Asian countries: China (61.33% of all computers infected), Thailand (56.67%) and Taiwan (52.92%). Turkey also exceeds 50% of infections (51.75%).

The global average was 39.79%. Sweden was the country with the lowest incidence of malware infections (27.29%), followed by Switzerland (29.02%), Norway (29.13%) and Germany (30.96%), all of them European countries. The graph below shows the countries with the lowest infection rates:

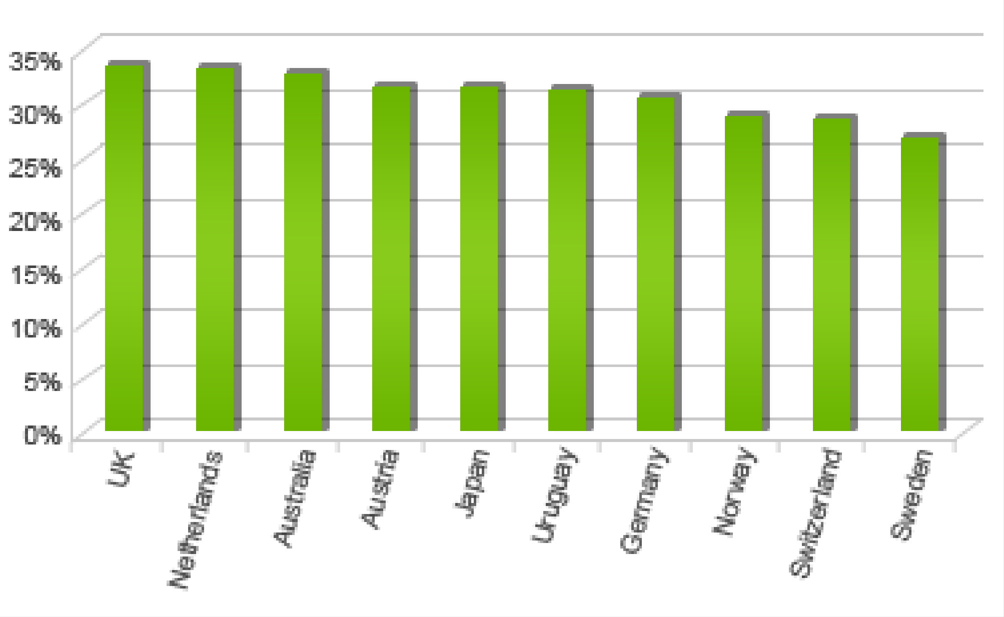


FIG.10. *COUNTRIES WITH THE LOWEST INFECTION RATE IN THE WORLD.*

04| Vulnerabilities

Just like last quarter, this section is full of interesting and unusual facts and trivia regarding computer vulnerabilities.

Nevertheless, for more detailed information on the security patches released by major vendors like Microsoft, Adobe and Oracle, please visit:

- http://www.microsoft.com/technet/security/current.aspx
- http://www.adobe.com/support/security/
- http://www.oracle.com/technetwork/topics/security/alerts-086861.html#SecurityAlerts

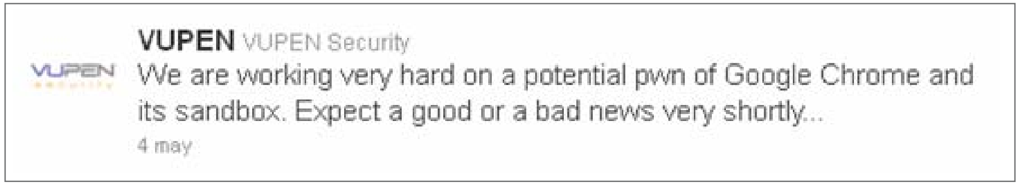
And, for more information about the vulnerabilities uncovered in these and other products, please go to:

- http://cve.mitre.org/cve/

We begin this section with a brief reminder of the Pwn2Own competition organized last March by the ZeroDay Initiative[1] team at security researchers TippingPoint. As mentioned in our first quarter report, VUPEN researches took advantage of a security flaw in the latest version of Safari's WebKit[2] engine to bypass the ASLR[3] and DEP[4] protection in the 64-bit version of a fully patched MacOSX Snow Leopard and win the prize. Similarly, Stephen Fewer, a security researcher at Harmony Security, prepared an advanced exploit that took advantage of three vulnerabilities to compromise Internet Explorer 8 (32-bit) running on a Windows 7 computer with Service Pack 1..

Google's Chrome was the only browser that hackers did not break, possibly because just a few days before the competition, Google made a series of last-minute fixes to it that discouraged researchers from even trying to hack it.

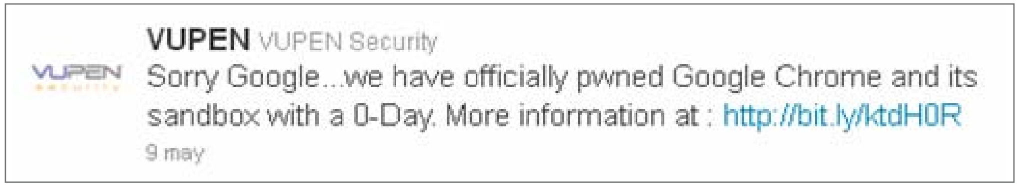
According to the results of the contest, Google Chrome would seem like the best option to surf the Web safely. However, reality shows that this browser can be compromised just like the others. Actually, two months after the Pwn2Own contest was over, on May 5, French security company VUPEN posted a message on Twitter (@VUPEN) saying that they were working hard on a potential vulnerability in the Google browser.



VUPEN VUPEN Security
We are working very hard on a potential pwn of Google Chrome and its sandbox. Expect a good or a bad news very shortly...
4 may

FIG.11. ***VUPEN'S TWITTER MESSAGE.***

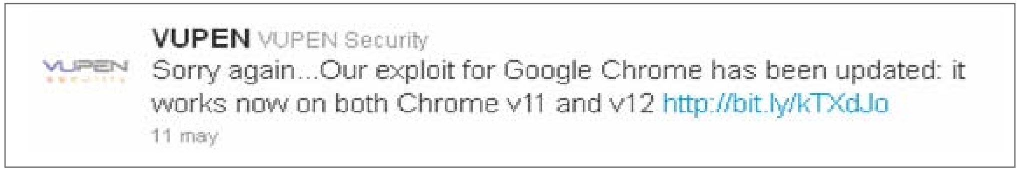
No sooner said that done. Five days later, VUPEN announced that its researchers had taken advantage of an exploit that bypassed Chrome's (v11) sandbox. The Twitter message included a link with more information and a video showing their method[5].



VUPEN VUPEN Security
Sorry Google...we have officially pwned Google Chrome and its sandbox with a 0-Day. More information at : http://bit.ly/ktdH0R
9 may

FIG.12. ***VUPEN'S TWITTER MESSAGE ANNOUNCING THEY HAD SUBVERTED GOOGLE CHROME'S SANDBOX.***

It seemed that Google Chrome 12 was not affected by this exploit but, two days later, on May 11, VUPEN announced that this version was also vulnerable to the sandbox escaping attack.

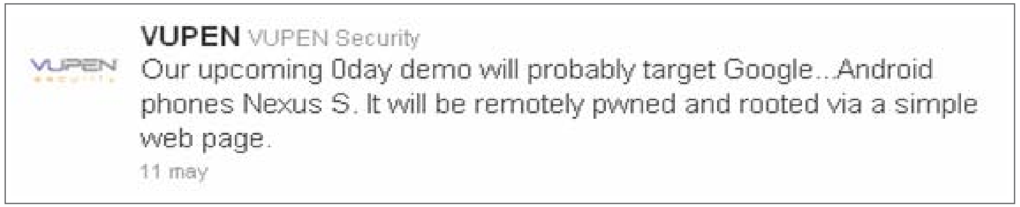


VUPEN VUPEN Security
Sorry again...Our exploit for Google Chrome has been updated: it works now on both Chrome v11 and v12 http://bit.ly/kTXdJo
11 may

FIG.13. ***VUPEN'S TWITTER MESSAGE ANNOUNCING THAT BOTH CHROME 11 AND 12 WERE AFFECTED BY THEIR EXPLOIT.***

On their blog, VUPEN explained that the exploit they had developed was one of the most sophisticated codes they had ever seen and created. The exploit could bypass all security features including ASLR/DEP/Sandbox on all 32-bit and 64-bit Windows systems. The exploit was completely silent, that is, there were no external signs of the attack. VUPEN did not make the exact details of the hack public, saying only that it would relay the details to government agencies on its customer list.

It seems that the company researches are dedicated to finding new and unpatched security vulnerabilities in systems that have stayed unhacked from competitions like Pwn2Own. We say this because VUPEN has announced that they are working on a 0-day exploit aimed at another product that has always survived the contest: Android, the popular mobile operating system owned by Google. According to VUPEN, a malicious user could gain control of a Nexus S running Android provided the user visited a malicious Web page. Quite possibly, the new 0-day exploit has been found in the WebKit[6] rendering engine used in the Android Web browser, which has been a source of security flaws in Safari and Google Chrome.



VUPEN VUPEN Security
Our upcoming 0day demo will probably target Google...Android phones Nexus S. It will be remotely pwned and rooted via a simple web page.
11 may

FIG.14. ***VUPEN TARGETS ANDROID.***

We still don't know if VUPEN has managed to achieve their objective but… Will they also dare to exploit ChromeOS, Google's operating system for Netbooks? We'll have to be very attentive to their next moves, as VUPEN is nowadays regarded as one of the top IT security companies providing vulnerability research and intelligence solutions.

This once again shows that a fully updated operating system is just not enough in today's world. You need to use additional security tools and technologies that help protect against intrusions, infections or theft of confidential information from home and business computers.

[1] http://zdi.tippingpoint.com/
[2] http://www.webkit.org/
[3] http://cansecwest.com/
[4] http://en.wikipedia.org/wiki/Data_Execution_Prevention
[5] http://www.vupen.com/demos/VUPEN_Pwning_Chrome.php
[6] http://www.webkit.org/

05| Conclusion

While the recent cyber-attacks may have spread a sense of insecurity, at the same time they have taught us an important lesson. Large corporations like Sony have learned the hard way that not taking security seriously can affect their business and even the value of their stock options.

Events like these have forced companies to give security the importance it deserves. And most importantly, we as users have also learned to demand the adoption of adequate measures to protect our personal and confidential information as, with identity and corporate information theft on the rise, it is essential to choose those organizations that can store our data securely.

06| 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/**

4462