Bitdefender®

H1 2012E-Threat Landscape Report

Author
Bogdan BOTEZATU – Senior E-Threat Analyst

Contributors:
LiviuARSENE – Mobile Threats Analyst
Loredana BOTEZATU – Communication Specialist
Adrian MIRON – Lead Antispam Researcher
Dragoș GAVRILUȚ – Lead Antimalware Researcher
Dan BERBECE - RTVR Database Administrator

Table of Contents

Table of Figures

Intro: Welcome to the Era of State-Sponsored Attacks

The discovery of Stuxnet not only took the security industry by surprise back in 2010, but also shed new light on what was called “cyber-warfare”: Internet-based conflict involving politically motivated attacks on information and information systems.

The first half of this year brought new surprises in terms of cyber-warfare with the discovery of Flamer – one of the most potent and complex e-threats to date. Designed to run stealthily and collect data through an astounding range of approaches, Flamer managed to evade AV detection for some five years.

Flamer is one of the biggest pieces of malware to date: it is comprised of more than 63 distinct files, including core components and plugins. The modular architecture allows it to rapidly extend its functionality with the addition of LUA code.

Governments continued to rely on malware for cyber-espionage purposes throughout the first half of 2012. Cyber-criminals from China have attempted to hit military personnel with targeted spam mail bundled with 0-day Flash exploits.

Malware Spotlights

- In the first six months of 2012, the malware landscape remained relatively constant, with Trojan.AutorunInf, Win32.Worm.Downadup and Exploit.CplLnk as the top three e-threats worldwide. The first two pieces of malware are more than four years old and, even though the vulnerabilities that allow them to infect systems have been addressed, they still claim victims.

- H1 2012 was also rich in data breaches and data disclosure. Extremely popular web services such as Last.FM, LinkedIn and Yahoo Voice, as well as high-traffic forums (such as Phandroid's Android Forums) were compromised, had their user database stolen and shared online. In some instances, the database leaks were followed by phishing attempts sent to victims.

- Computer users permanently connected to the Internet have different challenges than those who spend less time on the web. According to the **Bitdefender Cloud,** the most frequently-encountered risk to users who stay permanently online is Application.InstallCore, a module that pushes advertisements and is known to be installed by other malware without the user's consent. Other risks are TrojanAutorunInf, as well as Exploit.CplLnk and Win32.Worm.Downadup.

- Malware focused on direct financial gain is constantly gaining ground. Apart from the notorious Banker Trojans, covert Bitcoin miners have been growing since their discovery in mid-2011. Cyber-criminals either exchange the mined Bitcoins for local conventional currencies, or use them for trading on underground forums.

- Commercially-driven malware also played a key role in the first half of 2012 as gangs such as those behind Carberp or the Android porn malware scandal in Japan were arrested.

- The first half of the year concluded with the fallout of the DNS Changer infrastructure operated by Estonian cyber-crime corporation Rove Digital and dismantled by the FBI in November 2011. The shutdown of the malicious DNS servers forced the FBI to operate clean ones at the same IP addresses to preserve the web connectivity of infected hosts. As per the court order, the replacement DNS servers could be operated until July 9th, even though more than 350,000 hosts were still using the rogue DNS servers to connect.

Malware Threats in Review

The e-threat landscape for the first half of 2012 is relatively unchanged in terms the top three threats. Of particular importance is the increased activity of Win32.Sality.3, a variant of the notorious Sality botnet estimated to have comprised more than one million computers around the world. Trojan.FakeFolder.B has also jumped from ninth to the fifth place in less than six months, as the number of computers it affects nearly doubled.

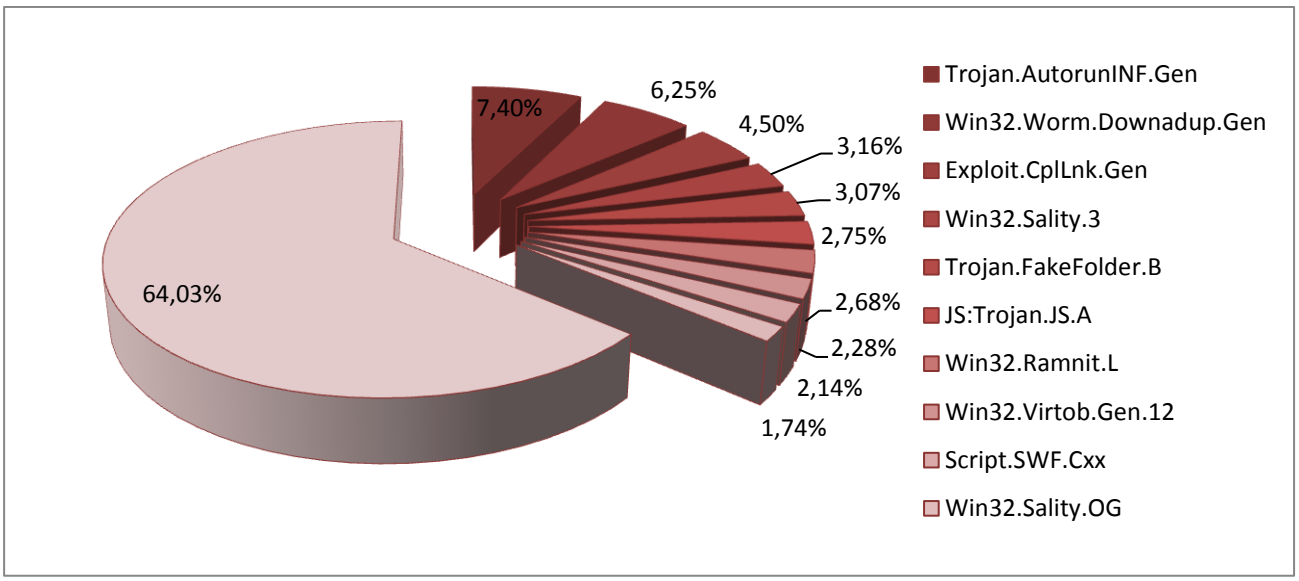


Figure 1: Malware breakdown for H1 2012

1. Trojan.AutorunINF.Gen– 7.40% (-1.14 / -)

Trojan.AutorunInf needs no introduction - it has been one of the world's top three e-threats for about four years. This detection addresses rogue Autorun files created by a variety of malware families to facilitate spreading via removable media. Although autorun.inf files are not malicious by default, they are frequently created by other e-threats with worm-like capabilities and placed on flash drives, along with the real malware. As soon as the device is plugged into a computer with the Autorun feature enabled, the autorun.inf file automatically executes the piece of malware, infecting the PC. This feature has been removed from Windows Vista SP1 and newer operating systems, but older OSes are still vulnerable.

2. Win32.Worm.Downadup – 6.25% (+0.58 / -)

The Downadup worm emerged in early 2008 and caused one of the largest epidemics of all times, as it managed to infect more than 12 million computers in less than 24 hours. The worm exploits a vulnerability in the Microsoft Windows Server Service RPC (also known as MS08-67) to spread on local networks. Infected computers are denied access to security updates, sites of antivirus vendors or those offering technical

support. The botnet was used to push rogue antivirus and other e-threats, but the Downadup worm hasn't seen any development in the past two years.

3. ExploitCPLLnk – 4.50%(+0.11 / -)

Exploit.CplLnk.Gen is the component in Stuxnet that allows it to launch itself whenever an infected USB drive is plugged in. The USB drive uses lnk (shortcut) files that trigger an exploit in the way the Windows operating systems display Control Panel items. This trick is one of the five zero-day exploits that Stuxnet used for spreading and works on all versions of the Windows operating system. Most likely, cyber-criminals behind the Stuxnet operation chose a zero-day exploit, and not the Autorun.inf approach for USB spreading, to minimize the chances of being spotted.

4. Win32.Sality.3 – 3.16%(-0.03 / +1 place)

Win32.Sality.3 scores 3.19 percent of global infections in H1 2012. This extremely aggressive file infector attaches itself to other scr and exe files on the victim PC, and tries to infect other systems in the same network. The Sality virus is highly encrypted to prevent antivirus detection. It is also equipped with a rootkit component used to kill antivirus solutions (which are otherwise out of the malware's reach). The Sality botnet is comprised of over one million infected computers to date, which can be remotely manipulated by the botmaster.

5. Trojan.FakeFolder.B – 3.07% (+1.49 / +4 places)

Trojan.Fake.Folder.B enjoyed explosive growth in less than six months, jumping from ninth to fifth place. This relatively new e-threat is a component of the Dorkbot Trojan, which uses it to keep the malware active in the computer's memory. The Dorkbot Trojan lists the folders on the infected PC, creates a shortcut to them, then hides them. Whenever the user tries to access the folder, the shortcut also starts the malicious component in the Recycler folder.

6. JS:Trojan.JS.A– 2.75% (new entry / new entry)

Ranking sixth in the e-threat top for H1 2012, Trojan.JS.A is an encrypted piece of JavaScript code that appends itself to HTML pages or to other JavaScript snippets. It is then used to redirect the user to a page that hosts other e-threats, particularly web exploits against the browser and the Java Runtime Environment. These landing pages also collect information about the compromised systems such as domain name, browser type and version, as well as location.

7. Win32.Ramnit.L – 2.68% (new entry / new entry)

Win32.Ramnit.L is a file infector that adds its malicious code to clean files with specific extensions. In order to run, it also injects its code into some processes, especially into the default browser. After it infects the computer, Win32.Ramnit.L contacts its command and control server and awaits instructions. Among other things, Ramnit can steal FTP login credentials, as well as browser cookies.

8. Win32.Virtob – 2.28% (-0.12 / -1)

This top's third file infector is Win32.Virtob, a piece of malware that also attaches to scr and exe files on the victim PC. Written in assembly language, the virus is optimized for speed and stealth. It pays extra attention to which files it infects and, to prevent the system from crashing and killing its host, it does not infect system files. Virtob's main specialties include file and cookies theft, and collects login credentials for all accounts authenticated on the system.

9. Script.SWF.Cxx – 2.14% (new entry/ new entry)

Ninth in the H1 2012 E-Threat Landscape Report, Script.SWF.Cxx is a detection that intercepts piece of ActionScript code used in a targeted attack against US military officials. This piece of code was bundled with an allegedly-secret Word document on Iran's oil and nuclear situation. Next to Exploit.CplLnk, Script.SWF.Cxx is the second piece of malware that has been used for gathering military intelligence.

10. Win32.Sality.OG – 1.74% (-0.66/ -2)

Win32.Sality.OG concludes the Top 10 Malware for H1 2012. This variant of the Sality virus preserves all the features of Win32.Sality.3, but uses an older, less advanced encryption algorithm to shield its code from analysis and detection. The virus dropped two places since the last half of 2011.

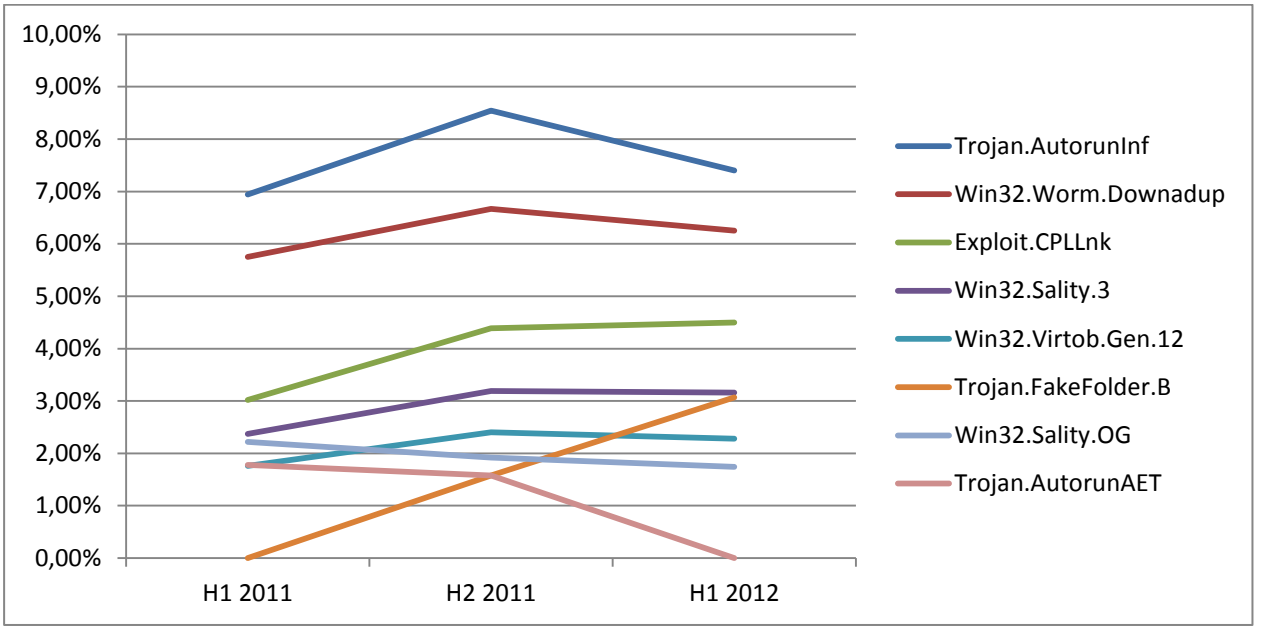


Figure 2: Malware evolution for H1 2011, H2 2011, and H1 2012

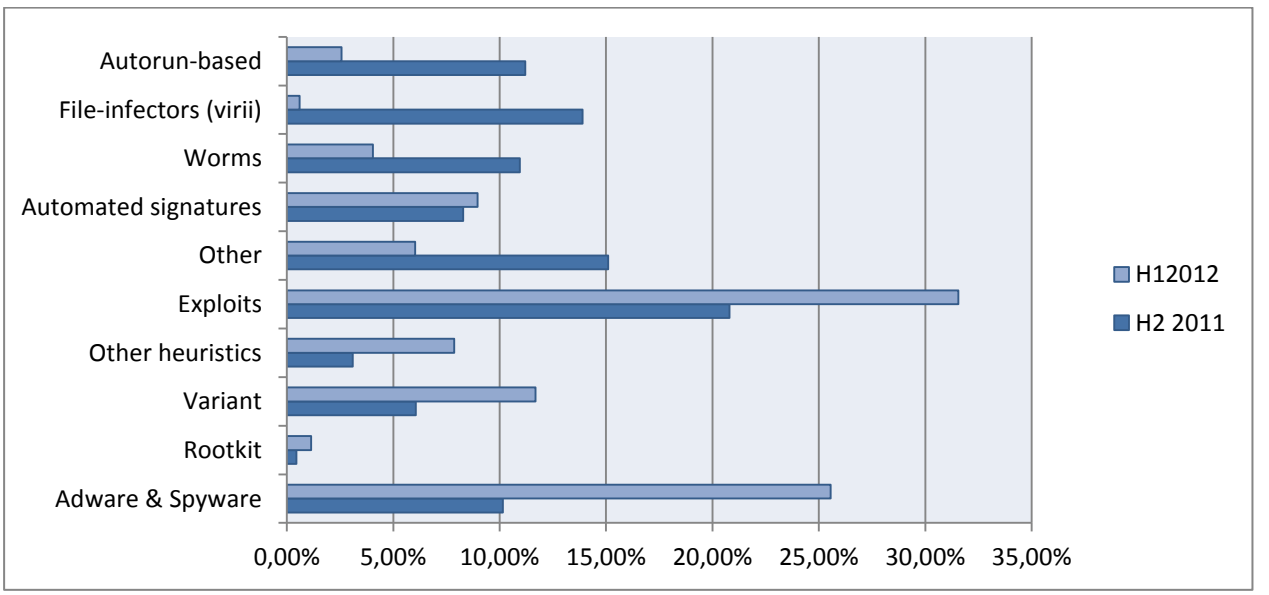


Figure 3:Malware breakdown for H1 2012 – Exploits are the infection vector of choice

Web-driven software exploits are now the most popular form of malware delivery – a direct result of the increased adoption of Internet around the world and liberalized access to exploit packs. Among the most vulnerable applications are Adobe Reader installations older than 9.04, the Java Runtime Environment 7 and older, as well as the Adobe Flash plugin.

Social Networking Threats

Regardless of their profile, social networks have a significant number of users freely sharing information about themselves, their jobs or their friends. Facebook's 900 million users have been exposed this half year to a multitude of scams, ranging from the consecrated "Facebook in other color" to the newer cons that promise the removal of the Timeline feature.

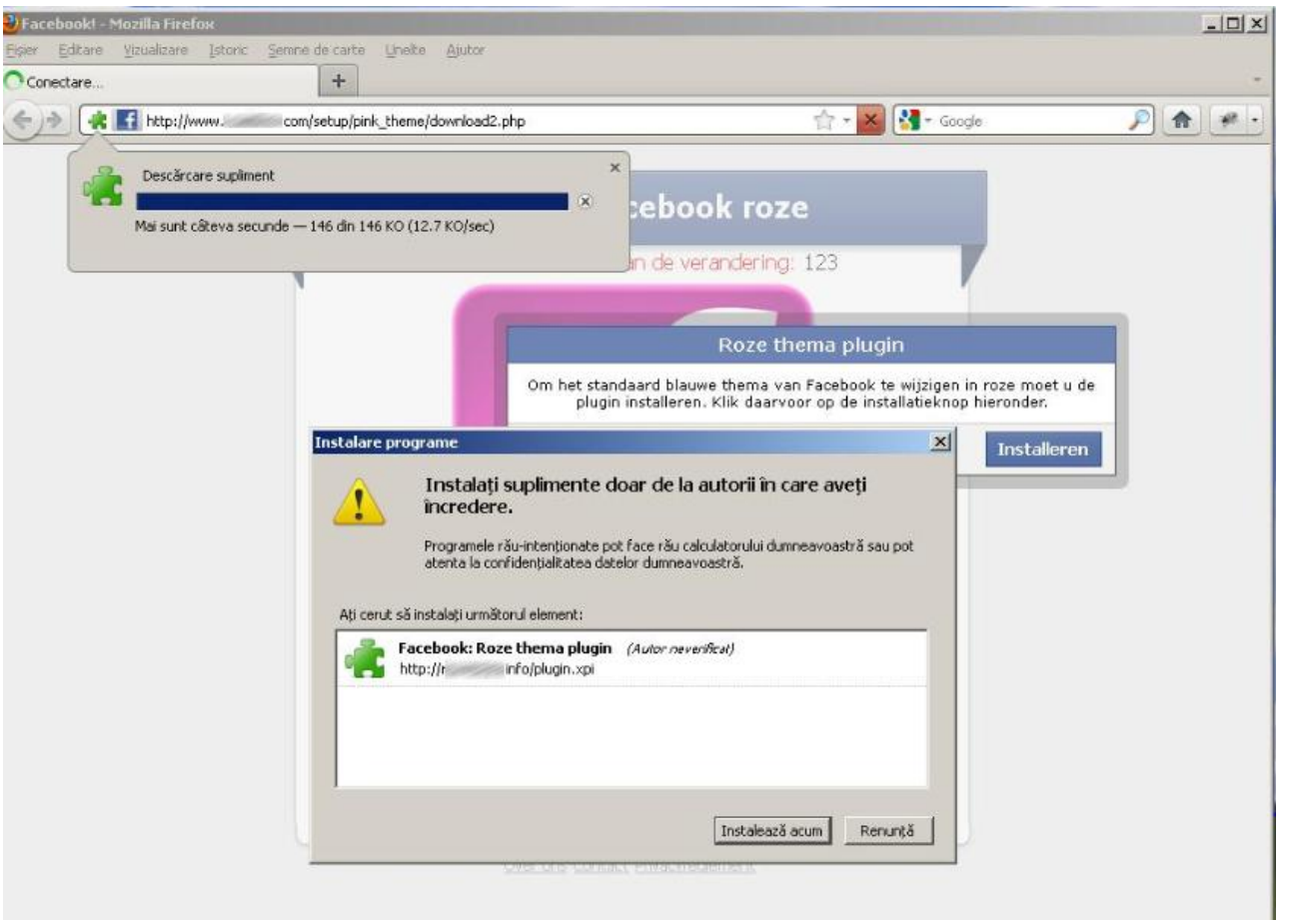


Figure 4: Facebook theme changer delivers malicious add-on to Chrome, Firefox users.

This campaign is addressed to users who would like to switch from the standard blue-ish theme to a different one (pink or green for instance). This highly-popular scam requires the user to download and run a file from a location outside the social network. The file turns out to be a browser add-on for either Firefox or Chrome which will re-skin the Facebook website by manipulating the CSS file, but will also perform random redirects to survey pages or premium-rate SMS services such as horoscope or ringtones.

Bogus Facebook applications developed and hosted by third parties have also been after users' data. This specific application discovered in mid-May targeted mobile users. The application, dubbed "Girlfriend

checklist" looks for mobile traffic and redirects the user to Android games that they are advised to install. To ensure spreading, the application requires tagging permission so "potential candidates" can be made aware of the fake application.

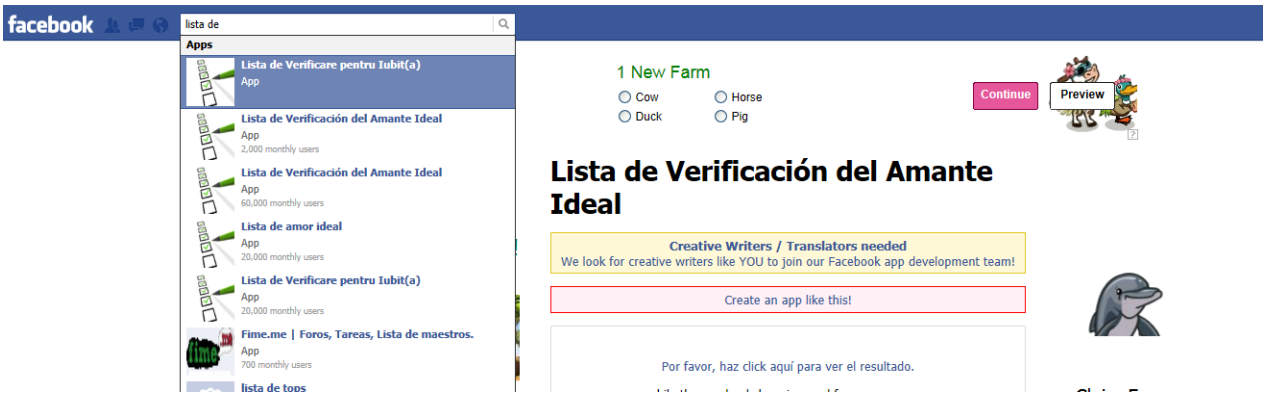
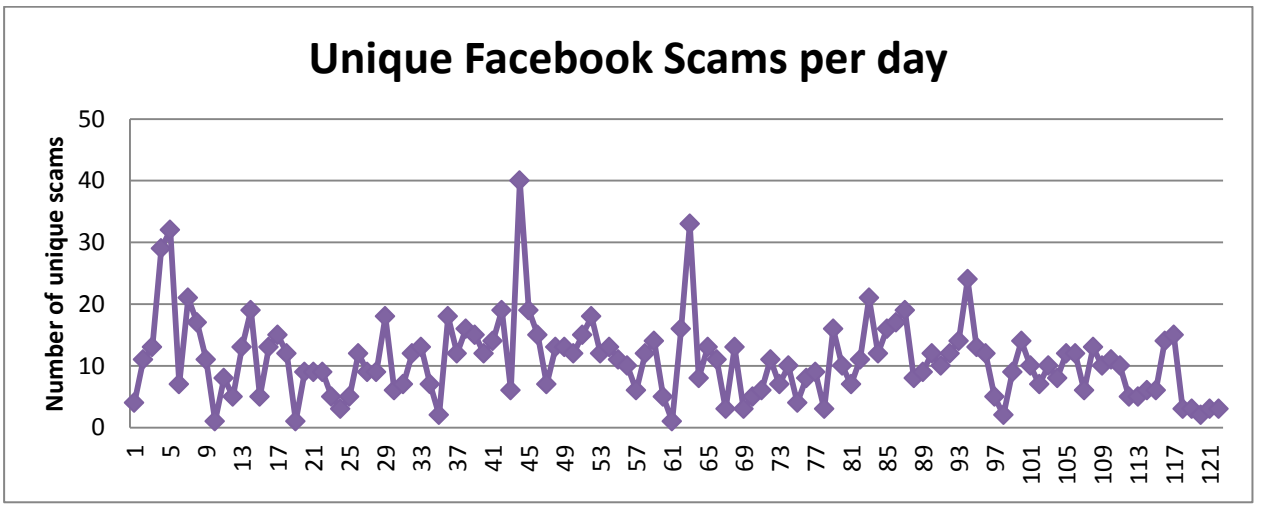


Figure 5: Bogus Facebook application redirects mobile traffic coming from Android handsets

Between January and July 2012, Bitdefender has identified an average of 7.3 new scams per day, as shown in the graphic below. These scams have reached more than one quarter of a million users. Given the small window of opportunity, it is safe to assume that these users were hit within a day or two of the scam's emergence.



Although it's the most popular social destination, Facebook was not the only targeted social network in H1 2012. As Google's Pinterest started to gain ground, numerous subversion tools became readily available on underground forums.

While some tools plant invisible "follow" buttons on third-party web pages, others take a more radical approach to socializing. One of these multi-purpose tools is the PinPal Bot, an application that allows the

generation of bulk accounts for spamming other Pinterest users with affiliate sale products disguised as legitimate content.

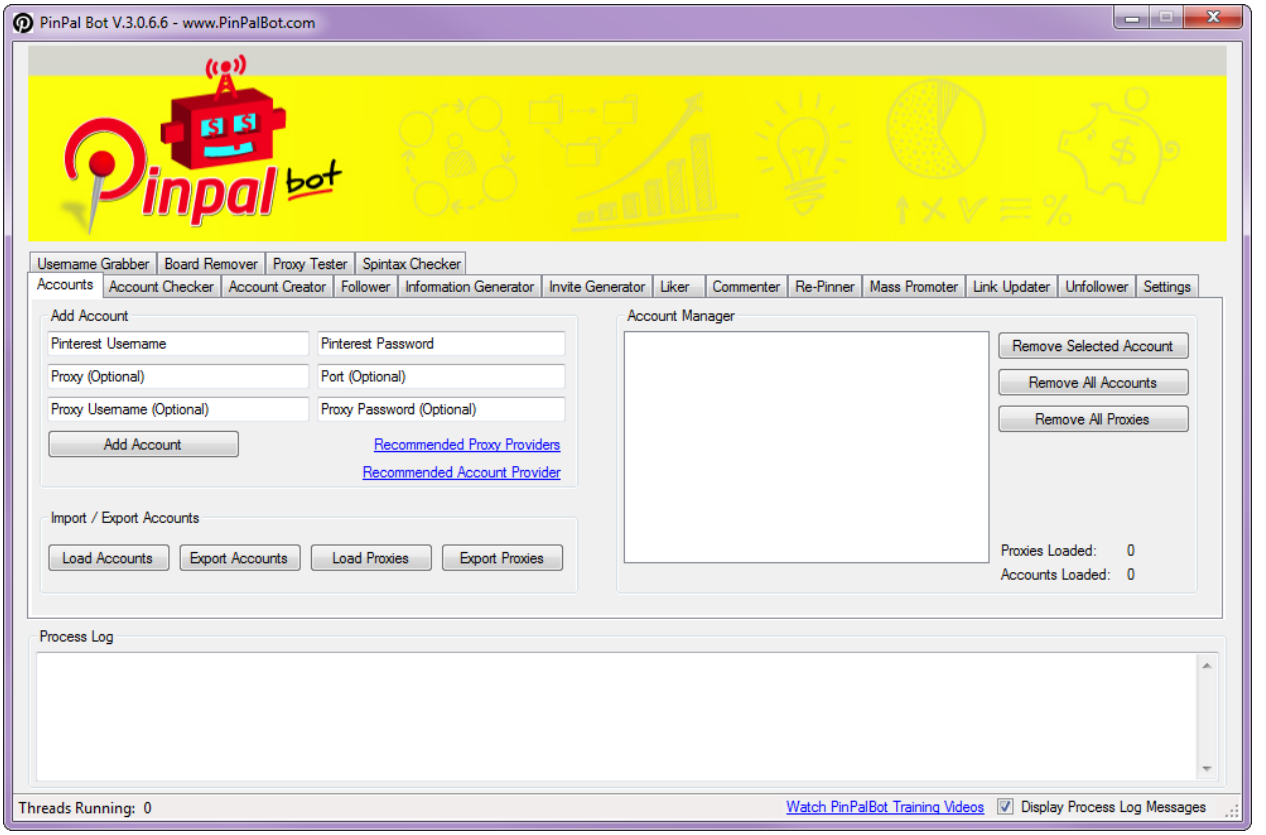


Figure 6: PinPal Bot, a multi-purpose abuse tool.

Spam Threats in Review

Spam continued its decline in the first six months of 2012, reaching an all-time low of around 70% of total amount of spam sent worldwide. As compared to the previous semester, the Bitdefender Antispam labs identified a drop of roughly 5 percent in volume. This appears related to the termination of smaller botnets as well as with the migration of spammers toward social networks where they can target victims more easily.

If most spam until the first half of 2011 was in English to cover broader audiences, regional spam was on the rise throughout the first half of 2012. One of these spam waves is a job offering message that comes in eight languages.

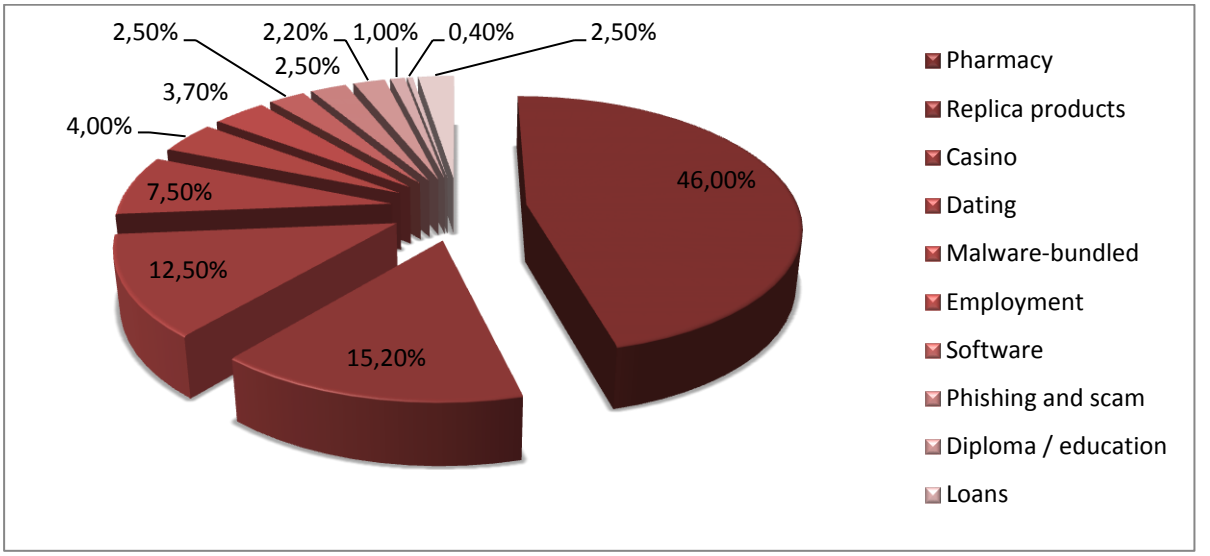


Figure 7: Spam breakdown by type

Pharmacy spam is once again the most crowded niche for spammers, with roughly 46 in one hundred spam e-mails promoting a vast assortment of products, from prescription-based drugs, Canadian Pharmacy sexual enhancers to diet pills that have not been approved by the FDA for public sale. Medicine spam campaigns have taken a multitude of forms, from complex, image-based messages to one-liners accompanied by links.

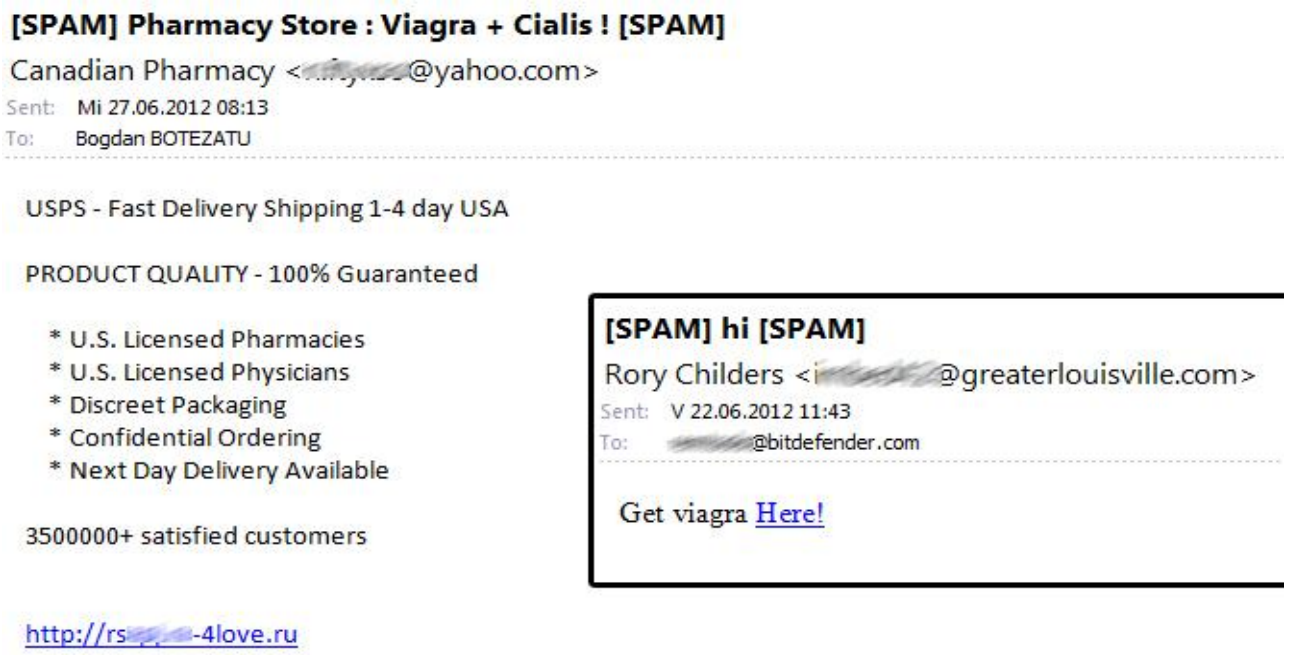


Figure 8: Canadian Pharmacy medicine simple spam templates

The number of spam messages with malicious attachments also increased throughout the first half of 2012, from 2.5% in H2 2011 to a whopping 4 percent. The most important spam campaigns bundled with malware feature the Zeus bot, as well as generic downloaders and older pieces of malware.

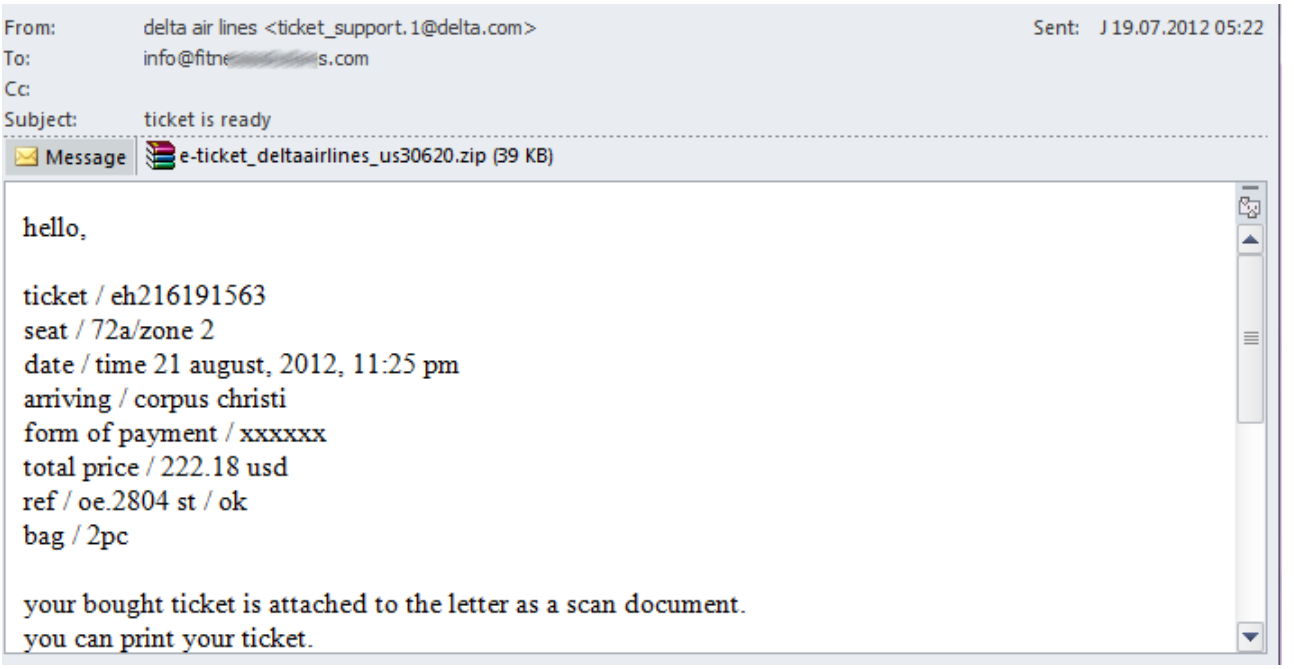


Figure 9: Zeus-bundled ticket confirmation spam message

Employment spam has soared in abundance for the past six months. Even amid a slight decrease in the number of messages (from 4.00% in H2 2011 to 3.7 in H2 2012), the spam waves have become more diverse and much more appealing to the end-user. The most intensively advertised jobs are those that allow telecommuting or part-time presence, as well as regional offerings. The spam waves identified through 1H 2012 are highly targeted and often translated in the victim's native language.

Although these job offerings may look appealing, especially in the context of the employment crisis, these are regular scams that either ask the victims to pay an "HR processing fee", ask for sensitive information for identity theft purposes or, more frequently, for money mulling – fencing money and goods obtained through cybercrime for the bad guys.

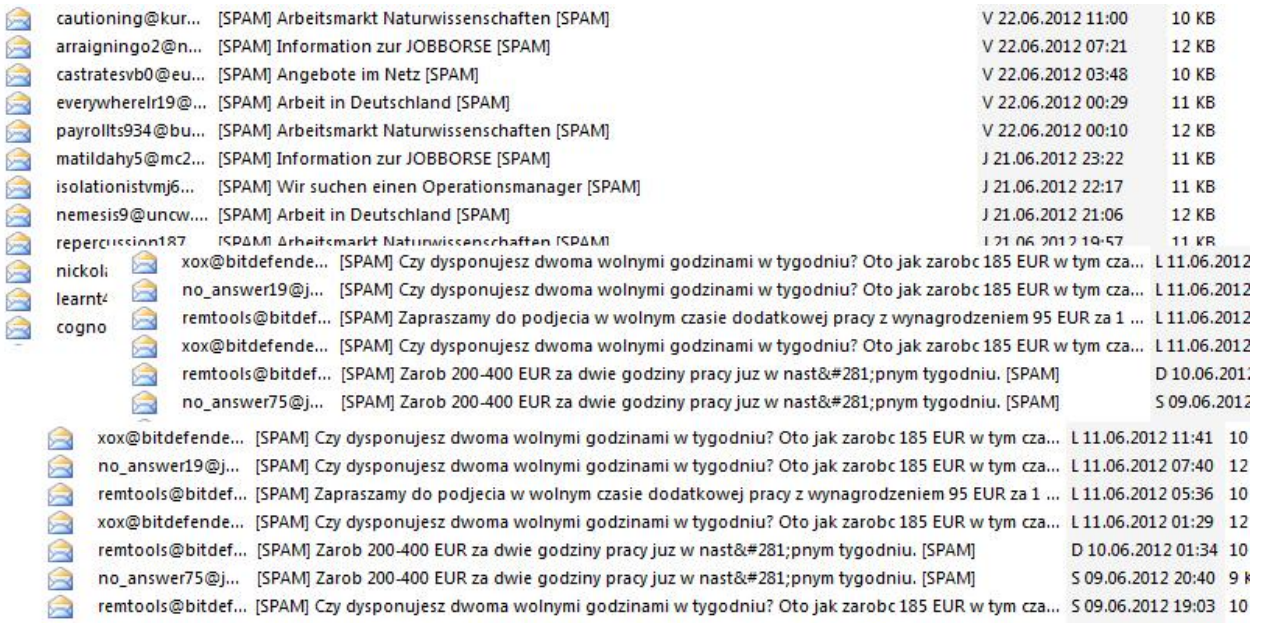


Figure 10: Job offerings with multiple monetization methods

Another significant and unusual spam wave that made its rounds in 2012 was the invasion of [no subject] messages sent through the Yahoo! infrastructure by computer users whose accounts were compromised. The one-line message included a link to a compromised website (usually a vulnerable Wordpress installation). The link leads the user to Canadian Pharmacy advertisements after a series of browser redirects.

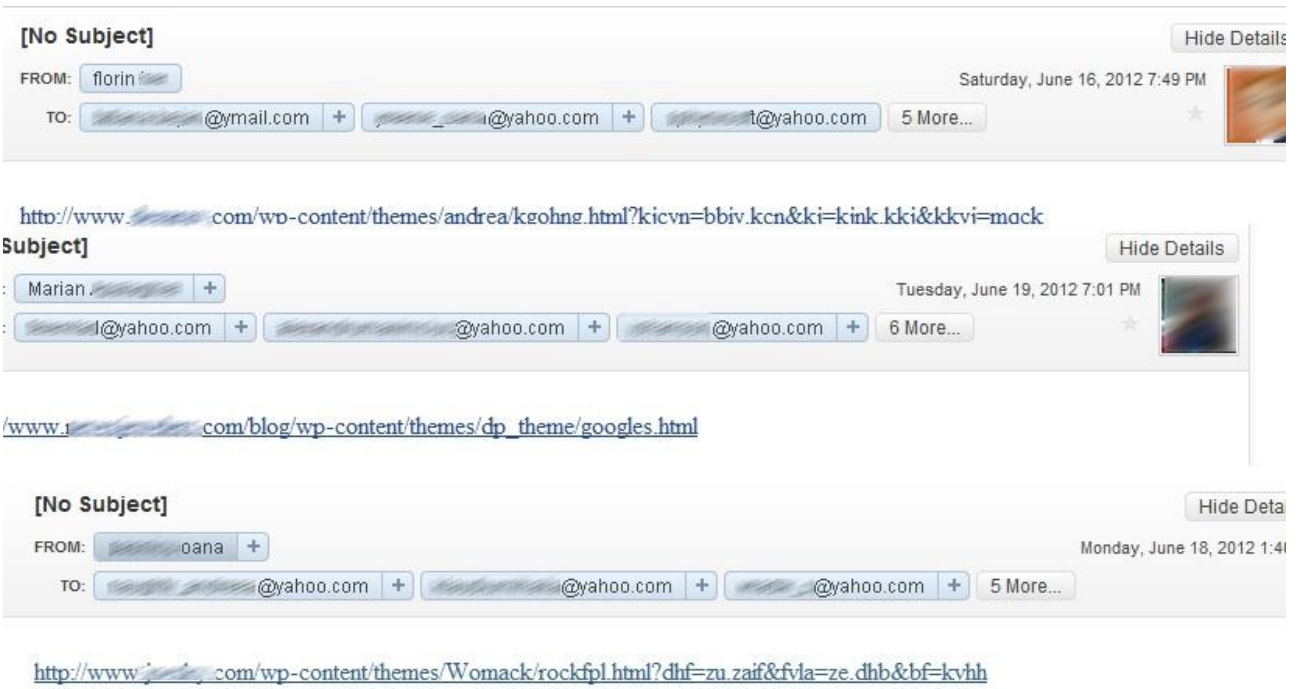


Figure 11: [No Subject] spam wave spreads like wildfire

Phishing and Identity Theft

During the first six months of 2012, phishers were more active than in the last half of 2011, raising their production from 1.5% of all spam messages sent worldwide to an estimated 2.5%. More than half (51%) of all phishing pages in the world were hosted on servers or fast-flux botnets in the United States. Other phishing-friendly countries are Germany (5.5%), the United Kingdom (4.5%) and Canada (4.2%).

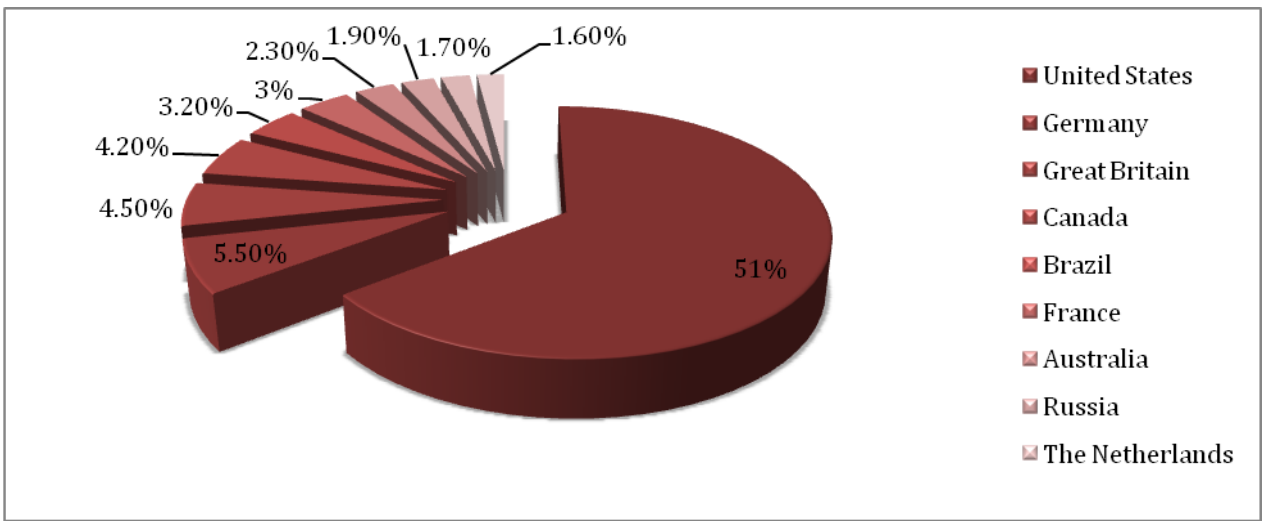


Figure 12: Top 10 countries harboring phishing pages in H1 2012

Financial institutions were once again the most targeted businesses in phishing e-mail. Online payment systems such as PayPal and Western Union have been targeted in numerous phishing attacks generated with mainstream DIY phishing kits.

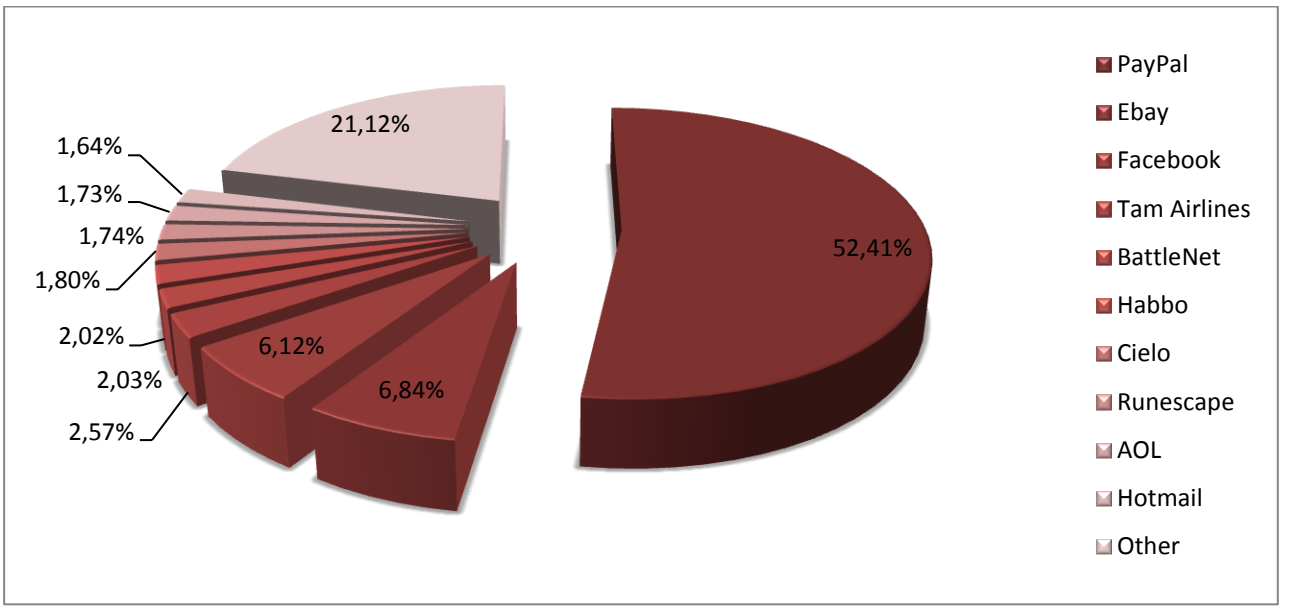


Figure 13: Top 10 Phished Brands for H1 2012

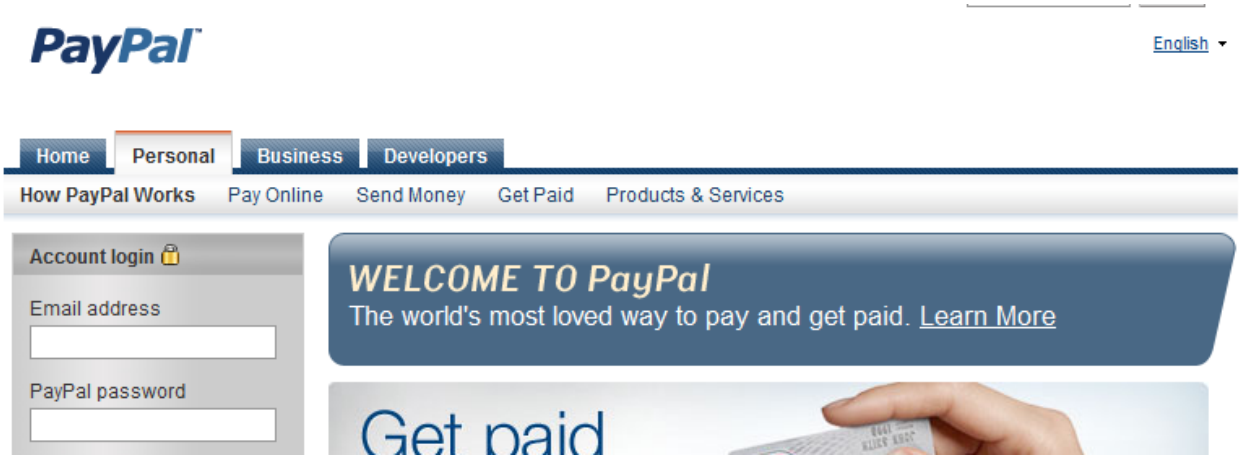


Figure 14: PayPal phishing page

Targeted phishing attacks were on the rise in the first half of 2012. Regular web users have been particularly hit by phishing that capitalizes on the data leaks in the LinkedIn, eHarmony and LastFM incidents. Even though the professional social network expressly stated that it will not send password change notifications to affected users, multiple spam waves have emerged following the database leak.

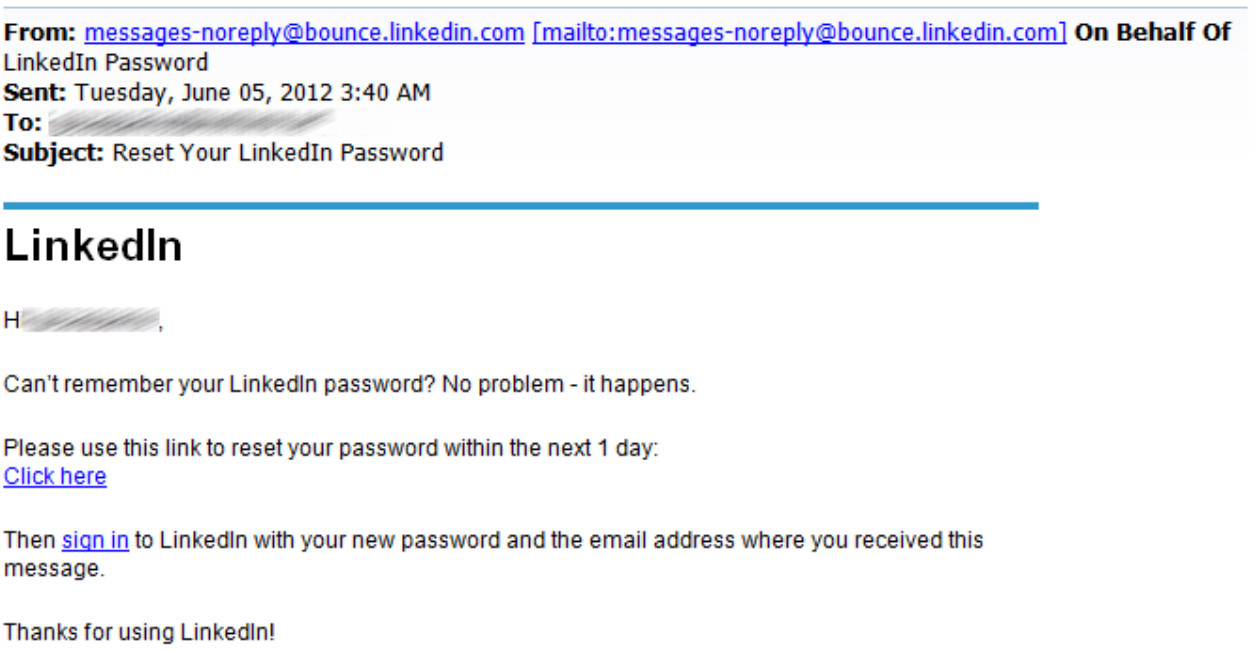


Figure 15: Alleged LinkedIn password change request

If regular web users may lose money to phishing, corporations and governments have to prepare for more than that: devastating security breaches, loss of sensitive data or even military intelligence leaks. This was the case with highly-targeted phishing attacks from China aimed at US military officials in mid-March.

The Android Landscape

For the past six months we've seen an alarming increase in detection of what we call **Android.Adware.Mulad.A**, which is basically adware injected into other apps. We could be looking at a semi-legitimate way of generating revenue for malware developers.
After injecting legitimate apps with adware code, these Mulad-infected apps are uploaded to third party marketplaces. While they are not malicious in nature, annoying ads popping up can ruin a gaming experience.

Although we won't include **Android.Adware.Mulad.A** in our top 10 malware chart for H1, we'll acknowledge that 25.94% of all scanned apps felt the presence of this type of adware. With one in four apps having Mulad, it's safe to conclude that you probably have at least one of these installed on your handset.

With no major threats creeping up these past six months, we've only seen an increase in malware that deals with data theft, rooting, and a general tendency for exhibiting the same behavior as PC malware. We've also seen a couple of examples on how Android malware used microblogging platforms such as Twitter to obfuscate C&C domain names.

Malware coders appear interested in setting up botnets via malicious apps, and exploring such opportunities is an obvious tactic as the mobile market share constantly increases. The only thing missing is ISPs to enable IPv6 support, making botnet smartphones the largest tool that could be used for DDoS attacks.

The evolution of Android mobile malware reveals that coders spend a lot of time developing intrusive apps. This trend will surely keep rising as smartphones are used for online banking, NFC payments and other activities that involve personal and confidential user information.

With almost one billion smartphones in use, they're becoming an appealing target as most users opt for carrier deals that involve an internet connection. As both personal and work tasks are handled by Android-running devices, malware will probably skyrocket in the immediate future.

H1 Spotlights

An interesting example is a recently discovered Android spyware that hides from users and then attempts to enable the Wi-Fi connection to collect information regarding nearby hotspots. This information, along with carrier details and GPS coordinates, is sent to an attacker-controlled domain. The details could be used to plan attacks on networks or for other malicious purposes.

An SMS bot spread through email attachments read from Android-running devices stood out, as it charged users with premium rated numbers without their knowledge. The Twitter obfuscated command and control domain also received bot ids so attackers could closely track how many devices they infect. The malware received instruction by accepting parameters such as phone number, message content, and the number of times the SMS should be sent.

This example proves that domain name obfuscation by means of microblogging platforms is picked up from PC malware. This technique will probably be used in other attacks as malware coders need to cover their tracks.

Ice Cream Sandwich, also known as Android 4.0.4, was the target of a proof-of-concept app that could enable attackers to root a device by means of a single app, without requiring a reboot. This framework attack was demo'ed with a clickjacking example, enabling attackers to gain control of how apps behave. With no malware sample with this type of attack, the demo is proof enough that new and sophisticated ways can be developed to target Android users.

Top 10 Android Malware Threats for H1 2012

Our H1 Android Mobile Malware Report was mostly dominated by exploits and Trojans - no surprise there. Malware usually uses exploits to gain privileged access to device resources and user rooted devices make it easier for malware coders to develop Trojans and more.

Willingly rooting personal Android devices is risky and opens numerous threats. As such, the number of detected exploits reflects the personal choices users make when they opt for a device rooting solution.

The percentages extrapolated below do not include the **Android.Adware.Mulad.A** samples, as they are considered adware and not malware.

Mobile Malware top for January – July 2012		
01.	ANDROID.TROJAN.FAKEDOC.A	21.83%
02.	ANDROID.EXPLOIT.RATC.A	13.53%
03.	ANDROID.EXPLOIT.GINGERBREAK.A	7.73%
04.	ANDROID.EXPLOIT.EXPLOID.B	5.64%
05.	ANDROID.HACKTOOL.FACENIFF.A	3.46%
06.	ANDROID.EXPLOIT.ASROOT.B	2.00%
07.	ANDROID.EXPLOIT.ASROOT.A	1.95%
08.	ANDROID.TROJAN.FAKEDOC.B	1.81%
09.	ANDROID.ADWARE.WALLAP.A	1.80%
10.	ANDROID.HACKTOOL.DROIDSHEEP.A	1.76%
11.	OTHERS	38.5%

1. Android.Trojan.FakeDoc.A

We've previously encountered this Trojan bundled with "Battery Doctor", an Android app supposed to optimize a user's battery. Before installation, the app requires access to the user's Gmail account so it can covertly broadcast location, emails and carrier ID to an attacker-controlled server every four hours. The user is also bombarded with popup ads. Scoring 21.83% of the global infections, the Trojan is ranked first in our H1 Android Mobile Malware Report.

2. Android.Exploit.RATC.A

Most commonly known as "Rage Against the Cage", it is used for rooting Android devices so users can gain privileged access to some of the device's resources. The downside is that if the rooted device is infected with malware, it can access the same privileged resources. Rooting Android handsets leaves the mobile OS vulnerable to malicious apps. Ranked second with a 13.53% infection rate, the exploit is still the one most commonly used for rooting.

3. Android.Exploit.GingerBreak.A

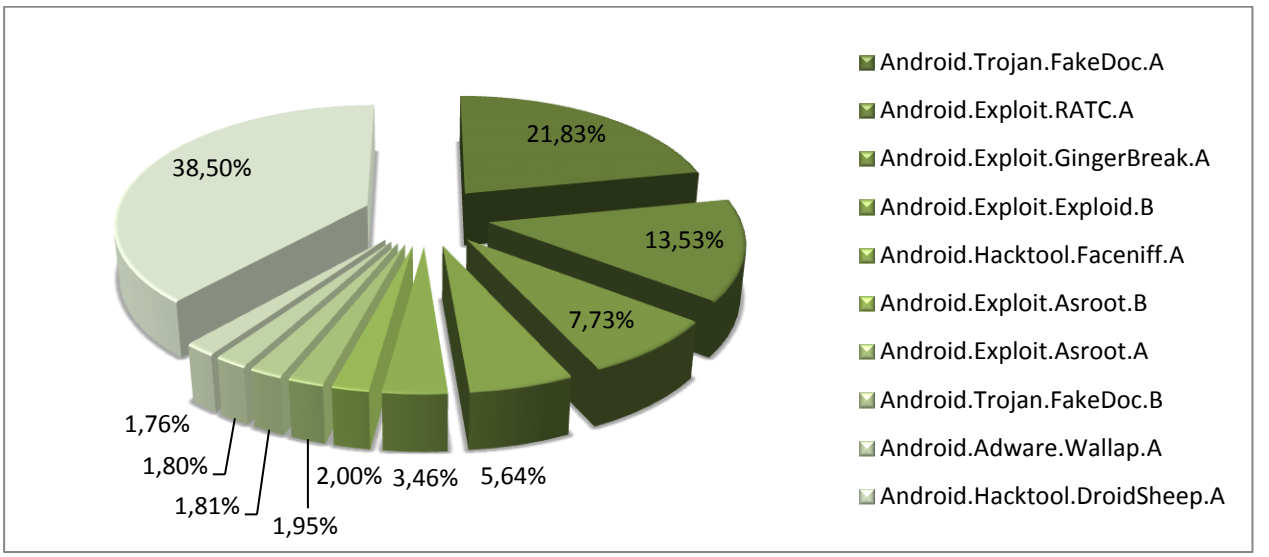
Gingerbread-running Android devices (also known as Android 2.3.3) are often rooted using this exploit and users fail to realize that malware often includes code coming from this specific exploit. Most Trojans packed with legitimate apps use this exploit's code to gain access to privileged resources. Although it scored 7.73% of global infections, it proves a large number of Gingerbread-running Android devices are still rooted by users.

4. Android.Exploit.Exploid.B

This is a third type of exploit for rooting Android-based devices. Its code is also used by various malware families that try to root devices without users' knowledge to run outside Android's security container. 5.64% of global infections were caused by this exploit, ranking fourth in our H1 report.

5. Android.Hacktool.Faceniff.A

Mostly used to intercept Wi-Fi traffic, this Android tool enables attackers to spot users and passwords for popular services such as Twitter, Facebook or other social networking platforms. This hacktool can be particularly useful to those who practice identity theft through social networking websites. The 3.46% infection rate places the malware fifth in our ranking system.



6. Android.Exploit.Asroot.B

This is yet another exploit used to root Android-running devices through a kernel bug triggered by a macro. This is a pretty common piece of code that malware uses to gain privileged access to a device. With a 2.00% global infection rate, the exploit still plays a major part in malware development.

7. Android.Exploit.Asroot.A

Just like the Android.Explot.Asroot.B, this new variant of the same exploit behaves in pretty much the same way, enabling Android malware to gain access to resources that otherwise it couldn't reach. This type of malicious code is usually bundled with apps from third-party marketplaces and can deliver various payloads.

8. Android.Trojan.FakeDoc.B

This Trojan is just a variant of Android.Trojan.FakeDoc.A. The only difference between the two is the apps that they come bundled with. It makes sense that malware coders would inject popular apps with malicious code to maximize their attacks. Although it has a lower infection rate than Android.Trojan.FakeDoc.A, of only 1.81%, it's unlikely that this malware Trojan family will completely go away.

9. Android.Adware.Wallap.A

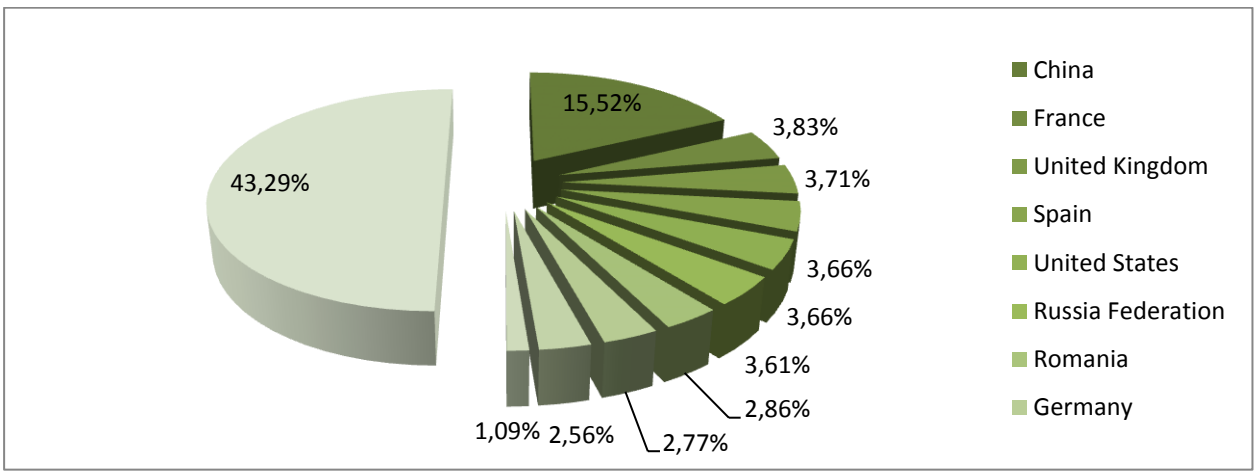
Another piece of adware that seems to be injected in legitimate apps and distributed via third-party marketplaces appears to be used to generate income. We've seen an alarming increase in apps that have been injected with such code, as Android.Adware.Mulad.A proves. Although Android.Adware.Wallap.A is only responsible for 1.80% of the global infection rate, it may gain traction.

10. Android.Hacktool.DroidSheep.A

Tenth in our globally-recorded infections chart, this hacktool is mostly used to hijack personal accounts by spoofing public Wi-Fi networks and collecting usernames and passwords from those connected. With a 1.76% infection rate, it proves that identity theft and account hijacking is still prevalent on Android-running devices.

Top 10 Countries Affected By Android Mobile Malware

Although Android malware isn't usually country-specific, except for premium number SMS Trojans, this H1 report reveals that most countries have almost the same infection percentages. Apart from China, which leads the chart with a 15.52% app infection rate, France and the United Kingdom are almost neck and neck with 3.83%, respectively 3.71% infection rate.



Spain and the United States have the same 3.66% Android malware infection rate, closely followed by Russia in sixth place with 3.61% app infection rate. These last five countries appear to spark the same kind of interest for all malware coders. The differences in percentage points are not very significant, meaning malware appears not to care about geographical localization, demographic, or culture.

Romania is ranked seventh with a 2.86% Android malware infection rate, followed by Germany and India with 2.77%, respectively 2.56%. Malaysia is 10th, with a 1.09% malware infection rate.

Future Outlook

The rampant evolution of malware will continue through the second half of 2012. We expect to see the number of malicious applications jump from 65,500,000 to approximately 76,000,000 as cyber-criminals tackle new means of obfuscation and delivery for e-threats.

Exploits against popular software will also continue to play a key role in compromising users' computers. Some of these exploits will target particular operating systems, but others will likely execute specific payloads depending on the operating system installed locally.

The release of Windows 8 in October will likely bring new challenges to both home and corporate users Based on previous experience with Windows Vista and Windows 7, the first live exploits for Windows will probably appear shortly after its release.

Corporations will have to deal with the security risks posed by the Bring-Your-Own-Device (BYOD) trend gaining increased popularity with managers all around the world. However, since many times these devices storing sensitive corporate data are not managed by IT personnel, the probability of data loss due device theft or loss is increasing.

The popular Android platform will come under heavy fire in the next six months, as its open application distribution model facilitates the delivery of malware through repackaged applications, especially in areas where an official Play Store is not available, such as China.