



**Bitdefender<sup>®</sup>**

# H2 2011 E-Threat Landscape Report

Author

**Bogdan BOTEZATU** – Senior E-Threat Analyst

Contributors:

- **Loredana BOTEZATU** – Communication Specialist (Malware Trends)
- **Răzvan BENCHEA** - Malware Analyst
- **Dragoș GAVRILUȚ** - Malware Analyst
- **Alexandru Dan BERBECE** - Database Administrator
- **Adrian MIRON** - Spam Analyst
- **Tudor FLORESCU** – SafEgo Database Administrator

# Table of Contents

- Table of Contents ..... 3
- Table of Figures..... 4
- Overview..... 5
- Malware Spotlights ..... 6
- Malware Threats in Review ..... 7
  - Top 10 E-Threats for H2 2011 ..... 7
- Web 2.0 Malware..... 13
  - Instant Messenger Malware..... 13
  - Social Networking Threats..... 15
- Spam Threats in Review ..... 17
- Phishing and Identity Theft..... 20
- Vulnerabilities, Exploits & Breaches ..... 22
- E-Threat Predictions..... 24
  - The introduction of HTML5 ..... 25
  - IPV6 and the end of the Internet..... 25
  - Windows 8 and zero-day exploits ..... 25
  - Targeted phishing attacks based on social-network shared data ..... 26
- Disclaimer ..... 26

# Table of Figures

|  |    |
|--|----|
| Figure 1: Top 10 most active families of malware .....   | 8  |
| Figure 2: Breakdown of Malicious Code Types .....  | 12 |
| Figure 3: Specially-crafted data packets trigger the exploitation .....                              | 13 |
| Figure 4: Various spam messages leading to adult content .....                                       | 14 |
| Figure 5: IM conversation leading to premium-rate SMS service .....                                  | 15 |
| Figure 6: Malicious link impersonating video content and leading the user outside of Facebook™ ..... | 15 |
| Figure 7: Scam breakdown provided by SafEgo.....   | 16 |
| Figure 8: Adult service ad promoted by a follow-everybody bot.....                                   | 17 |
| Figure 9: Spam breakdown by category .....   | 18 |
| Figure 10: Pharmacy-related spam message - simple e-mail template including one link.....            | 18 |
| Figure 11: Job offerings: fencing products bought through CC fraud.....                              | 19 |
| Figure 12: Malware-bundled spam message pointing to malware .....                                    | 20 |
| Figure 13: Phishing incidents between January and December 2011 .....                                | 21 |
| Figure 14: PayPal phishing campaign: “You’ll find out why you’re blocked when you log in” .....      | 22 |

# Overview

Twenty years ago, a revolutionary means of electronic communication was born. It would become so popular with all ages and professions that it is still the most used data communication mechanism even today: introducing the SMS – the short message service.

Today, mobile phones are more than bulky gadgets that can move voice and messages from one point to another: they are must-have gear in a World 2.0 – so powerful and so complex, running their own operating systems and, consequently, facing their share of cyber-trouble.

While the first six months of 2011 were marked by software vulnerabilities and high-profile data breaches, the second half cast the spotlight on not only a new family of malware, but also uncovered a user espionage scandal that apparently involved an array of mobile phone carriers and the controversial software vendor CarrierIQ.

The malware landscape was dominated by Trojan.Autorun.Inf and Win32.Worm.Downadup, two malicious contenders that have roots in the Windows XP era, but managed to keep their places even though operating system upgrades or applying patches would have solved security issues exploited by these pieces of malware. The top contenders for H2 2011 are Trojan.AutorunInf, Win32.Worm.Downadup, and Exploit.CplLnk.

Data breaches attributed to the Anonymous gang and its satellite hacking groups continued throughout the second half of 2011. Among the most important targets were Mitsubishi Heavy Industries, Adidas, RIM, Tiroler Gebietskrankenkasse, Nexon and even the United Nations.

Corporate trust also came under close scrutiny, as the DigiNotar incident in H1 2011 exposed unwary users to a massive phishing attack that used stolen digital certificates generated for high-profile institutions and government agencies such as Google, Tor, CIA and Israel's Secret Service, the Mossad.

Social networks have also played a key role in disseminating malware and spreading fake news about the deaths of high-profile personalities such as Muammar Gaddafi or Steve Jobs. Of particular importance were the malicious campaigns built around the alleged movie of Gaddafi's execution and the commemorative giveaway in honor of the late Steve Jobs.



**Fake iPhone giveaway message to commemorate the death of Steve Jobs.**

## Malware Spotlights

- Though patched in 2008, the Autorun feature continues to be the most abused technology across the Windows operating systems. Following in the autorun family's footsteps, the Downadup worm ranks as the second-most destructive e-threat for H2 2011. An interesting aspect of the e-threat landscape is that these two pieces of malware continue to wreak havoc although their code hasn't been updated in years and the cyber-criminal gangs who created them have likely gone extinct.
- Social networks and compromised websites have been two of the most important vectors of infection. Facebook's nearly 800 million users have been constantly lured into clicking on "flashbang" stories (highly viral social engineering schemes leading the victim outside the social network). At the same time, the situation of a couple of second-level domain services such as .co.cc and .co.tv harboring web-based exploit kits has escalated in such a manner that it forced giant search-engine Google to de-index the entire .co.cc spectrum. As cyber-crime was moving on to other free SLDs and blacklisting the .co.cc space proved ineffective, the .co.cc second-level domain has been added back to the Google index.
- Malware-bundled spam that gained ground in the first half of 2011 continued to increase rapidly. The most significant spam waves bundled with malware would

impersonate notifications from The Automated Clearing House, a financial service offered by the U.S. electronic payments association NACHA. Upon opening the attachment, a generic downloader fetches a variant of Zeus from the Web and installs it on the local machine.

- Mobile phones running an Android operating system have seen new threats emerging in the second half of 2011. Advanced pieces of malware such as the Android System Message utility that records incoming and outgoing conversations or the jSMShider Trojan that siphons out incoming SMS messages. In late December, Google also pulled out 22 different applications from the Android Market after confirmed suspicions that they were exploiting a vulnerability of the OS to trick users into sending SMS messages to premium-rate phone lines. These applications were downloaded more than 14,000 times before they got pulled out.

## Malware Threats in Review

The malware top for the first half of 2011 has suffered a variety of modifications, but the most important is related to Downadup losing ground in favour of software cracks. Another significant presence in the half-year malware top is Exploit.CplLnk.Gen, a generic routine that intercepts the Control Panel exploit used by the incipient variants of the Stuxnet worm.

### Top 10 E-Threats for H2 2011

While it is relatively true that the e-threat landscape remained relatively unchanged as compared to the first half of the year, H2 2011 brought up a new piece of malware that has not made it in the top 10 e-threats, but it cannot be left aside due to its complexity and importance.

Dubbed Win32.Worm.Duqu.A, the e-threat discovered on September 1<sup>st</sup> 2011, is much more than the average e-threat: its rootkit components bear a striking resemblance to another notorious piece of malware: Stuxnet. Bitdefender revealed similarities between Stuxnet and Duqu, including the fact that they both rely on zero-day Windows kernel vulnerabilities, and are signed with valid, yet stolen, digital certificates

However, unlike Stuxnet, Duqu has a more down-to-earth mission, namely setting up a covert environment for a regular keylogger, rather than aiming at sabotaging nuclear facilities.

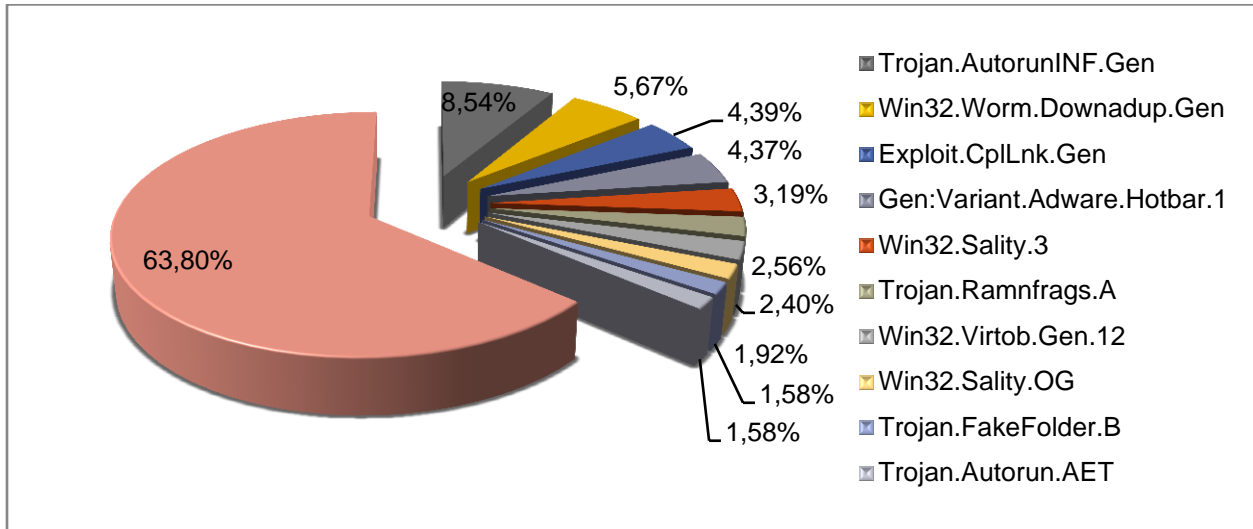


Figure 1: Top 10 most active families of malware

## 1. Trojan.AutorunINF.Gen

Dating back to 2009, Trojan.AutorunINF.Gen is a generic detection that intercepts rogue autorun.inf files, which are usually used by malware to allow them auto-execution from removable media such as USB sticks and memory cards. At the moment, most worm families have a specialized routine that infects mounted removable drives with copies of the payload, and then create a highly-obfuscated autorun.inf file that starts the worm as soon as the infected drive has been plugged in. Win32.Worm.Downadup, Stuxnet, or variants of OnlineGames are only a few of the many families of malware abusing the Autorun feature.

## 2. Win32.Worm.Downadup.Gen

One of the most persistent worms of all time, Win32.Worm.Downadup, has managed to hold its position since early 2008. This piece of malware was designed by a team of professionals with in-depth knowledge of the operating system as it exploits a vulnerability in the Microsoft Windows Server Service RPC (also known as [MS08-67](#)) to propagate. If it has successfully infected the PC, it denies the user access to antivirus vendor websites, as well as to forums focused on malware removal and computer troubleshooting. It has been used as a vector for rogue antivirus and other e-threats due to its viral propagation capabilities.

Ranking second in the Bitdefender malware top for the first half of 2011, Trojan.Crack.I is an e-threat bundled with various “cracks” designed to defeat commercial protection of shareware applications. This e-threat is particularly prominent in countries with increased rates of piracy, including Romania, Spain and France. Apart from generating the desired license key for various commercial applications, Trojan.Crack.I attempts to download specific files from the web and run them on the local machine, which may result in additional malware being installed. This e-threat is new to the Bitdefender E-Threat Landscape Report, but jumps straight to second place with 6.62 percent of the global infections.

## 3. Exploit.CplLnk.Gen

Exploit.CplLnk.Gen is a piece of malware that needs no introduction. The detection identifies malicious code used by the notorious Stuxnet worm to launch itself whenever an infected USB drive has been plugged in. Rather than using an Autorun-based approach, the worm uses lnk (shortcut) files that make use of a vulnerability in all Windows® operating systems to execute itself. Previously ranked fifth in the H1 2011 top, Exploit.CplLnk.Gen gained three positions, with 4.93% of the total number of infected PCs.

## 4. Gen:Variant.Adware.Hotbar.1

Gen:Variant.Aware.Hotbar.1 is a generic routine that intercepts a family of adware applications trying to push advertisements on users' desktops. This class of adware generates revenue for its creator either by displaying contextual advertisements in the users'

browser, or by pushing these ads directly on the top-right corner of the desktop. In order to increase the ads' relevance, Gen:Variant.Adware.Hotbar.1 monitors and logs users' surfing habits and creates user navigation profiles. This e-threat has kept its previous position in the Bitdefender e-threat top.

## 5. Win32.Sality.3

Fifth in the H2 2011 e-threat malware, topWin32.Sality.3 scores 3.19 percent of the global infections. This family of viruses is known for the brutality of the attack: they start infecting all scr and exe files they find on the PC, including files stored on remote drives (drives on other PCs which are shared over a network). Whenever a scr or exe file is found, the virus adds its heavily encrypted malicious code to the respective file.

To evade AV detection, the virus also plants a rootkit component that attempts to annihilate the locally installed antivirus, opening the way to a third component - a backdoor that allows an attacker to seize control over the infected PC.

## 6. Trojan.Ramnfrags.A

Trojan.Ramnfrags.A is a new addition to the Bitdefender malware top. Ranking sixth with 2.56 percent of the total number of infections for H2 2011, this e-threat is a dll file that acts as the main component of the notorious Ramnit virus. This virus infects Windows executable files and HTML files, and can also spread to removable drives. Among other features of Ramnit, it can lift Facebook credentials and use them to spread infected links on users' walls.

## 7. Win32.Virtob.Gen.12

The Virtob virus is the second most spread file infector after Sality. Unlike the latter, Virtob is highly optimized for speed and size, as it is written in assembler language. Just like Sality, it infects both scr and exe files, but skips system files in order not to damage the operate system. This approach allows it to run undetected for longer periods, as the operating system stays free of errors. Whenever a connection to the Internet is detected, the virus uses the IRC protocol to connect to a server of choice, where it waits for instructions from its

creator. Successful infection with Virtob would result in massive compromise of the accounts the user has ever logged on to, as the virus is able to steal files, cookies, passwords or other critical information.

## 8. Win32.Sality.OG

Win32.Sality.OG is a variant of the Win32.Sality virus and ranks eighth with 1.92 percent of the globally-recorded infections during the first half of 2011. This e-threat has all the features described in the note on Win32.Sality.3, but uses an older encryption algorithm.

## 9. Trojan.FakeFolder.B

Ranking ninth in the H1 2011 E-Threat Landscape Report, Trojan.FakeFolder.B is responsible for 1.58 percent of the infected computers around the world. This newcomer is actually a specially-crafted shortcut file belonging to the Dorkbot family of malware. For every folder on the infected PC, Dorkbot creates a shortcut and hides the original folder. When clicked, the shortcut opens both the original folder and the malicious component located in the Recycler folder.

## 10. Trojan.Autorun.AET

Trojan.Autorun.AET ranks last in the H2 2011 E-threat Landscape Report with 1.583% of the total infections worldwide. This is a specific detection to autorun files created by the Downadup worm, which allows the malware to load its payload whenever that specific removable drive is accessed.

| Malware top for July – December 2011 |                             |                     |
|--------------------------------------|-----------------------------|---------------------|
| 01.                                  | TROJAN.AUTORUNINF.GEN       | 8.54% (H1: 6.94%)   |
| 02.                                  | WIN32.WORM.DOWNADUP.GEN     | 6.67% (H1: 5.75%)   |
| 03.                                  | EXPLOIT.CPLLNK.GEN          | 4.39% (H1: 3.02%)   |
| 04.                                  | Gen:Variant.Adware.Hotbar.1 | 4.37 (H1: 5.49%)    |
| 05.                                  | WIN32.SALITY.3              | 3.19% (H1: 2.37%)   |
| 06.                                  | TROJAN.RAMNFRAGS.A          | 2.56% (H1: -)       |
| 07.                                  | Win32.Virtob.Gen.12         | 2.40% (H1: 1.76%)   |
| 08.                                  | Win32.Sality.OG             | 1.92% (H1: 2.22%)   |
| 09.                                  | TROJAN.FAKEFOLDER.B         | 1.58% (H1: -)       |
| 10.                                  | TROJAN.AUTORUN.AET          | 1.583% (H1: 1.78%)  |
| 11.                                  | OTHERS                      | 63.08% (H1: 62.16%) |

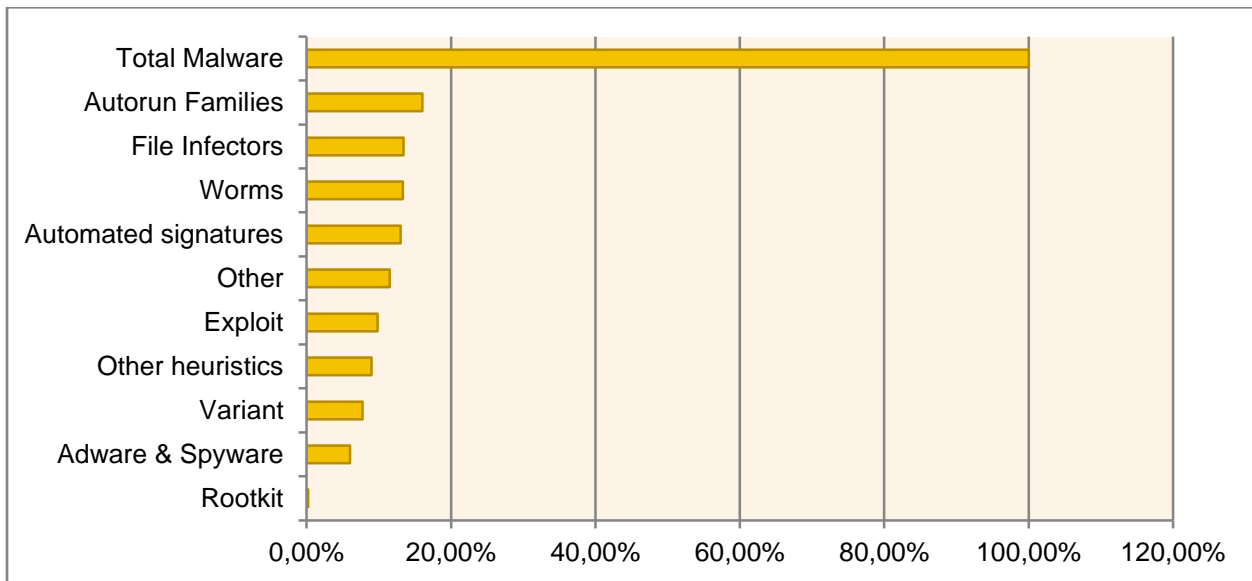


Figure 2: Breakdown of Malicious Code Types

Autorun-based malware was the most prevalent type of e-threat as of December 2011, with 16.04% of all malware types, followed by file infectors (viruses) and worms. Rootkits are situated at the opposite end, with only 0.2% of all malware in the world.

# Web 2.0 Malware

Social networks were the target of a wide range of e-threats during the second half of 2011. Personal information theft and dissemination of malicious links have been the key concerns for cyber-criminals, but spamming for financial gain also witnessed major developments.

## Instant Messenger Malware

Instant messenger malware is not new: over the years, cyber-criminals took advantage of nearly every instant messaging platform to disseminate malicious links or spam their products as part of massive affiliate marketing campaigns. However, the second half of 2011 brought new dangers for computer users running the popular Yahoo Messenger client.

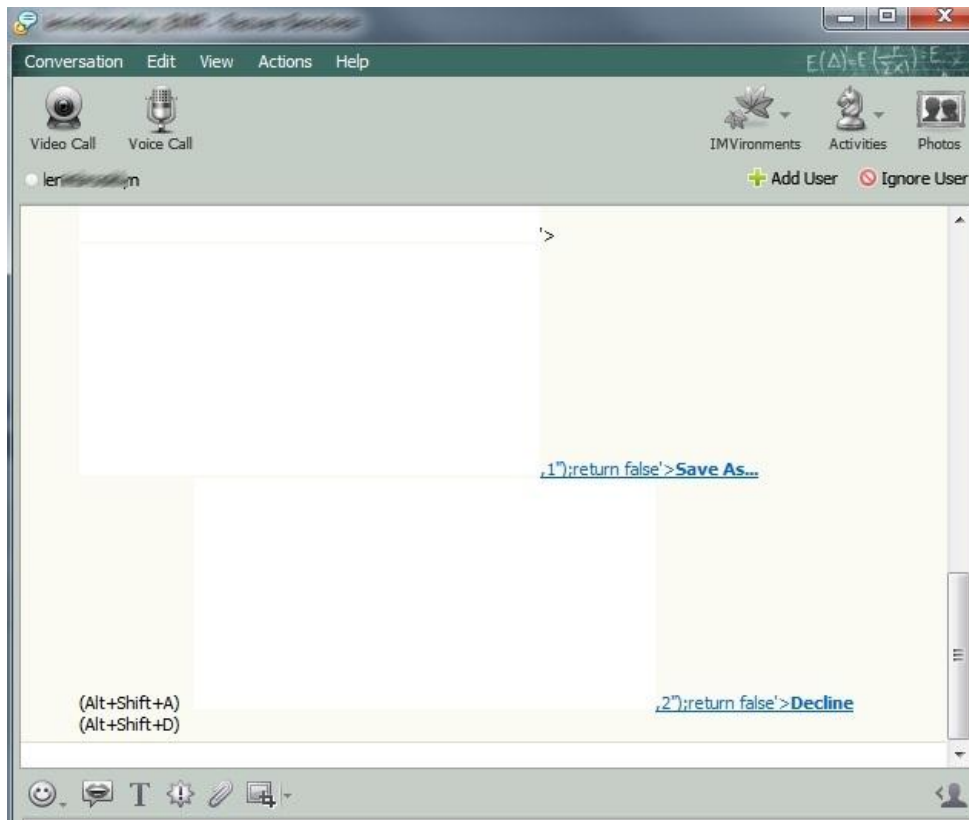


Figure 3: Specially-crafted data packets trigger the exploitation

This exploit has been detected in the wild on December 5<sup>th</sup> and affected version 11.x of the Messenger client (including the freshly-released 11.5.0.152-us), Successful exploitation of the client allows a remote attacker to arbitrarily change the status message of virtually any Yahoo Messenger user that runs the vulnerable version.

The exploit relies on the fact that the Messenger application does not check to see if a specific input is valid, so a malformed file transfer request can trigger any action supported by Yahoo Messenger, including status changes, contact information exports and even accessing a remote location via the default browser.

Spamming through the IM application has also increased during the second half of 2011. Most of the links passed through IM were advertisements to online dating services or other websites with adult content

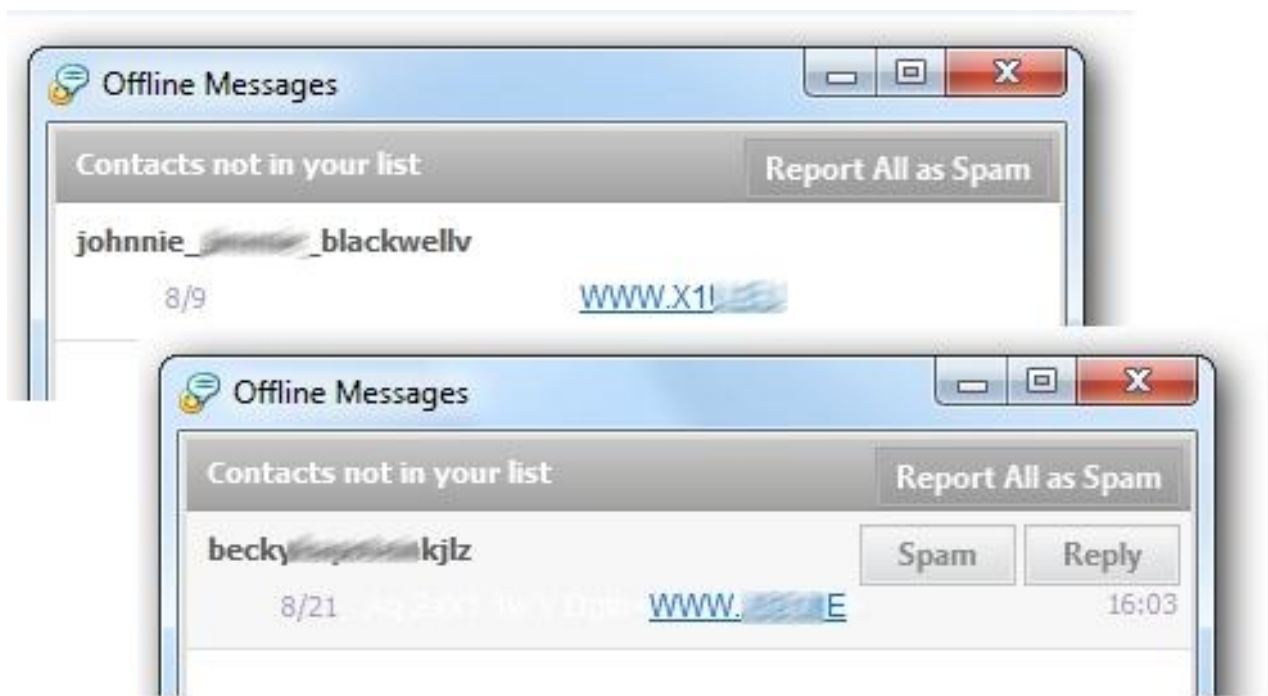


Figure 4: Various spam messages leading to adult content

Other significant spam waves carried on Yahoo Messenger advertised dubious business proposals and contests, including taking part in surveys, applying for “work-from-home-jobs” that recruit people for fencing stolen goods or human-assisted CAPTCHA-breaking services.

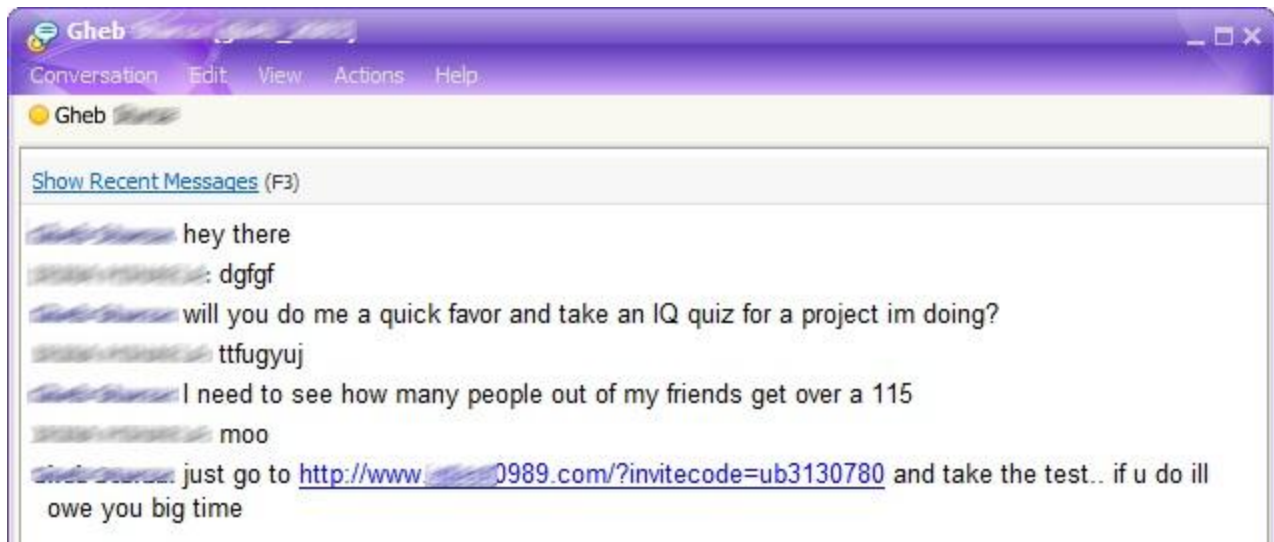


Figure 5: IM conversation leading to premium-rate SMS service

## Social Networking Threats

The second half of 2011 not only brought new e-threats to Facebook's significant user base of over 800 million, but also saw malware creators re-circulate older scams with increased efficiency. Social engineering techniques have been by far the most effective way of convincing users to re-share dangerous content. Cyber-crooks also capitalized on the interest in the death of Muammar Gaddafi and Steve Jobs, two of the most important events of H2 2011.

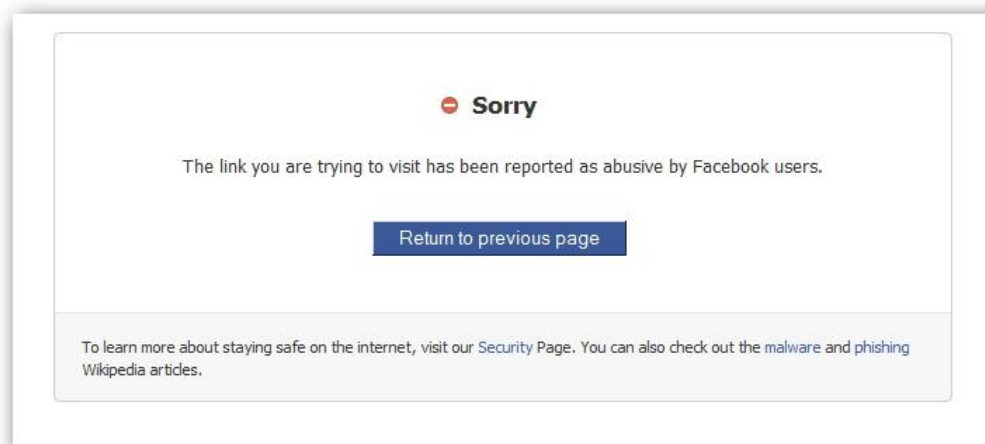


Figure 6: Malicious link impersonating video content and leading the user outside of Facebook™

The anatomy of a Facebook attack is divided into three distinct stages. It always starts with luring legit users into visiting a malicious link that promises either an inciting video or a guaranteed giveaway. Celebrity or national event themes are also frequent, but are used irregularly.

Using a mix of social engineering, applications or click-jacking vulnerabilities, the malicious content gets re-shared and made available to more and more contacts.

The third stage of the attack is monetization, with survey-filling or affiliate sales as the mechanism of choice. Other methods of cashing in on an attack involve collection of personal or login information that will either support other campaigns or get sold on the underground market.

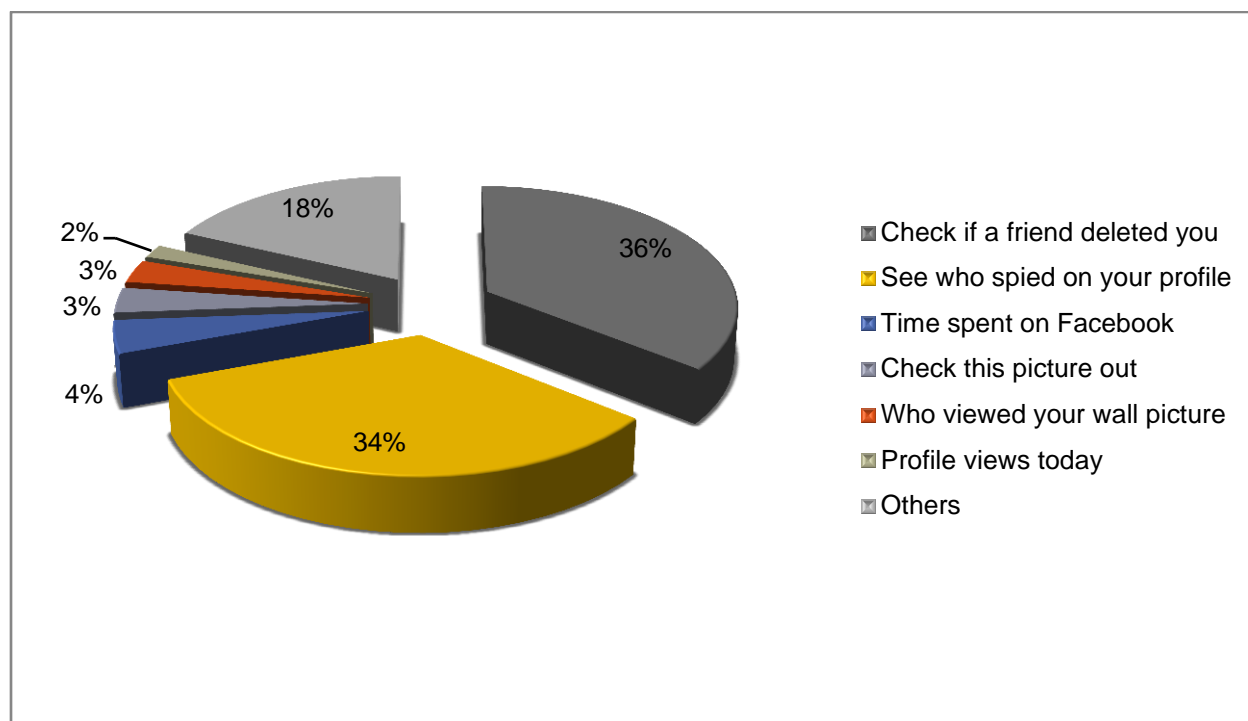


Figure 7: Scam breakdown provided by SafEgo

Most rogue applications that emerged during the first six months of 2011 focused on collecting personal information. These applications are advertised through wall-worms and lead the user to a page where the application is asking for access to basic information, such as the full name, e-mail address, networks, hobbies and all the other information that is publicly available. These details are collected into a large database that can be filtered by habits, region, preferences,

language, and so on. As soon as the details have been collected, the application posts on the user's wall the same enticing message they have initially clicked on, becoming visible to the victim's friends.

Although it gets the largest chunk of cyber-criminal attention, Facebook is not the only social network pestered by spam and malware.

By design, **Twitter** offers free access to users' timelines, unless they explicitly lock their accounts. This model allows third parties to follow anyone without their consent, including Twitter automated bots that closely monitor discussions and send replies based on keywords.



Figure 8: Adult service ad promoted by a follow-everybody bot

## Spam Threats in Review

Although the spam industry received numerous blows in 2011, starting with the termination of the world's largest affiliate spam service (SpamIt) and continuing with the takedown of Rustock, the world's most potent and effective botnet, spam has kept a steady pace. In the second half of 2011, the spam index reached 75.1 percent of the total number of e-mail messages sent worldwide. The spam breakdown on categories is as follows:

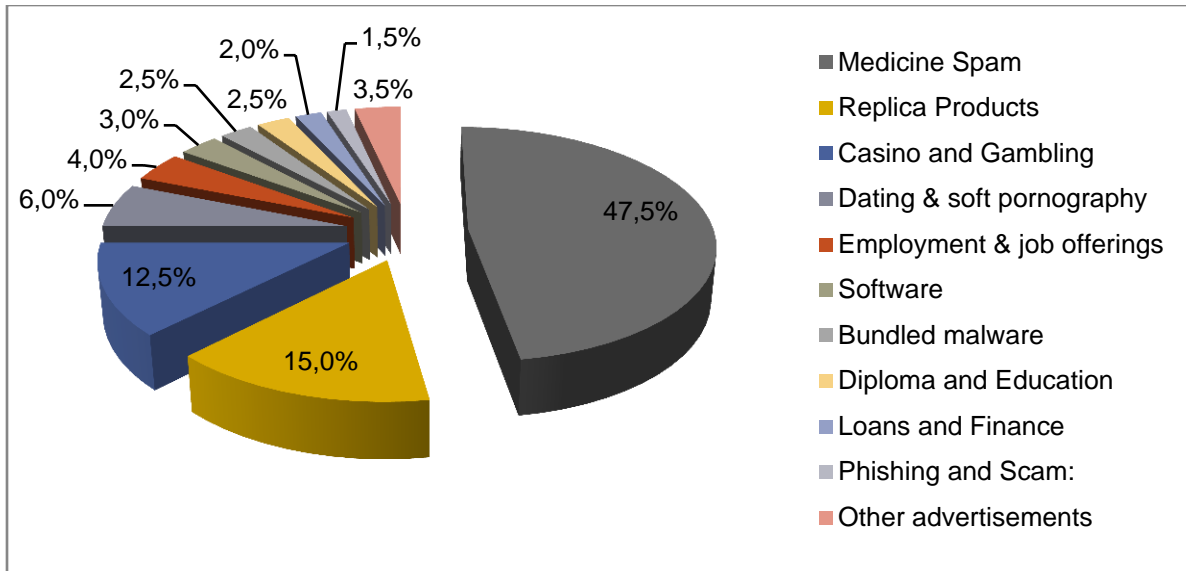


Figure 9: Spam breakdown by category

Pharmacy spam holds the lion's share with 47.4 percent of all spam messages sent globally. The medicine offerings range from classical sexual enhancements that have been part of the Canadian Pharmacy portfolio since the beginning to controlled substances such as Prozac and Zoloft.

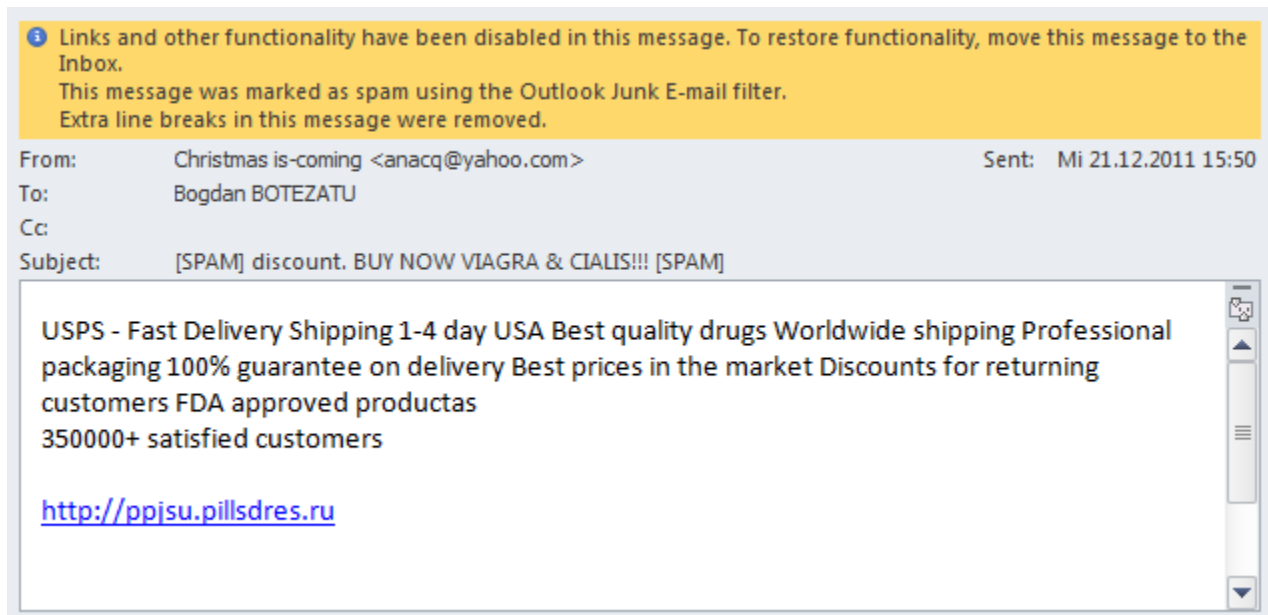


Figure 10: Pharmacy-related spam message - simple e-mail template including one link

Four years ago, most job offerings promoted via spam mail used to lure victims into paying an application fee, but the global economic crisis has shifted this approach: you could be working for the bad guys without having to pay a dime. However, the cyber-criminals are actually seeking money mules and stolen goods fencers to prevent authorities from tracing the money back to them.

---













|   |   |                |      |
|---|---|----------------|------|
|  | bogdan.b... New job vacancy - see details     | Mi 12.10.20... | 8 KB |
|  | bogdan.b... Position opening in your area     | Mi 12.10.20... | 8 KB |
|  | bogdan.b... Employment you've been searching! | Mi 12.10.20... | 8 KB |
|  | bogdan.b... Vacancy - apply online            | Mi 12.10.20... | 7 KB |
|  | bogdan.b... Employment you've been searching! | Mi 12.10.20... | 8 KB |
|  | bogdan.b... Work offer inside                 | Mi 12.10.20... | 7 KB |
|  | bogdan.b... New job vacancy - see details     | Mi 12.10.20... | 7 KB |
|  | bogdan.b... New job vacancy - see details     | Mi 12.10.20... | 7 KB |
|  | bogdan.b... Job opportunity - hurry to apply! | Mi 12.10.20... | 8 KB |
|  | bogdan.b... Job offer match, respond to apply | Ma 11.10.2...  | 7 KB |
|  | bogdan.b... Work offer inside                 | Ma 11.10.2...  | 7 KB |
|  | bogdan.b... Position opening in your area     | Ma 11.10.2...  | 7 KB |

Figure 11: Job offerings: fencing products bought through CC fraud

Although relatively low in numbers compared to medicine spam or knock-off products, malware-bundled messages compensate with destructive potential. Some of the most prominent spam campaigns bundled with malware have abused the identity of well-known payment processor services (such as NACHA or PayPal) or parcel delivery companies (UPS). Most of these messages come with executable attachments disguised as PDF files. Once opened, the computer gets infected with a variant of the Zeus banking Trojan.

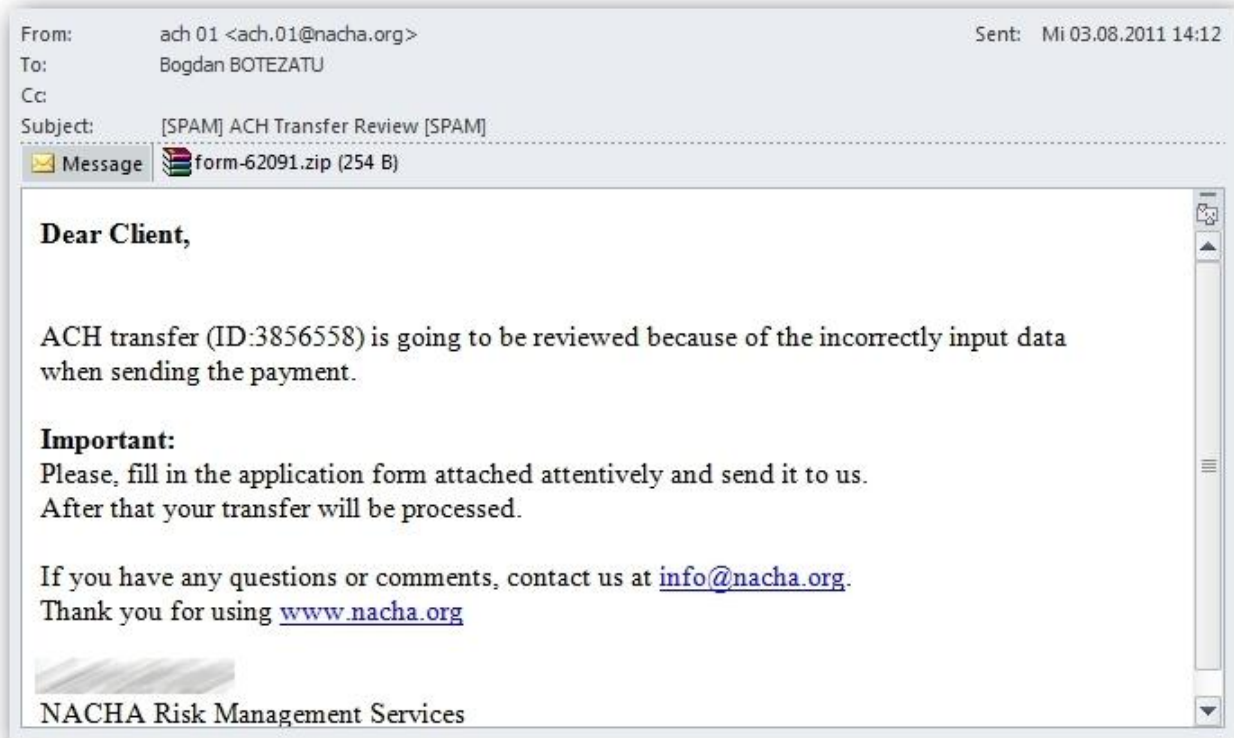
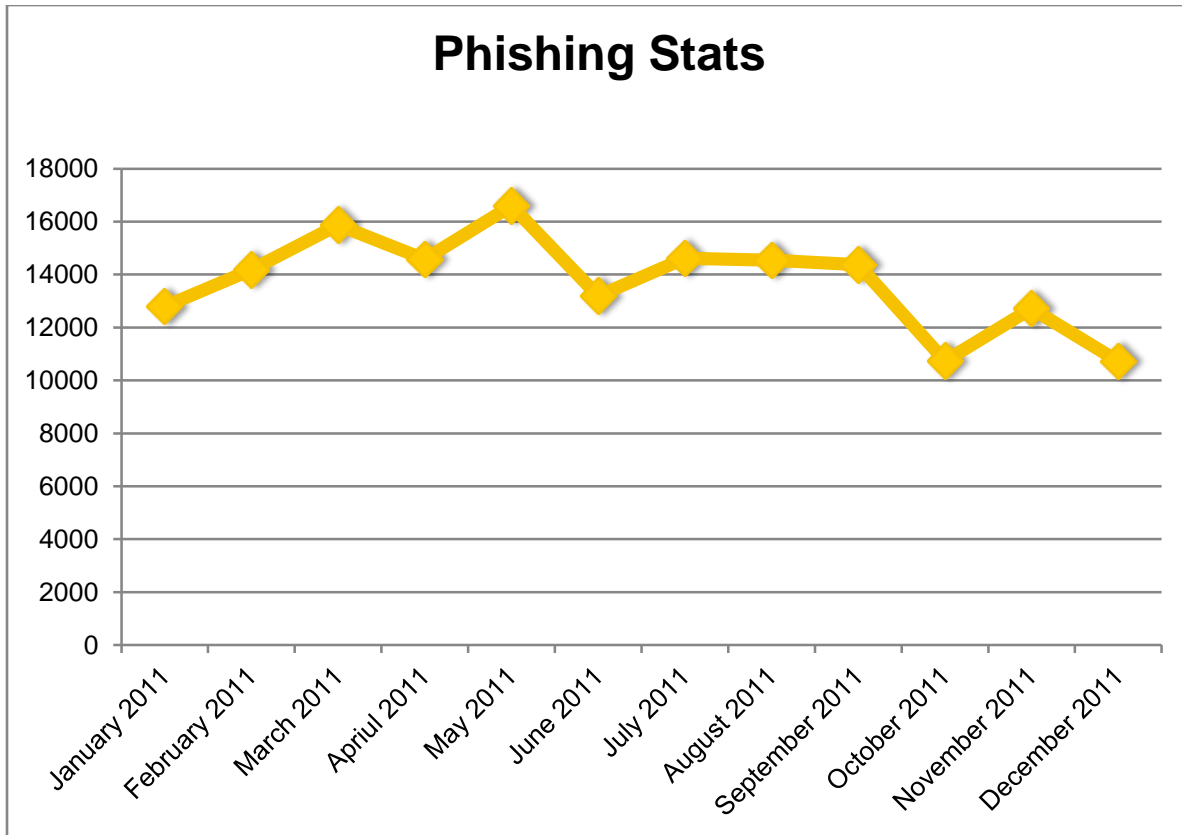


Figure 12: Malware-bundled spam message pointing to malware

## Phishing and Identity Theft

During the last six months of 2007, phishing messages have entered a slightly descending slope, proportional with the level of spam sent during the two semesters. While the phishing messages have kept a constant pace between July and September, their number started to decrease in early October, when the Kelihos (a.k.a. Waledac 2.0) botnet was taken down in a coordinated effort between Microsoft and Czech Internet Service Providers. The shutdown of Kelihos freed roughly 41,000 infected computers that were responsible for sending about 3.8 billion spam messages per day.



**Figure 13: Phishing incidents between January and December 2011**

During the second half of 2011, phishers' interest stayed with financial institutions, with PayPal and eBay as top targets, followed by online games and social networks. Most social network credentials that have been successfully "phished" are dumped on public sharing websites (such as the 10K usernames and passwords released by team TeamSwaStika in October).

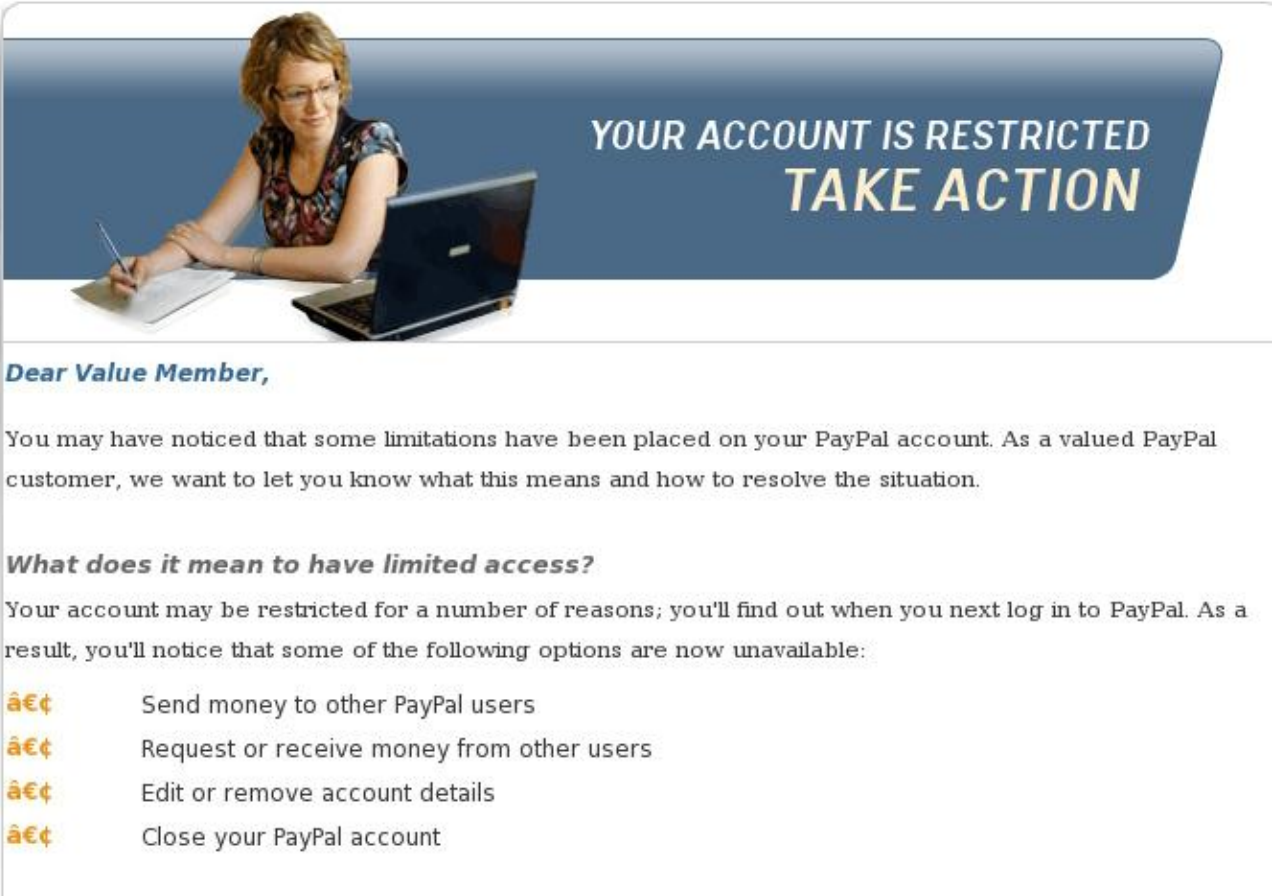


Figure 14: PayPal phishing campaign: "You'll find out why you're blocked when you log in"

## Vulnerabilities, Exploits & Breaches

The series of high-profile data breaches that started in early 2011 under the supervision of the Anonymous hacking group continued throughout the second half. Among the most important victims were both corporations and government agencies, and the information achieved in the hacks has been indiscriminately made public.

Early July started with a hack of the Arizona law enforcement infrastructure, following by the release of private information of 1,200 officers. Two days later, one of Apple's servers was broken into and a list of 27 usernames and passwords were published online. Apple's database dump only contained a list of users who took parts in surveys, which dramatically downplayed the severity of the attack.

The situation got serious on July 11, when Anonymous published 90,000 military e-mail addresses and their corresponding MD5 hashes were leaked online after a successful breach into the network of defence contractor's Booz Alan Hamilton. The incident, dubbed Military Meltdown Monday, was only the first of a series of high-profile attacks against military objectives.

The online edition of British newspaper The Sun was hacked one week after the BAH incident and visitors were redirected to a page announcing the false news of Rupert Murdoch's death.

July ended with two more high-profile breaches. The first, carried on July 28, yielded more than 500 MB of NATO intel that was posted for the public. The second attack was initiated one day later against FBI contractor ManTech, as well as against the infrastructure of the Department of Homeland Security. The hacker group leaked classified documents detailing the creation of personal management software that could allegedly be used to manipulate and spy on public opinion on social networks.

In August, Anonymous also released more than 10G of data gathered from 76 U.S. Sheriff offices. The information was seized after the group breached the security of the hosting provider accommodating the Sherrifs' databases.

Vanguard Defense Industries, a Texas-based aerospace and defense firm, was hit with a massive DDoS attack in late August. During the attack, Anonymous were able to copy 1 GB worth of personal information from company employees, which they subsequently leaked on Torrent trackers.

The year ended with an attack on the infrastructure of yet another major defence contractor known as Stratfor - a Texas-based consultancy that provides military-grade services in foreign affairs and security issues to the US Government. The hacking group managed to seize copies of the company's customer list and credit card information, and the identities of 221 British military officials and 242 NATO employees, along with other confidential information.

# E-Threat Predictions

Year 2011 was extremely rich in malware activity. A year that started under the auspices of data-breaches and corporate leaks continued with the emergence of highly sophisticated bots such as ZeroAccess or TDL4 and ended with a bang with the revelation of Duqu, “the son of Stuxnet.”

Malware will continue its rampant growth throughout 2012 to reach a whopping 90 million samples, almost 17 million more than at the end of 2011. The malware pool will contain both old variants repackaged to avoid detection and new malware built around 0-day vulnerabilities in the operating system and additional software.

Social networks will be the focus of malware authors during 2012. With Facebook surpassing 800 million active users, it has become the largest community on the web. Although the company has made significant progress in securing the interactions between users and minimized the response time to threats, more than 400 million users are vulnerable to short-lived threats at all times of the day. In 2012, we expect intensification of the scams run on Facebook & Twitter, as well as one major family of malware to spread via infected links posted on users' walls.

The Android operating system has become a major player in 2011, as a variety of smartphone and tablet vendors have integrated their own distributions to power their hardware. Since its introduction in 2008, the Android market share has increased exponentially, taking up between 25% and 50% in the US and UK respectively, two countries with the largest penetration of smartphones. At the same time, the number of threats targeting the Android OS considerably increased, as did the risk of private data leaks.

For 2012, Bitdefender estimates the number of threats specifically designed for Android will exponentially grow as the OS is gaining ground in the low-end and mid-range gadget market.

New technologies will also play a key role in malware incidents. Among these technologies, a crucial role will be played by the following:

## The introduction of HTML5

At the moment, HTML5 is universally supported across major browsers and brings new layers of interactions between the user and the site. While enhanced interaction is the main purpose of releasing a major version of the popular mark-up language, the new features will allow cyber-crooks to craft more convincing scams against regular web users via the newly introduced Web Notifications, to track victims with geo-location data (especially if they use HTML5 on their smartphone), or even to initiate attacks against other sites straight from the victim's browser.

## IPv6 and the end of the Internet

It is estimated that all IP addresses in the IPv4 system will be exhausted in the last quarter of 2012. This serious shortcoming that will prevent any new subscriber from getting access to the web has been anticipated since the implementation of the IPv6 protocol has started. The protocol is supported in most operating systems such as Windows Vista, Windows 7, Mac OS/X, all Linux devices and BSD. By default, IPv6-capable devices support stateless auto-configuration which allows them to communicate with other IPv6 network devices and services on the same network segment by advertising its presence via the IPv6 Neighbor Discovery Protocol (NDP). However, this automated process may expose the network devices to attackers or, in extreme situations, to allow an attacker to take complete control over the network device.

IPv6 traffic also supports IPSec, a mechanism that allows traffic to flow encrypted between source and destination. Although this feature protects against traffic sniffing, it will likely become abused by cyber-criminals in order to mask botnet traffic to and from the command center in an attempt to boost their botnets' stealth.

## Windows 8 and zero-day exploits

This year will bring Microsoft's brand-new operating system, Windows 8, to the table. Releases that get leaked on torrent and p2p sharing web services ahead of time are usually repacked versions of the OS laden with malware that subvert the OS before it is even fully loaded, making detection and disinfection much harder. Vulnerabilities in third-party software will also be an important vector of infection as they are constantly capitalized on in the so-called exploit packs.

## Targeted phishing attacks based on social-network shared data

The 800 million users active on Facebook post large amounts of private and business-related information on the social network, and many times, these details are made available to non-friends through poor privacy settings. These pieces of information will increase the chances of targeted phishing attacks in 2012.

## Disclaimer

The information and data included in this document represent the current opinion of BitDefender® on the topics addressed as of the date of publication. This document and the information contained herein should not be interpreted in any way as a BitDefender's commitment or agreement of any kind.

Although every precaution has been taken in the preparation of this document, the publisher, authors and contributors take no responsibility for errors and/or omissions. Nor is any liability undertaken for damage resulting from the use of the information contained herein. In addition to that, the information in this document is subject to change without prior notice. BitDefender, the publisher, authors and contributors cannot guarantee further related document issuance or any possible post-release information.

This document and the data contained herein are for informative purposes only. BitDefender, the publisher, authors and contributors make no warranties, express, implied, or statutory, as to the information stated in this document.

The document content may not be suitable for every situation. If professional assistance is required, the services of a competent professional person should be sought. Neither BitDefender, the document publishers, authors nor the contributors shall be liable for damage arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred to in this document as a citation and/or source of current or further information does not imply that BitDefender, the document publisher, authors or contributors endorse the information or recommendations the individual, organization, independent or collective work, including printed materials, electronic documents, websites, etc. may provide.

Readers should also be aware that BitDefender, the document publisher, authors or contributors cannot guarantee the accuracy of any information presented herein after the date of publication,

including, but not limited to World Wide Web addresses and Internet links listed in this document which may have changed or disappeared between the time this work was written and released and the moment it is read.

The readers are entirely responsible to comply with all applicable international copyright laws arising from this document. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of BitDefender.

BitDefender may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from BitDefender, this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

All other product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.

*Copyright © 2011 BitDefender. All rights reserved.*