Bitdefender®

H2 2012 E-Threat Landscape Report

Author
Bogdan BOTEZATU – Senior E-Threat Analyst

Contributors:
Liviu ARSENE – Mobile Threats Analyst
Loredana BOTEZATU – Security Researcher
Adrian MIRON – Lead Antispam Researcher
Dragoş GAVRILUŢ – Lead Antimalware Researcher
Răvan BENCHEA – Malware Researcher
Csaba-Zsolt JUHOS - Malware Researcher
Alexandru BĂETU - RTVR Database Administrator

Table of Contents

© 2012 Bitdefender

Table of Figures

© 2012 Bitdefender

Intro: Welcome to the Era of State-Sponsored Attacks

The Flamer cyber-espionage tool discovered in June 2012 set new a new record for complexity of malware used in state-sponsored attacks. Its discovery built on other major security incidents throughout 2012 that affected regular PCs, OSX users and the Android operating system alike.

For the first half of the year, zero-day vulnerabilities played an essential role in disseminating malware with exploit packs as a favorite vector of infection. The dangerous zero-day exploit in the Java Runtime Environment (CVE-2012-4681) was documented and proof of concept was added to Metasploit, which became public knowledge before a fix was made available.

As a direct result, three billion devices running Java were vulnerable to remote code exploitation for roughly 48 hours. A second exploit hit in September and targeted Internet Explorer 9. Successful exploitation would allow remote compromise of the system with the installation of the Poison Ivy backdoor. Both zero-day exploits were used in advanced persistent attacks.

2012 saw fluctuations in the amount of junk e-mail as a proportion of e-mail traffic. The year began with a slight decrease in spam e-mails, but spam constantly gained ground towards the middle of the year. According to data gathered from the Bitdefender Antispam lab, the second half saw growth again, with small variations towards the end of 2012. The increase in the number of junk e-mails was nonetheless minor, by only 5%, leading to a rough value of 73% of the total number of e-mails sent worldwide.

Once again, **Trojan.AutorunInf** scores the top position in the global e-threat landscape, with 4.2% of all infections. Although still first, its impact has significantly dropped to more than 5% as compared to the previous time period. However, its downfall is compensated by the emergence of a new breed of e-threats: aggressive adware that is now present in about 4% of worldwide computers connected to the Internet.

© 2012 Bitdefender

Malware Spotlights

During the second half, Trojan.AutorunInf fell more than 3% from 7.4% in H1 to 4.6% in H2 2012. The fall is most likely associated with the shrinking market share of Windows XP, which is still vulnerable in its default configuration to autorun-based threats. It is also a sign that modern malware families are slowly ditching this obsolete vector of infection in favor of others that yield better.

Data breaches continued throughout 2012 with high profile companies such as Philips and small businesses such as a couple of Australian ISPs having their servers breached and their customers' data exposed on the Internet.

Another massive data breach at digital agency Blue Toad resulted in one million unique Apple UUIDs accompanied by a significant amount of Apple customer data making its way on Pastebin. The dumped data was the *piece de resistance* in Antisec's attempt to sully the image of the FBI, as the anonymous hacker group claimed the data had been stolen from the FBI and it only represents a little less than a 10th of what they recovered from the FBI laptop.

Exploit code originally found in Stuxnet now ranks third in the worldwide e-threat top. While some samples detected in the second half of 2012 are remnants of the Stuxnet worm, other samples are strictly civilian creations that borrowed from Stuxnet's crafty code. This is the most eloquent example about how regular computer users become collateral damage in cyber-wars waged by sovereign nations.

Adware is becoming more and more prominent as cyber-criminals seek ways to make money without blatantly breaking the law. The massive anti-cyber-crime operations that lead to the arrest of prominent gangs such as the team behind Carberp or the dissolution of spam affiliate programs have scared cyber-criminals somewhat.

At the same time, on the other side of the world, the teams behind ZeroAccess and SpyEye continued their attacks. Bitdefender intelligence revealed that some breeds of malware are

© 2012 Bitdefender

blending ZeroAccess with SpyEye to create a malicious environment that can't be disinfected with regular anti-malware tools.

Malware Threats in Review

The e-threat landscape is relatively unchanged for the first three spots. Of particular importance is the increased activity of Win32.Sality.3, a variant of the notorious Sality botnet estimated to include 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.

1. Trojan.AutorunInf -4.66% (-2.74 / previous 1st position)

Trojan.AutorunInf was discovered in 2008 and has made it into the top three malicious applications ever since. This detection intercept specially-crafted Autorun files that are highly obfuscated to prevent users from reading them if opened. The files are created by the most well-known e-threats such as Sality, Virtob, Downadup or Stuxnet and placed into the root of removable drives, along with a copy of the executable malware. Whenever the removable medium is plugged into a PC, operating systems prior to Vista reads the autorun.inf file and tries to automatically execute the accompanying malware.

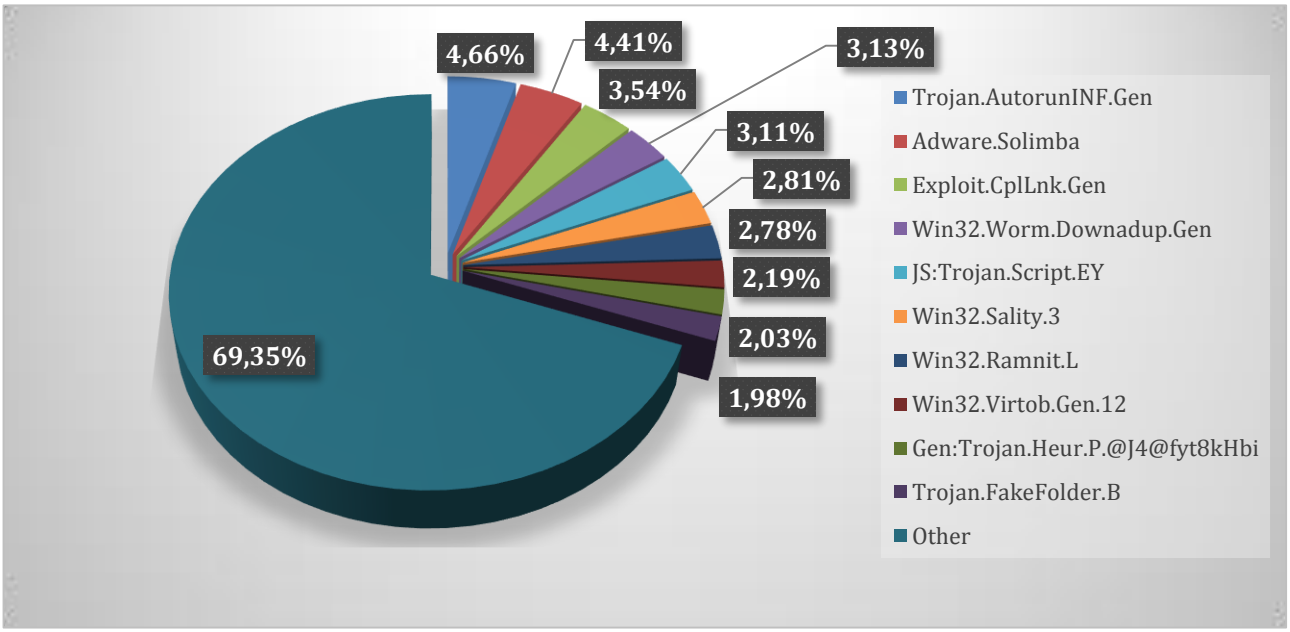


Figure 1: Malware breakdown for H1 2012

© 2012 Bitdefender

2. Adware.Solimba – 4.41% (new entry / new entry)

This generic detection behaviorally flags potentially unwanted installation of third-party software [1] along with the product the user is trying to install. Representative for Adware.Solimba is an executable file written in C# that acts as a downloader. It tries to fetch executable files from the ad network, depending on campaigns. This adware has potentially malicious behavior, as it collects user-data. Adware.Solimba affects the Windows running system ranging from Windows 2000 to Windows 7.

3. Exploit.CplLnk.Gen – 3.54% (-1.12 / previous 3rd position)

Ranking third in this issue of the E-Threat Landscape Report, this detection is specific to .lnk files (shortcut files) that use a vulnerability in the Windows operating system to execute arbitrary code. The vulnerability is caused by the routine that tries to display the icon for the shortcut file. In some cases, when the shortcut points to a module in the Control Panel, the operating system tries to load the module in order to display the icon. This malicious code was used as an infection mechanism in the Stuxnet attack. Since its emergence, it has also been integrated in various families of "homemade" malware as well.

4. Win32.Worm.Downadup – 3.13% (-3.12 / ↓ 2 places)

Downadup is a worm that emerged roughly at the same time as Trojan.AutorunINF. In 2008, it was one of the most aggressive e-threats and managed to compromise more than 12 million computers in just one day. The worm can remotely infect computers on the same network by brute-forcing their administrative credentials and denies access to antivirus sites to prevent disinfection. The worm was used to install rogue AV software on infected computers, among other uses.

[1] Loredana BOTEZATU, Adware Shifts Focus from Advertising to Data Harvesting, [fetched November 20th 2012], the Hot For Security Blog

© 2012 Bitdefender

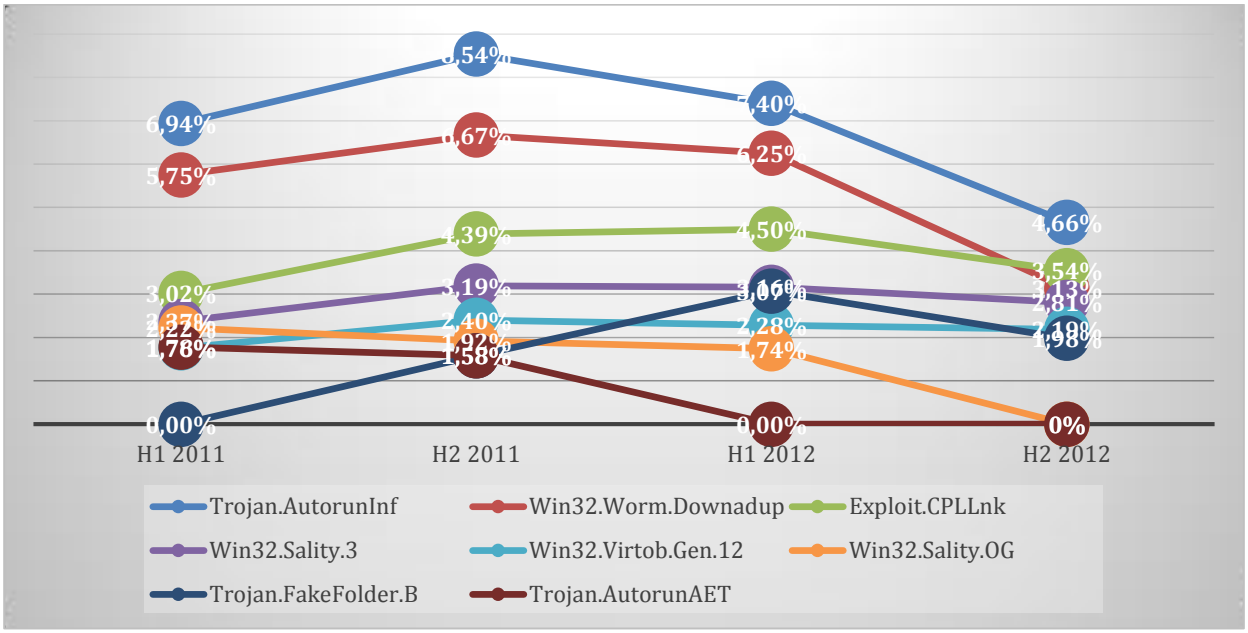


Figure 2: Evolution of the most prominent malware families during the last four semesters. Autorun-based malware is in free-fall.

5. JS:Trojan.Script.EY – 3.11% (new entry / new entry)

Ranking fifth in the Landscape Report top is JS:Trojan.Script.EY - a piece of malformed JavaScript code usually found injected into web pages to redirect users to malicious, third-party websites where exploitation code is hosted.

6. Win32.Sality.3 – 2.81% (- 0.35 / ↓ 2 places)

Win32.Sality.3 is a variant of the famous Sality file infector, a virus whose highly encrypted payload has allowed it to thrive years after its initial detection. The Sality virus comes with a rootkit that shields other files from the user and attempts to disable the locally installed antivirus. Apart from infecting executable files, Sality has a bot component that allows an attacker to completely seize control over the computer and command it remotely.

7. Win32.Ramnit.L – 2.78% (+ 0.1% / -)

Win32.Ramnit.L is also a file infector that adds its malicious code to clean files with specific extensions. It subverts the default browser on the PC by injecting its malicious code into it and opens a communication channel with its master. The virus specializes in stealing FTP

© 2012 Bitdefender

credentials and login cookies, information that is probably used by its creator to host other malware.

8. Win32.Virtob – 2.19% (- 0.09% / previous 8th position)

The Virtob virus is another e-threat that infects executable files with exe or scr extensions. Unlike other aggressive viruses, Virtob does not infect system files so as to avoid crashing the system and rendering it useless. However, it infects user-installed applications and even other malware that may reside on the same computer. It is written in assembly language, which offers it the benefit of speed. This family of malware is polymorphic, which allows it to mutate its code from one infection to another to avoid detection. Like Sality, it opens a backdoor that allows its creator to take control of the PC.

9. Gen.Trojan.Heur.P – 2.03% (new entry / new entry)

Ranking ninth is a generic heuristic detection that intercepts highly encrypted malware associated with e-banking fraud and rogue antivirus or ransomware.

10. Trojan.FakeFolder.B - 1.98% (-1.09% / ↓ 5 places)

Trojan.FakeFolder.B rounds out the malware top for the second half of 2012. It is a component of the Dorkbot Trojan that keeps the malware active in the computer's memory. The Dorkbot Trojan lists the folders on the infected PC, creates a shortcut to them, and then hides them. Whenever the user tries to access the folder, the shortcut starts the malicious component in the Recycler folder.

© 2012 Bitdefender

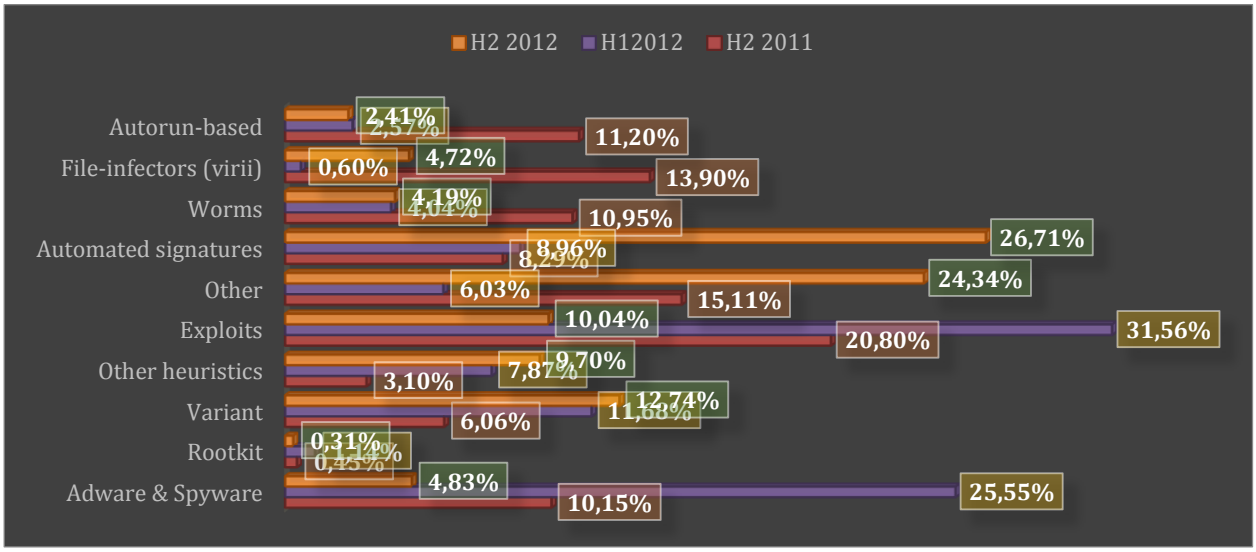


Figure 3: Malware breakdown by signature type

Social Networking Threats

If social networks are usually the way to go when trying to disseminating malicious or spammy links, the second half of the year has been particularly dangerous for social networking users. Apart from the regular scams, some vulnerabilities in the Facebook platform allowed cyber-criminals to syphon mobile phone numbers associated with social network accounts.

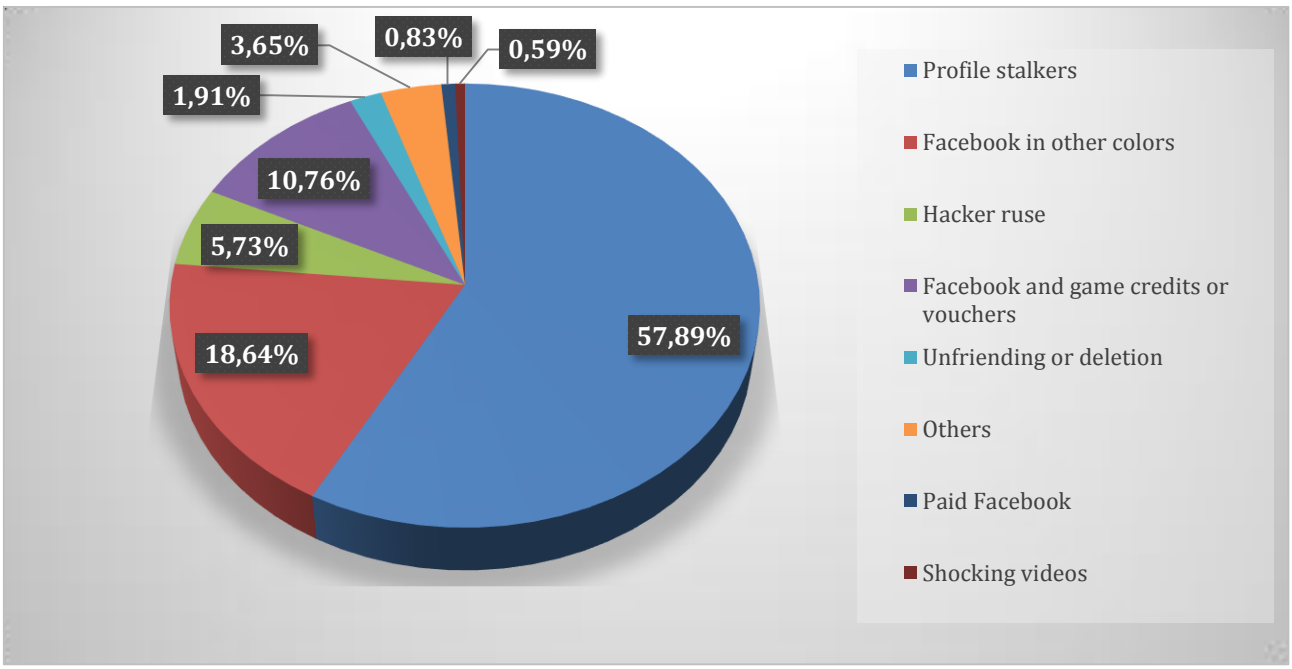


Figure 4: Breakdown by scam type

© 2012 Bitdefender

The most prolific type of scam throughout the second half of 2012 continued to be "see who's stalking you," with variations ("see who viewed your profile" or "Amazing, I can now check my profile visitors").

Free promotions were also a highly appealing take to mislead the users into clicking and sharing malicious links

Third place is taken by scams advertising Facebook in other colors, a scam that cons users into installing a browser toolbar. Even if this toolbar modifies the Facebook style in real time by manipulating the CSS file, it also performs malicious tasks in the background – a technique we described in February on HotForSecurity. Depending on campaigns, these scams are also tag-jacking or leading users into filling in surveys.

The biggest privacy hit in the second half was the documented exploit that allows practically any Facebook user to harvest phone numbers along with the full name of the victim. Back then, Facebook allowed mobile users to find friends based on their phone number, and bruteforcing a range of numbers would yield a database with full names and phone numbers. A savvy attacker could use these details to craft vishing (voice phishing) messages aimed at CEOs and decision makers.

On November 26th, a new wave of messages started popping up on users' walls as Facebook's new privacy rules stirred unrest. The message advised anyone who wants to claim copyright for the information they post to re-publish the statement on their own walls. Even though there was no malicious payload associated with the message, the campaign demonstrates how easy it is for an attacker to manipulate large numbers of users into reposting content by exploiting basic fears.

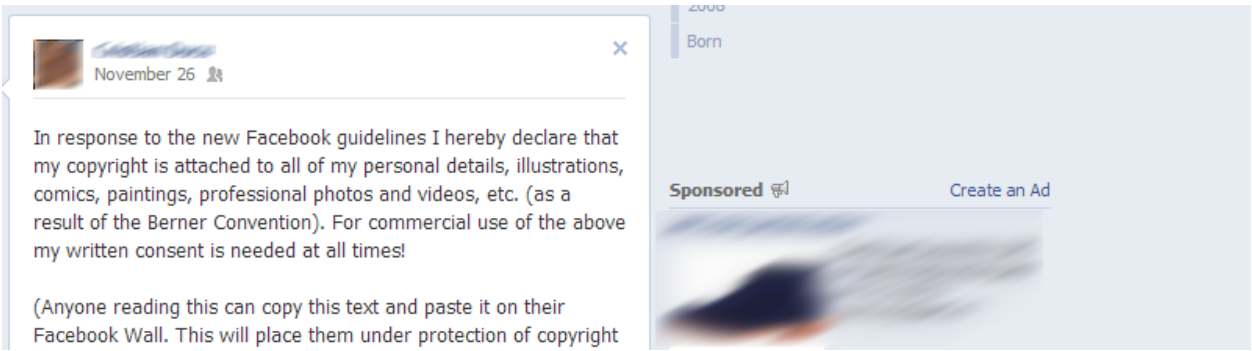


Figure 5: Viral Facebook hoax without malicious payload

© 2012 Bitdefender

Spam Threats in Review

2012 saw some fluctuation in the junk e-mails as a proportion of traffic. The year began with a slight decrease in spam e-mails. Towards the middle of the year, the Antispam lab reported a period of stability, but spam began to grow again in July with small variations towards the end of 2012. The increase in the number of junk e-mails was minor - about 5% - leading to a rough value of 73% of e-mails sent worldwide.

As the most-used language in the world, with millions of people able to speak it or at least understand it, spam messages are most frequently in English. Second position is Russian because a lot of spam campaigns originate in botnets created by Russian-speaking scammers and slanted towards Russian-speaking users. Third ranks the Asian duo of Chinese and Japanese languages with focus on promoting bogus self-development and business trainings or conferences.

These four languages cover 95% of spam sent worldwide, while the other 5% is a joint effort of the rest of the languages, including Italian, Spanish, German or French.

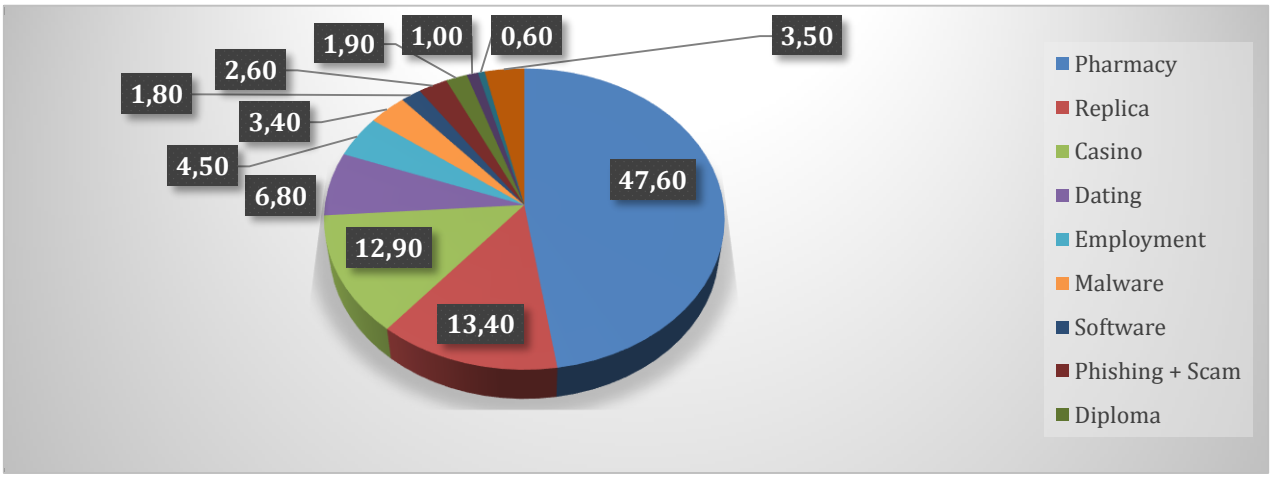


Figure 6: Spam breakdown by type

Even though scammers constantly add new social-engineering maneuvers to trick people with their messages, the old recipes continue in the top positions with offers ranging from the

© 2012 Bitdefender

notorious Canadian Pharmacy sexual enhancement, diet and body-cleansing pills to hard-to-ignore knock-offs, casino discounts or grotesque dating tips from "dating professionals."

1. Viagra spam

Viagra had its ups and downs but one thing is certain - it will never go away. In the last six months, it accounted for 47.6% of all spam sent worldwide. No matter how many botnets go down, the Canadian business still strives to reach users' inboxes with offers such as Viagra, erectile dysfunction pills, penis enlargement products, bio medicine for losing fat in no time without any exercise or diet.

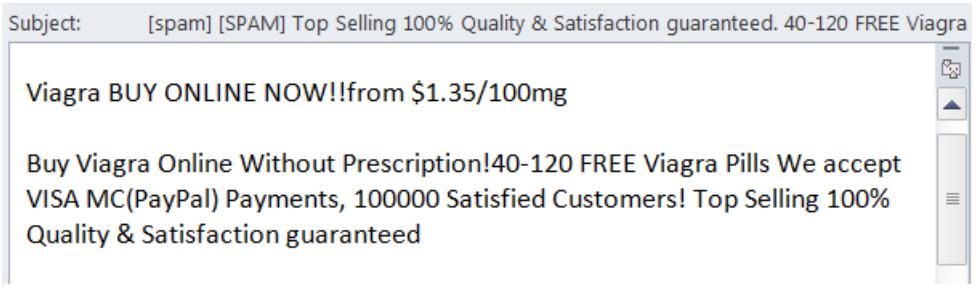


Figure 7: Sample spam message referencing Viagra

2. Replica products

13.4% of all spam sent sells "affordable" luxury products. Advertised as the perfect gift for friends and business partners or promoted as "the status accessory" for a successful person, replica watches, fake bags or jewelries make it to a dishonorable second place in the top of most frequently used spam lures in the last months of 2012. Their presence significantly increased in the last couple **of weeks, probably boosted by the upcoming winter holidays.**

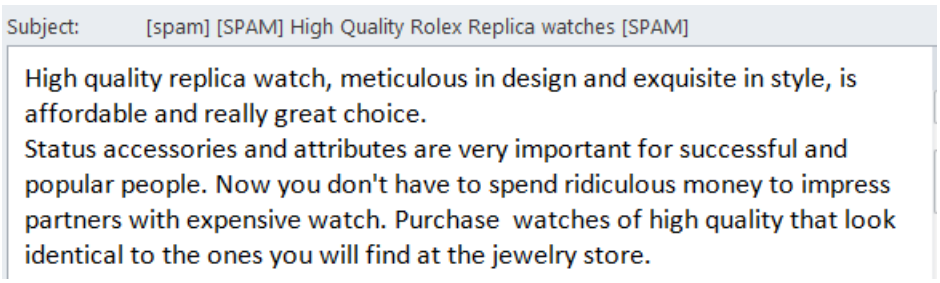


Figure 8: Sample spam message referencing replica products

3. Casino and online games spam

© 2012 Bitdefender

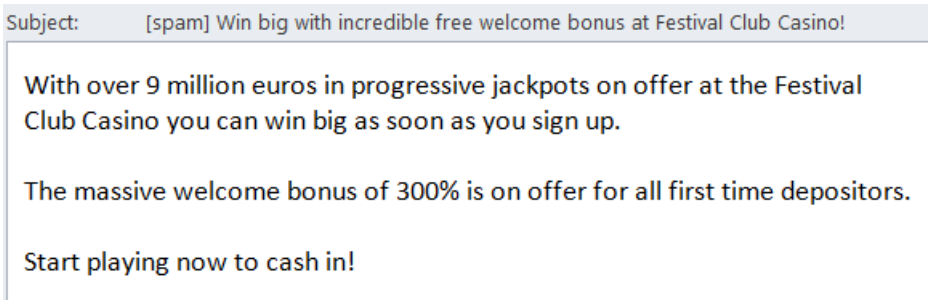


Figure 9: Sample spam message advertising casino activities

Third is the Casino-scam. 12.9% of recent spam lures users to sign up for big wins at the Festival Club Casino. People are charmed with jackpots of 9 million euros that can fill their pockets once they start making deposits. First time depositors are offered a welcome bonus of 300% in some spam campaigns, while in others bringing friends to the table or spamming contacts with referrer links wins players bonus points.

4. Dating spam

Russian dating websites with beautiful women who want to love Westerners still bring a lot of money to scammers, placing this type of spam in fourth place, with 6.8 percent of all spam sent around the globe. These e-mails include links to online dating websites that collect identification data of the gullible men who land on their pages. This data will be used for impersonation, extortion, money muling or future scams.

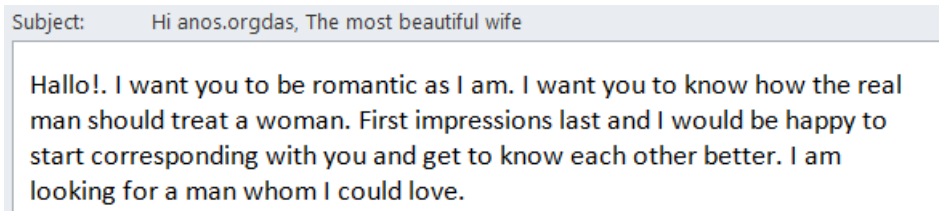


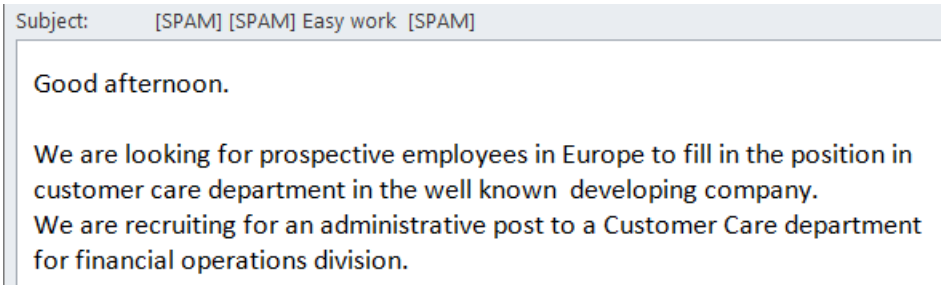
Figure 10: Sample spam message with a Russian Brides twist

5. Easy work

Fifth is the spam wave related to job offers. Users receive, for instance, an ad for an apparently innocent administrator position in a Customer Care department for a financial operations division. This however translates in an unwary person being asked to forward packages or cash money orders. It is a rather easy job that could be done by the employers themselves, if it

© 2012 Bitdefender

were legal. Packages and money usually come from credit card fraud. If police manage to track down the address, unwary users would go to jail, absolving crooks of any blame.


Subject: [SPAM] [SPAM] Easy work [SPAM]

Good afternoon.

We are looking for prospective employees in Europe to fill in the position in customer care department in the well known developing company.
We are recruiting for an administrative post to a Customer Care department for financial operations division.

Figure 11: Money-mule recruitment spam

In the last six months, almost all social, political and meteorological events, Hollywood celebrities, public holidays including Independence Day, Labor Day, Halloween and Black Friday triggered a dedicated spam campaign to persuade people to open e-mails, pay for products and services they will never receive, click links and type in identification data or credit card-related information, only to have their identities stolen and used in other spam campaigns, in money muling or malware dissemination.

Despite numerous warnings from the press and the security community, Nigerian scams remain highly effective to this date and continue to flood users' inboxes with sorrowful stories woven to impress the victim into sending money or account credentials to unknown people. In the meantime, professionals in various fields were again lured with promises of greatness and public recognition in return for a $1,000 dollar fee.

Spam bundled with attachments

E-mail messages delivering attachments, a special category of spam, are used by crooks mainly in Nigerian-type scams (almost 50%), as fill-in forms in numerous phishing attacks or as archived malware samples sent directly into intended victims' inboxes.

© 2012 Bitdefender

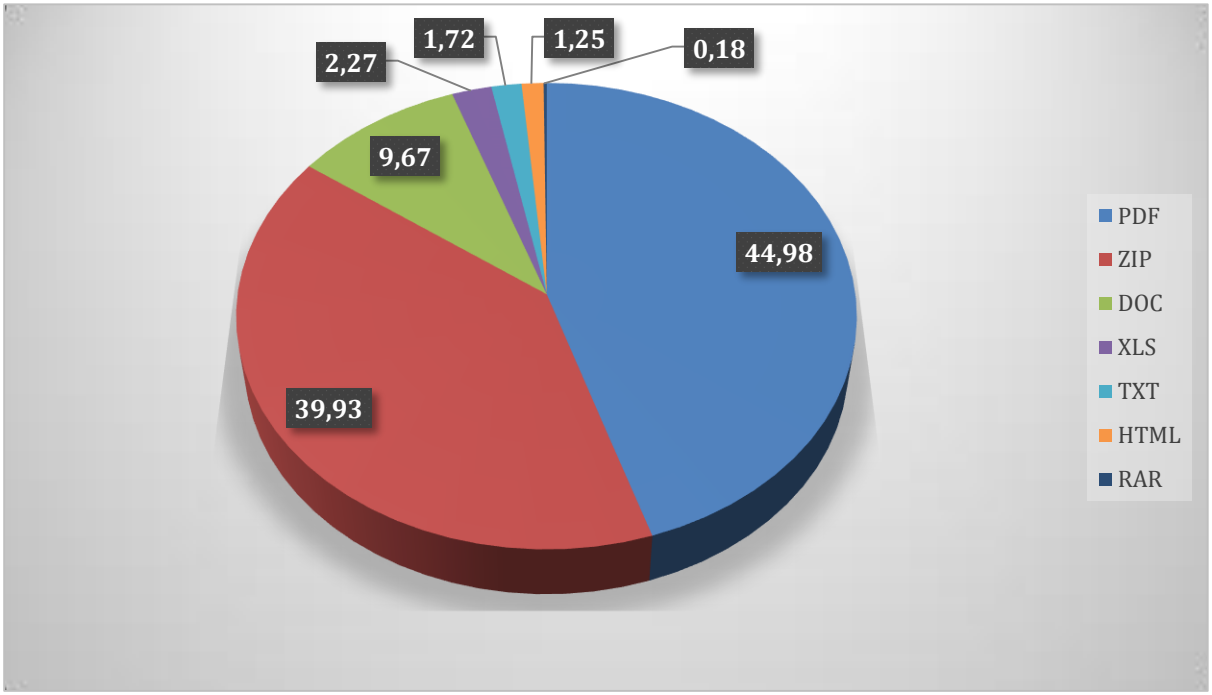


Figure 12: Spam attachment breakdown by type

Spam carrying attachments makes up for 5% of the number of spam circulated in the second half of 2012, registering a discrete yet steady rise from last year.

File extensions found in attachments

Ranging from HTML pages used as acquisition forms in phishing attacks and PDF files bundled with 0-day vulnerabilities to Trojans, viruses and worms archived using zip or rar formats, attachments are dangerous malware-disseminating tools able to reach numerous unwary users' inboxes at once.

E-mails delivering malware in attachments also rose in the second half, adding an extra 1% to the 1.5% increase registered in the first months of 2012, accounting overall for 5 percent from the total of spam with attachments.

The Bitdefender Antispam Lab identifies certain scenarios common to most spam e-mails with attachments. Naturally these aren't the only ones, but are among the most notorious tricks that have been successfully used for years.

© 2012 Bitdefender

1. The official notification asking users to “check their account” because irregular activity was detected with the user’s Internet banking account.
2. The “complaint report” filed by a company customer asking the recipient to take notice and address the issue as soon as possible.
3. The “attached scanned document” carrying a zipped file allegedly a scan made with a Hewlett-Packard machine.
4. The eternal package delivering fail notification with the order details sent in attachment.
5. The compromising photos attached by someone claiming to be a friend.

The notorious BlackHole exploit kit has been constantly popping up in spam campaigns these past few months. Some e-mails spreading this menace via spam had themes such as “PayPal Account Modified”, “American Express Alert: Your Transaction is Aborted”, “Payroll Account Holded by Intuit”, “Your Card Services Blocks” or “Scan from your Xerox machine”.

Scammers mass mail millions of users, impersonating various institutions to trick people into clicking a malicious link, downloading or opening an infected attachment that will expose users to exploits served by a certain version of the BlackHole Exploit Pack. Users with systems vulnerable to the exploit delivered will eventually get infected with a fresh ZBot variant, a banker, a downloader, a keylogger, a backdoor or whatever the scammer chooses to deliver.

Sold underground to attackers of all skill levels, BlackHole lets buyers customize this do-it-yourself cybercrime tool. They can pick from a list the exploit that targets the very vulnerability they want to use in that spam campaign. Exploited vulnerabilities range from old holes people are reluctant to fix to 0-day bugs that have just surfaced in the cybercriminal underworld.

© 2012 Bitdefender

The Android Landscape

Adoption of the Android OS increased rapidly. Android market share rose to 72.4% in the third quarter of 2012 from 52.5% a year earlier as unit sales more than doubled to 122,000 from 60,000, according to Gartner. The number of malware-infected devices soared along with it.

Our Android H2 Landscape report, based on reported detections from July 1 to December 1, revealed an increase of 41.09 percentage points in devices infected.
The total number of malware and adware reports spiked during H2 2012 to 292%, which translates into a 75% increase in the number of reported detections during H2 compared to H1.

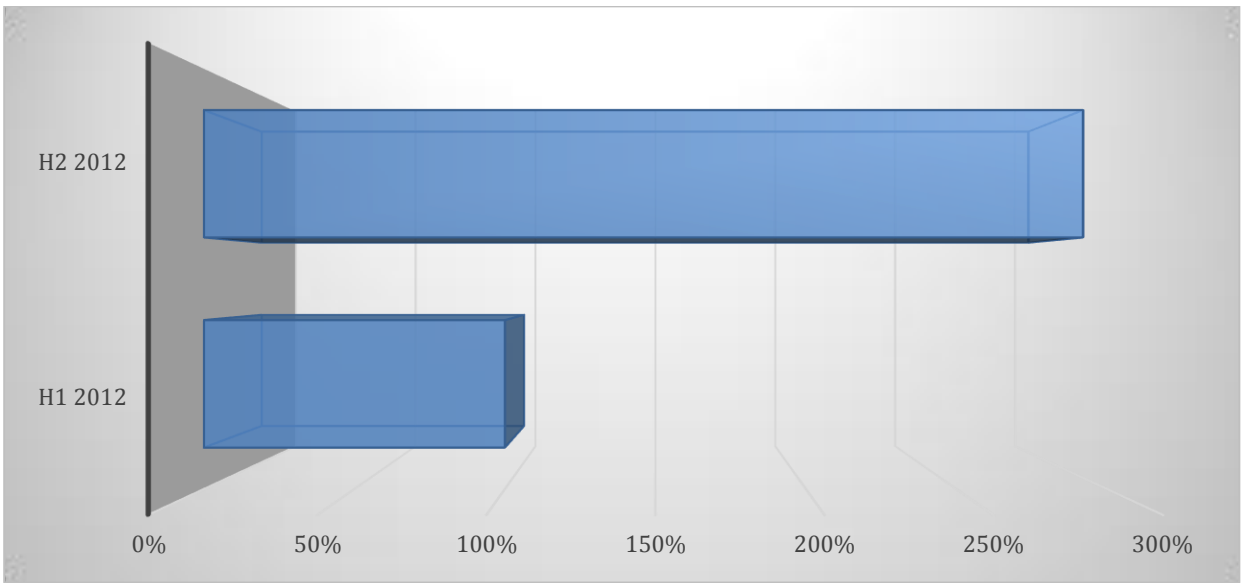


Figure 13: Total Reports in 2012

Although adware is not inherently malicious, aggressive adware can place additional shortcuts on a users' home screen or change the default search engine. Ad notifications are also displayed even if the app is not running, making it hard for users to pin down the app responsible for the aggressive ads. Users may have been notified of the app's intentions, but phone owners don't often thoroughly read app permissions and understand them.

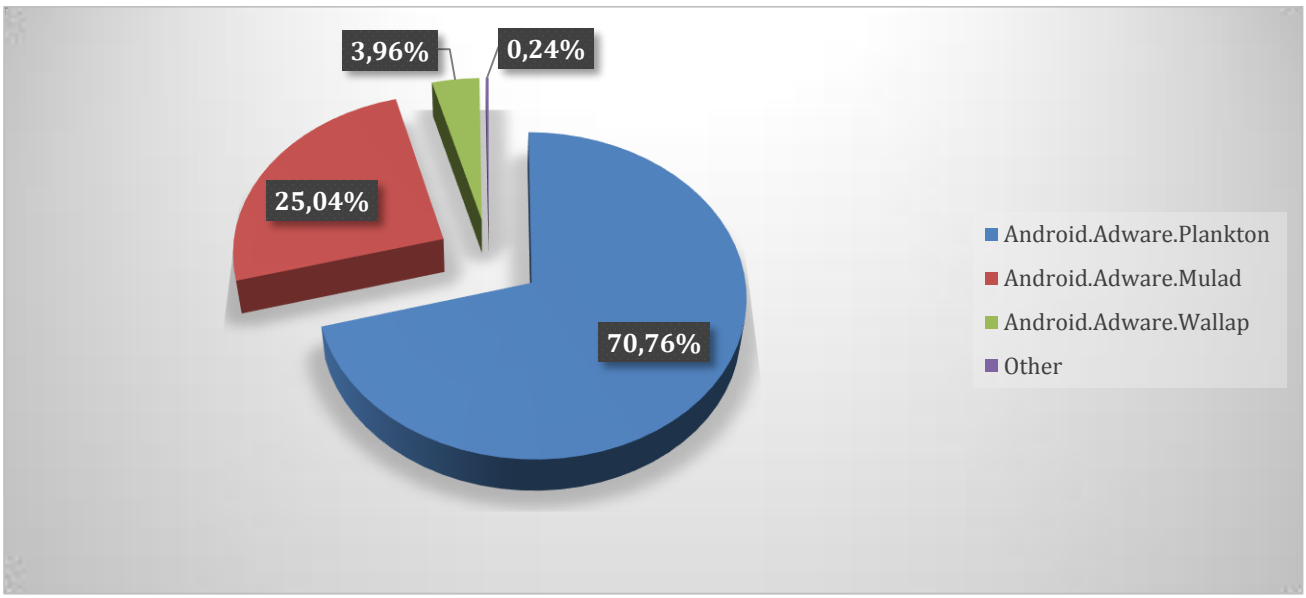
© 2012 Bitdefender

Dominating our Top 10 Mobile Adware for H2 2012, the Android.Adware.Plankton and Android.Adware.Mulad adware families have gained significant traction, clocking in 48.88% of total analyzed samples.

Plankton is mostly found in legitimate apps and developers use it to generate revenue from click-based ads. Mulad is also found in legitimate apps, but some of these apps have no functionality - they just pack several ad libraries to generate revenue. Although adware is a common and benign tool used by developers to generate revenue, abusing it irks users.

With Plankton providing more flexibility in ad placement and control, our analysis concluded that 70.76% of all samples bundled with aggressive adware fall under the Android.Adware.Plankton family.

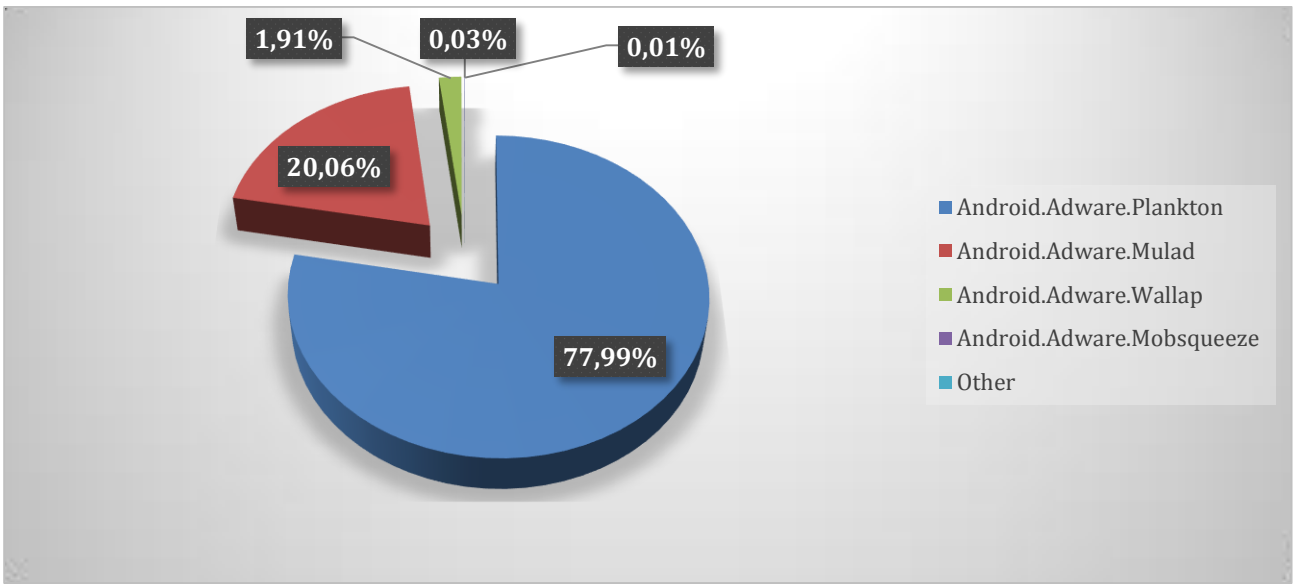
Adware Distribution by Family		
1	Android.Adware.Plankton	70.76%
2	Android.Adware.Mulad	25.04%
3	Android.Adware.Wallap	3.96%
4	Other	0.24%



Illustrating the popularity of Android.Adware.Plankton, 77.99% of all reported adware from the market confirmed it as truly widespread.

© 2012 Bitdefender

Top Adware Family Distribution By Reports		
1	Android.Adware.Plankton	77.99%
2	Android.Adware.Mulad	20.06%
3	Android.Adware.Wallap	1.91%
4	Android.Adware.Mobsqueeze	0.03%
	Other	0.01%



Other types of adware can collect user information to generate a behavioral profile that could be used to serve targeted ads and even be sold in underground black markets to companies that want to target a specific demographic.

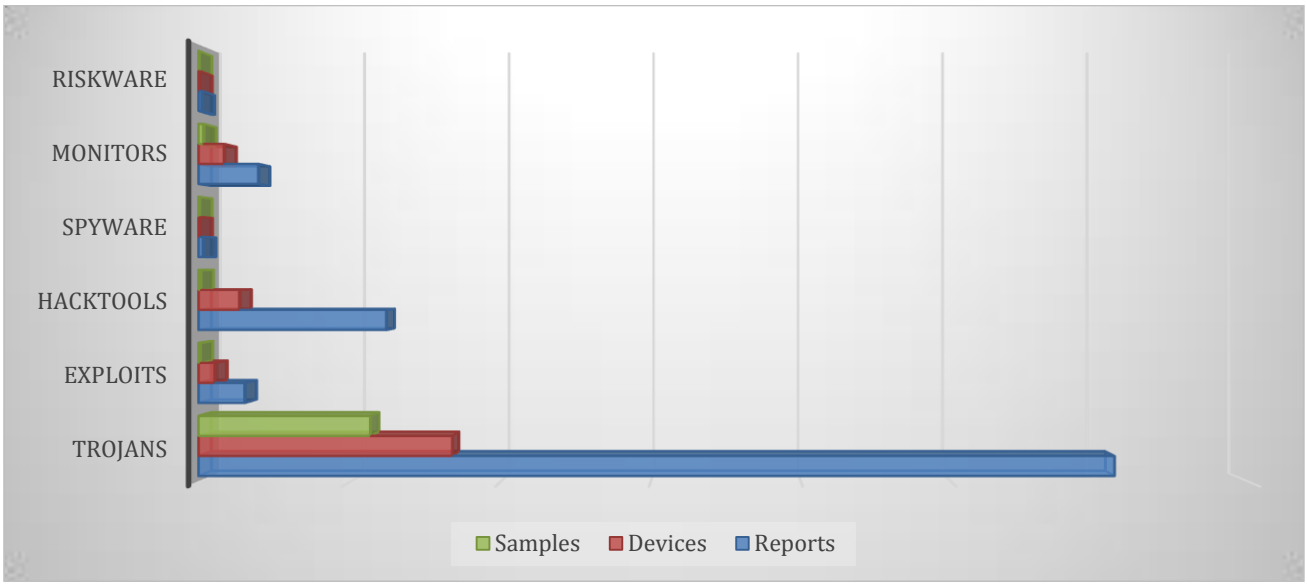
The evolution of Android malware also spiked as third-party app download portals lured an increasing number of users with the promise of interesting apps that sometimes contain malicious code.

From apps that vow to optimize battery performance to games and tools, Android malware is mostly devised to send premium rated SMS messages without users' knowledge. Money appears to have been the main incentive for malware coders and new samples of SMS Trojans have been added to existing malware strands.

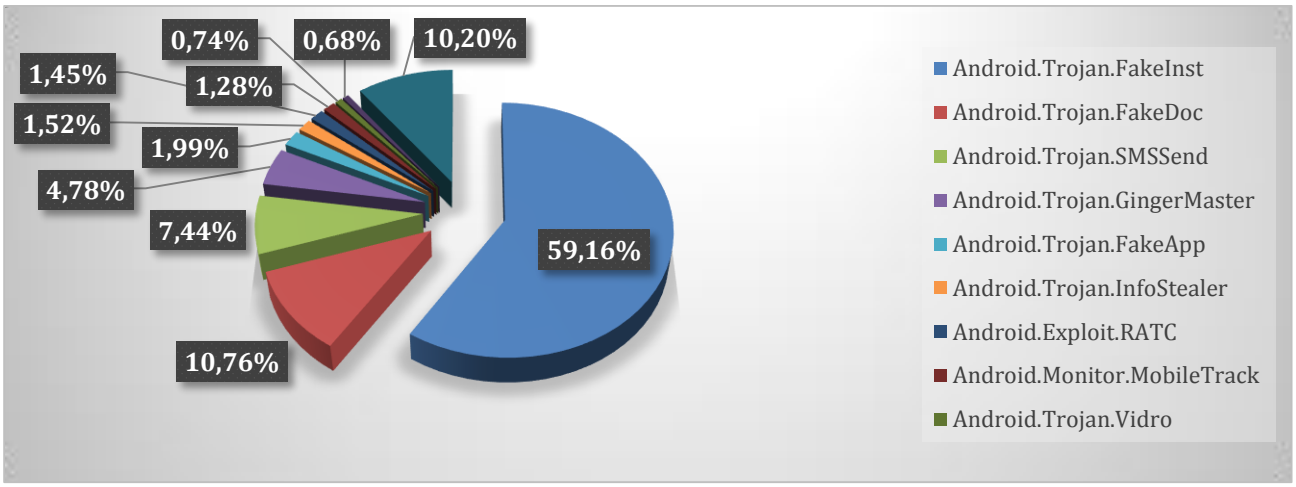
When comparing the number of devices that at one time were infected with malware to the number of unique malware samples and the number of reported malware, we concluded that

© 2012 Bitdefender

Android Trojans amount to 94.35% of all unique malware samples, being spotted on 74.79% of all devices that reported malware.



An interesting breed of Android malware also stands out, powered by malware coders' need to reach deeper into users' pockets. Bitdefender Labs pinned down the Android.Trojan.FakeInst as the malware family most commonly used to scam users by sending SMS messages to premium rate numbers. With a whopping detection rate of 59.16% of all reported detections in the time period, the malware works by pretending to be a legitimate app. Whether the application is truly functional or not, it's probably one of the most profitable Android malware families yet.

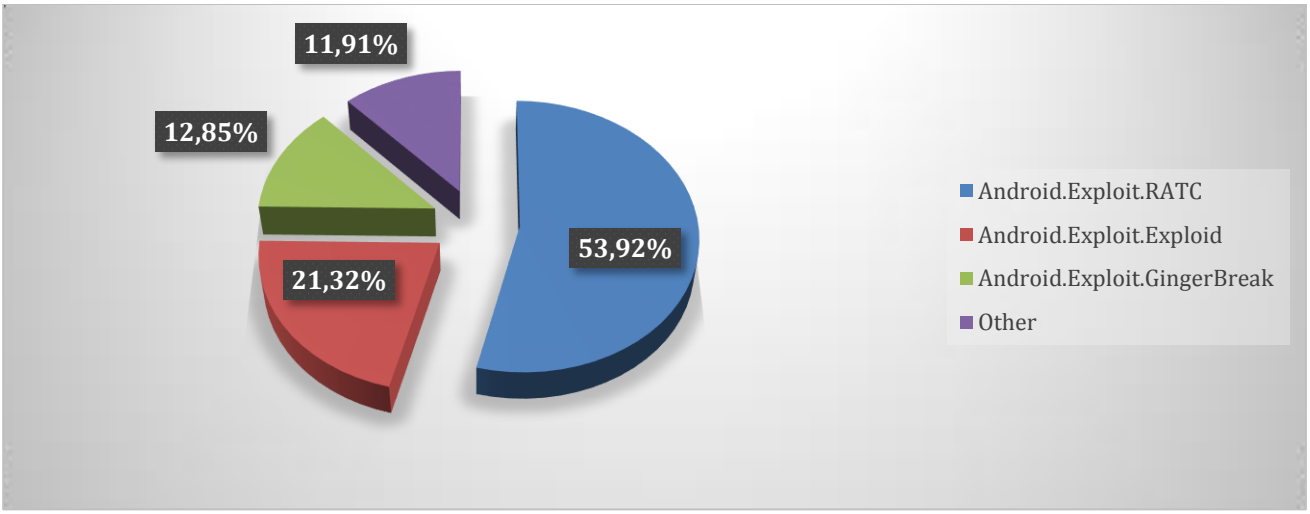


FakeInst is actually short for "fake installer" and it usually offers to install an app, but requires users to agree to pay for it by sending a premium rated SMS message. Although it usually

© 2012 Bitdefender

downloads the app and asks users if they agree to send the SMS, the app it offers to download is usually free - the entire process is a scam to trick users into paying for free apps. However, if users refuse to pay, no premium rated SMS message will be sent.

When looking at a breakdown of some of the most popular Android exploits, we concluded that Rage Against The Cage leads the chart, with 53.92% of analyzed exploit samples. As users are still interested in rooting their Android handsets, the Android.Exploit.RATC family will show up in future charts as well.



With threats in the form of OS vulnerabilities, such as USSD vulnerabilities and other exploits, Android users are advised to exercise even more caution than before when downloading third-party apps, browsing, or engaging in other activities.

H2 Spotlights

It was recently demonstrated that USSD codes can be used against some Android OS builds to trigger a restore-to-factory-settings action. By using a specifically crafted SMS message, QR code or URL link, unsuspecting users could end up having their devices wiped if the default built-in dialer kicks in. Having users’ safety in mind, Bitdefender’s timely release of USSD

© 2012 Bitdefender

Wipe Stopper prevented such codes from being triggered by ill-intended individuals.

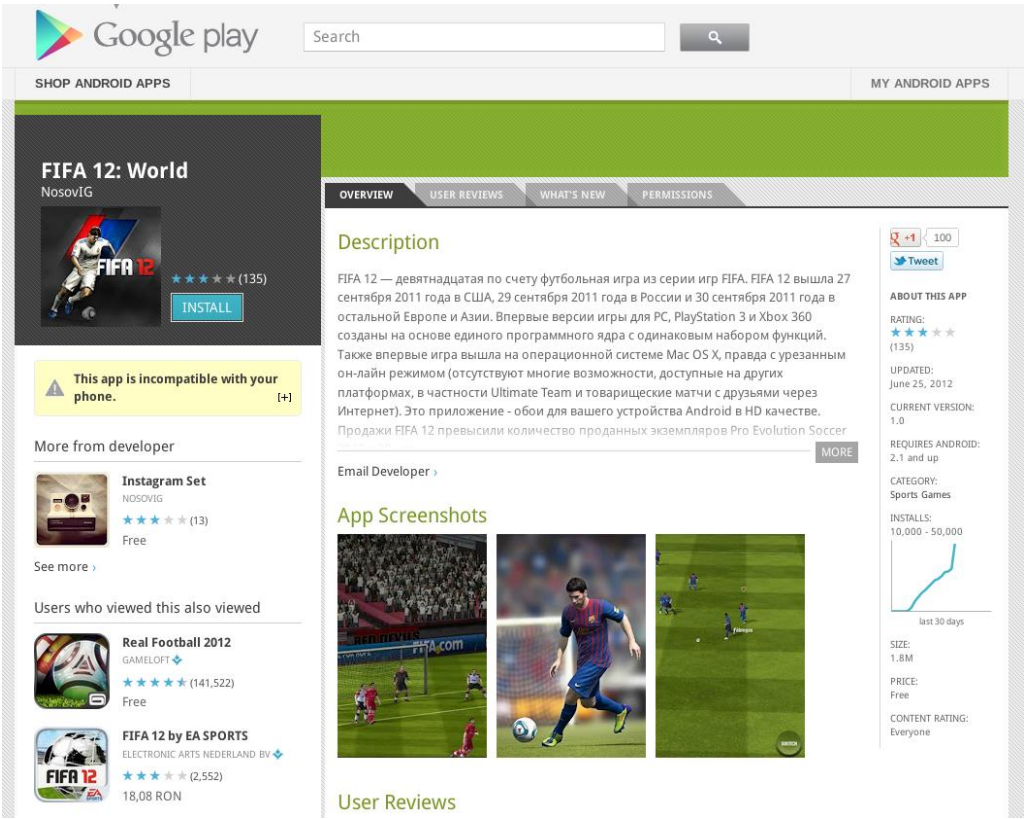
Google and its OEM partners rushed a patch distribution to prevent USSD codes from executing, but not all Android handsets have been updated. Depending on the model and Android build, some users still remain exposed to the vulnerability.

A battery optimization app that caused distress especially in Japan promised to improve users' battery life but instead stole their phone numbers and emails. We've detected the Trojan as Android.Trojan.InfoStealer.D. This was just one of a wide variety of detections that behaved much in the same way.

```
if (Integer.parseInt(localCursor1.getString(localCursor1.getColumnIndex("has_phone_number"))) > 0)
{
  Uri localUri2 = ContactsContract.CommonDataKinds.Phone.CONTENT_URI;
  String[] arrayOfString2 = new String[1];
  arrayOfString2[0] = str1;
  localCursor3 = localContentResolver.query(localUri2, null, "contact_id = ? ", arrayOfString2, null);
  if (!localCursor3.moveToNext())
    localCursor3.close();
}
else
{
  localStringBuilder.append(str2 + ":");
  str3 = "";
  Uri localUri1 = ContactsContract.CommonDataKinds.Email.CONTENT_URI;
  String[] arrayOfString1 = new String[1];
  arrayOfString1[0] = str1;
  localCursor2 = localContentResolver.query(localUri1, null, "contact_id = ? ", arrayOfString1, null);
}
```

To dodge suspicion that they don't actually work, a Japanese message was displayed saying "I am sorry. Your terminal is not available due to unsupported". Other apps with the malware lured users with videos or photos of local female celebrities.

© 2012 Bitdefender



Multi-stage payloads in legitimate Android apps have also been spotted in legitimate wallpaper apps that downloaded an additional .apk file from a Dropbox account. Available in Google Play for a couple of days, Bitdefender Labs spotted three other legitimate-looking apps that promised users the ability to use FIFA or Super Mario wallpapers.

Once the "Activator.apk" was downloaded from the Dropbox account, it sent one or two premium rate SMS messages and then it prompted to be uninstalled to avoid detection.

```
D/download(  413): http://dl.dropbox.com/u/**********/srv.txt : srv.txt
I/dalvikvm(   70): Jit: resizing JitTable from 1024 to 2048
D/activate(  413): download
D/download(  413): http://dl.dropbox.com/u/**********/Activator.apk : activator.apk
D/procedure(  413): end
```

Top 10 Android Malware Threats for H2 2012

Leaving aggressive adware and the FakeInst Trojan family aside, the ranking detection in H2 2012 was Android.Trojan.FakeDoc, which was also the number one threat in our H1 Landscape Report for 2012.

	Top 10 Mobile Malware 2012	
1	Android.Trojan.FakeDoc	24.05%
2	Android.Trojan.SMSSend	16.62%
3	Android.Trojan.GingerMaster	10.69%

© 2012 Bitdefender

4	Android.Adware.Wallap	8.26%
5	Android.Trojan.FakeApp	4.45%
6	Android.Trojan.InfoStealer	3.39%
7	Android.Exploit.RATC	3.23%
8	Android.Monitor.MobileTrack	2.85%
9	Android.Trojan.Vidro	1.65%
10	Android.Trojan.DroidKungFu	1.52%
	Other	23.29%

1. **Android.Trojan.FakeDoc**

The Trojan is known to be a battery optimization that goes by the name of "Battery Doctor". Once installed, it starts broadcasting location, emails and carrier ID to an attacker-controlled server. Android.Trojan.FakeDoc accounted for 24.05% of all reported detections in the last six months and had an increase of 2.45 percentage points from our last report. "Battery Doctor" is unlikely to go away soon.

2. **Android.Trojan.SMSSend**

The Trojan has many variants, but its main goal remains to send premium-rate SMS messages after it sneaks into users' devices. With a detection rate of 16.62% the Trojan ranked second in our malware chart for H2 2012.

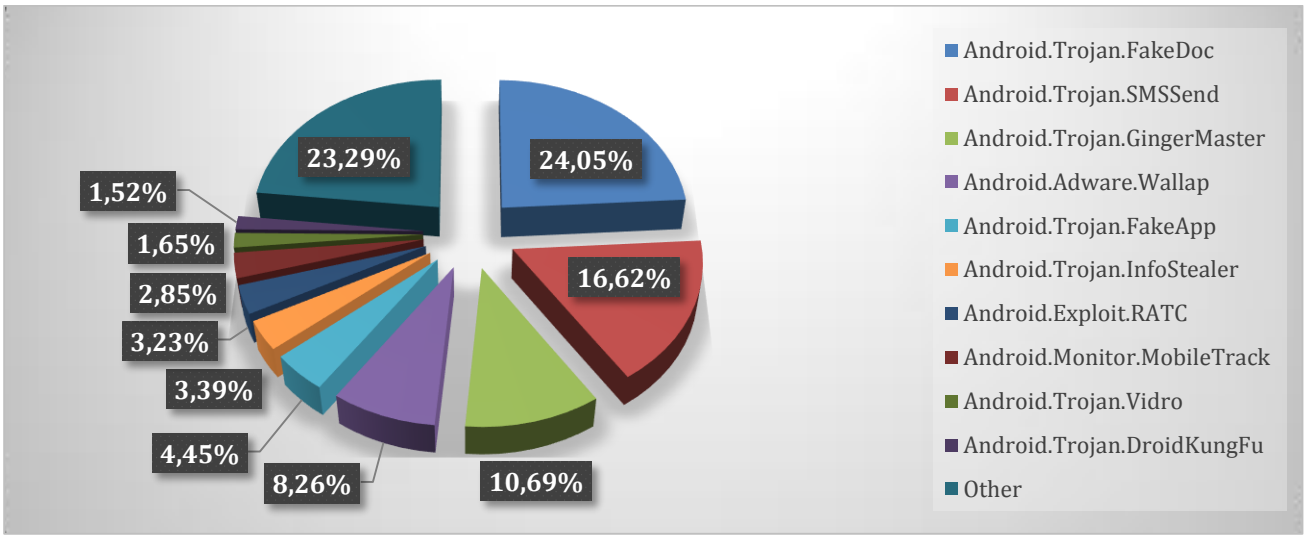
3. **Android.Trojan.GingerMaster**

GingerMaster is a malware that's injected or repacked with legitimate apps. It usually downloads apps from third party marketplaces in the background to increase ranking on specific markets. Mostly found in China, the Trojan artificially boosts the popularity of certain apps by making it seem that lots of users download them. Although end users are not specifically targeted and they don't risk losing any personal data, the Trojan can have significant impact on bandwidth and ultimately rack up phone bills.

4. **Android.Adware.Wallap**

© 2012 Bitdefender

This type of adware is mostly found in apps that promise access to a wide collection of wallpapers. As it's benign, it only uses a wide variety of libraries meant to serve ads so developers can generate easy revenue.



5. **Android.Trojan.FakeApp**

The Trojan usually pretends to do something useful, such as recharge a phone by means of an on-screen solar panel, only to trick them into downloading and installing it. Since it usually features adware as well, it could also broadcast a users' IMEI or location.

6. **Android.Trojan.InfoStealer**

This particular Trojan family collects sensitive user data, such as name, location, phone numbers, emails, and device IDs. Where the information is broadcasted and how it's used afterwards is completely up to the malware coder.

7. **Android.Exploit.RATC**

Also known as "Rage Against the Cage", the exploit is mostly used by Android users who opt to root their devices, thus exposing themselves to obvious threats. While the exploit itself is not malicious and it only enables users to gain "superuser" rights, the same privileges could be used by malware to gain unrestricted access to the devices' resources.

© 2012 Bitdefender

8. Android.Monitor.MobileTrack

Users who want to monitor a device for various reasons often turn to monitoring software that can keep close track of what emails or SMS messages have been sent from a particular phone, or what conversations were carried out. Since apps that fall in this category are perfectly legit, they can also be used to backup emails or SMS messages. However, users should be notified that a monitoring app is installed on their device.

9. Android.Trojan.Vidro

The Trojan is mostly found in the form of video viewing software that promises users access to adult content. Upon install, it broadcasts premium-rate SMS messages at specific time intervals without users' knowledge and blocks text messages coming from specific numbers.

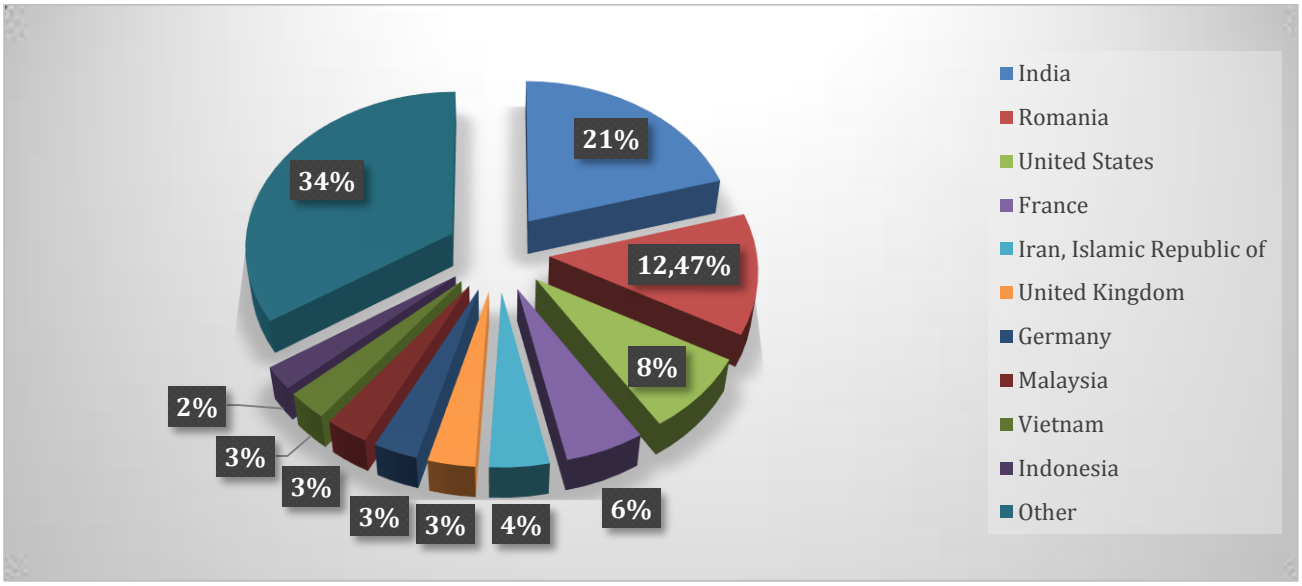
10. Android.Trojan.DroidKungFu

This type of Android malware has the ability to root Android devices by using encrypted root exploits, such as "Rage Against The Cage", gaining the ability to collect data, install/uninstall apps, and grant itself unlimited access to a users' device.

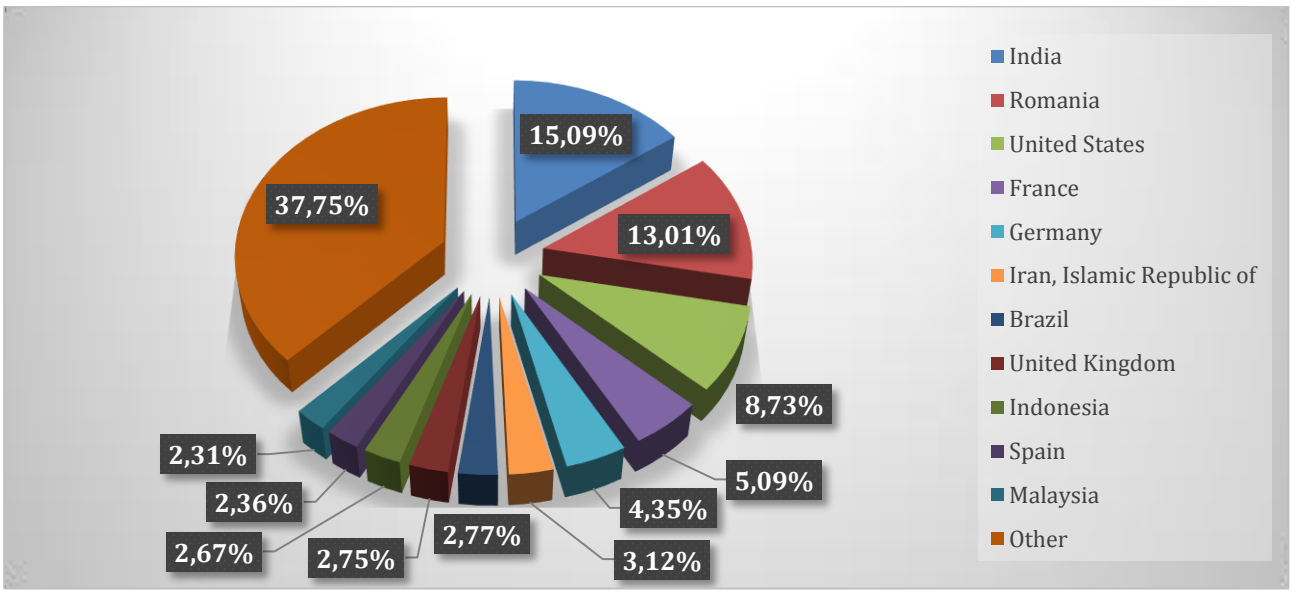
Top 10 Countries Affected By Android Mobile Malware

Malware and adware distribution by analyzing the top 100 countries revealed that most reported detections came from India, which lead the chart with 20.54%. Romania came in second with 12.47%, while the United States, France, and Iran scored between 8% and 4%.

© 2012 Bitdefender



Analyzing the same top 100 countries affected by malware, India reported the largest number of devices that at some point detected malware or adware. Taking a closer look at the distribution of devices that report malware and adware, India ranked first with 15.09%.



Romania came in second with 13.01%, while the United States followed third with 8.73%. France ranked fourth with 5.09% and Iran fifth with 3.12%.

What's Next in the Android Landscape?

As Android malware grows in complexity and number, the urge of malware coders to make money has gained new heights and aggressive adware has become widespread. With

© 2012 Bitdefender

aggressive adware picking up a detection rate of 48.88% of all analyzed samples, it's safe to conclude the ascending curve will continue at least through H1 2013.

In 2013 we will probably see an increase in Android malware disseminated through drive-by attacks and emails, as smartphone and internet adoption increases. With smartphones taking over PC functionalities, such as emails and browsing, Android malware will proliferate.

Although Android 4.2, also known as Jelly Bean, introduces new concepts in terms of security and malicious app detection, it remains to be seen if it will significantly impact malware. However, the new software upgrade will not be distributed to all Android handsets because of obvious hardware limitations and software fragmentation, leaving the vast majority of users exposed to current and future threats.
With third-party marketplaces still popular, we estimate the number of users affected by exploits or Trojans is likely to increase during 2013. Rapid growth of the Android platform will continue to attract more malware coders as devices hold both personal and business-related sensitive data.

Since a growing number of smartphone users surf the web using Android devices and also perform e-payments, we're expecting to see more sophisticated attacks that take aim at users' pockets via premium rate SMS Trojans or other money-stealing techniques.
Concluding that Android malware is disseminated through third-party marketplaces, we encourage users to start using a mobile antivirus solution and also be mindful of what apps they download, and from where.

© 2012 Bitdefender

Future Outlook

The e-threat landscape is continuously shifting to take advantage of new opportunities opened by emerging technologies as well as to meet the increasingly complex demands of cyber-criminals. Apart from the trends we have been observing for the past four years, 2013 will likely bring new dangers to the cyber-world.

Malware shifting to the legitimate software business model

Some modern groups of cyber-criminals are structured in a similar manner with legitimate software vendors. After successfully introducing R&D, testing, marketing and even tech support, cyber-criminals are now taking the game to a whole new level, by internationalization. Modern malware comes translated in multiple languages to cover larger geographic areas and to make the message easier to comprehend to more users. At the moment, some species of ransomware use this technique and we expect to see this become a de-facto standard over the next year.

Attacks against the hypervisor

As virtualization becomes the next big thing for millions of customers worldwide and businesses and services move to cloud-based virtual environments, cyber-criminals will try to find new ways to subvert the entire server and the virtual machines running on top of its hypervisor.

New mobile OS, new troubles

Android malware will continue its exponential boom throughout 2013. The next year will also bring the Firefox OS, a brand-new operating system built on open web-standards. According to estimations, the Firefox OS will have a market share of about 2% by the end of the year – a user base that will be exposed to whatever design flaws the new OS might have.

Old threats going down, new threats surface

As Windows 7 has finally overtaken long-runner Windows XP in market share, the e-threat landscape will witness significant changes. Most likely, Autorun-based threats will go extinct in the last quarter of 2013, along with the notorious Downadup / Conficker worm. Their

© 2012 Bitdefender

places will be claimed by generic – yet intrusive – adware, and by rootkit-based infection mules such as the ZeroAccess.

Infected PCs, electronic currency miners

As Bitcoins become increasingly important in the global economic ecosystem, cyber-criminals will likely envision novel approaches to Bitcoin mining on compromised computers.

Windows 8 and UEFI

The release of Windows 8 will likely translate into significant adoption of the UEFI technology, a BIOS replacement that has been around for years, but that failed to get traction until now. As more and more PCs and laptops are built on UEFI-based motherboards, cyber criminals will likely shift their attention to a much more permissive environment than the obsolete BIOS.

Windows 8 will also be a target itself. Throughout 2013, Windows 8 is expected to overtake Windows Vista in terms of market share and cyber-criminals will likely go hunting for platform-specific vulnerabilities, be they at the kernel level or at the web-browser's surface. However, these specific vulnerabilities will not get used in the wild until the newest OS from Microsoft gains real traction.

© 2012 Bitdefender