H2 2010 E-Threat Landscape Report

MALWARE, SPAM AND PHISHING TRENDS

Author

Bogdan BOTEZATU, Senior Communication Specialist

Contributors

Loredana BOTEZATU, Communication Specialist – Malware & Web 2.0 Threats

Răzvan BENCHEA, Malware Analyst
Dragoş GAVRILUŢ, Malware Analyst

Alexandru Dan BERBECE - Database Administrator

Dan VANDACHEVICI - Spam Analyst
Irina RANCEA – Phishing Analyst

Table of Contents

Table of Figures

Overview

The information security landscape has been shifting for quite some time, as the natural fight between cyber-criminals and antivirus vendors unfolds: new technologies make place to new attack vectors, which are fixed by new technologies again. It took more than 40 years for malware to morph from programming flaws and innocent pranks into a money-making industry cashing on the unwary, but it took it less than 5 years to reach its next evolutionary step and become one of the most feared weapons of cyber-warfare.

While Black-Hat SEO has sensibly diminished as compared to the first half of the year, critical 0-day vulnerabilities discovered in widespread software applications have played an important role in malware dissemination. Amongst the most targeted pieces of commercial software running on Windows were Adobe Reader and Internet Explorer. The Windows operating system itself suffered a series of critical vulnerabilities that made it easier for remote attackers to plant malware on users' systems.

One of the most important e-threat leveraging on Windows 0-day vulnerabilities was the notorious Stuxnet worm, a highly sophisticated malicious tool primarily targeted at compromising industrial processes running on SCADA infrastructures. During the second half of the year, Stuxnet used no less than four distinct 0-day vulnerabilities[1] to explosively infect home user and industrial systems alike. Its increased potential of infiltration, along with highly sophisticated stealth mechanisms propelled the Stuxnet worm to the top 10 e-threats for the second half of 2010.

During the last half of 2010 we also witnessed a series of high profile DoS attacks carried out against well-known financial institutions. Unlike the "average" Distributed Denial of Service attempts in the past, which were primarily fueled by financial gains, these massive attacks encompass a form of protest against opposing organizations on the Internet.

The malware landscape sees two old contenders – Trojan.AutorunInf and Win32.Worm.Downadup, ranking first and second, respectively. These pieces of malware that have their roots in the Windows XP era, but managed preserve their dominance, despite the fact that operating system upgrades or applying patches would have solved the security issues exploited by these pieces of malware.

[1] The Print Spooler Server vulnerability had been discovered about one year ago, but it was never patched.

Malware Spotlights

- Social networks have constantly been in the cyber-criminals focus. With a user base of more than 500 million active users[2], Facebook ranks as the largest social network in the world. Cyber-criminals have been increasingly interested in disseminating their malicious creations to the social network's user base, while also trying to harvest whatever information they find on users'profiles to carry on subsequent attacks.

- While the web still remains the favorite channel of infection, the increased presence of Autorun worms & Trojans reveal that removable media plays a key role in disseminating malware.

- Rogue security software has been constantly increasing its presence during the second half of 2010. Following the rules of evolution, rogue AV creators have refurbished their products to mislead the user that their creations are actually genuine antivirus software from trustworthy publishers. More than that, rogue software extended their scope to other system utilities such as "hard-disk defragmenters" and "registry fixing" software.

- Do-It-Yourself malware has made it easier for script kiddies and people with limited IT knowledge to launch attacks against other computer users. **The Facebook Hacker**, **Gmail Hacker** and the **iStealer keylogger** have been some of the tools of choice for junior cyber-criminals.

- Phishers have paid much more attention to social networks than to financial institutions. During the past six months, Facebook has become the prime target of cyber-criminals, with PayPal and Visa ranking second and third, respectively. Online gaming websites conclude the list of the most targeted institutions and services.

[2] Statistics taken from the Facebook Stats page, available at http://www.facebook.com/press/info.php?statistics

Malware Threats in Review

The malware top for the second half of the year suffered some minor modifications as compared to the first semester, with Trojan.AutorunInf, Win32.Worm.Downadup and Exploit.PDF-JS as top three e-threats. This semester's noteworthy additions are Exploit.CPlLnk.Gen – the Control Panel exploit used by the Stuxnet worm – as well as s variant of the Virtob virus that infects .exe and .scr files and opens backdoors for remote attackers.

World's Top Countries Hosting Malware

Information gathered during the past six months revealed that the e-threat landscape has remained relatively unchanged, except for some minor shifts. China, Russia and Brazil are still ranking first, second and third, respectively in the top ten countries hosting malware. As compared to the H1 2010 landscape, Ukraine has advanced 2 positions from the 10th place to the 8th, although the malware percentage hosted in Ukraine has regressed 0.15 percent from the value in H1.

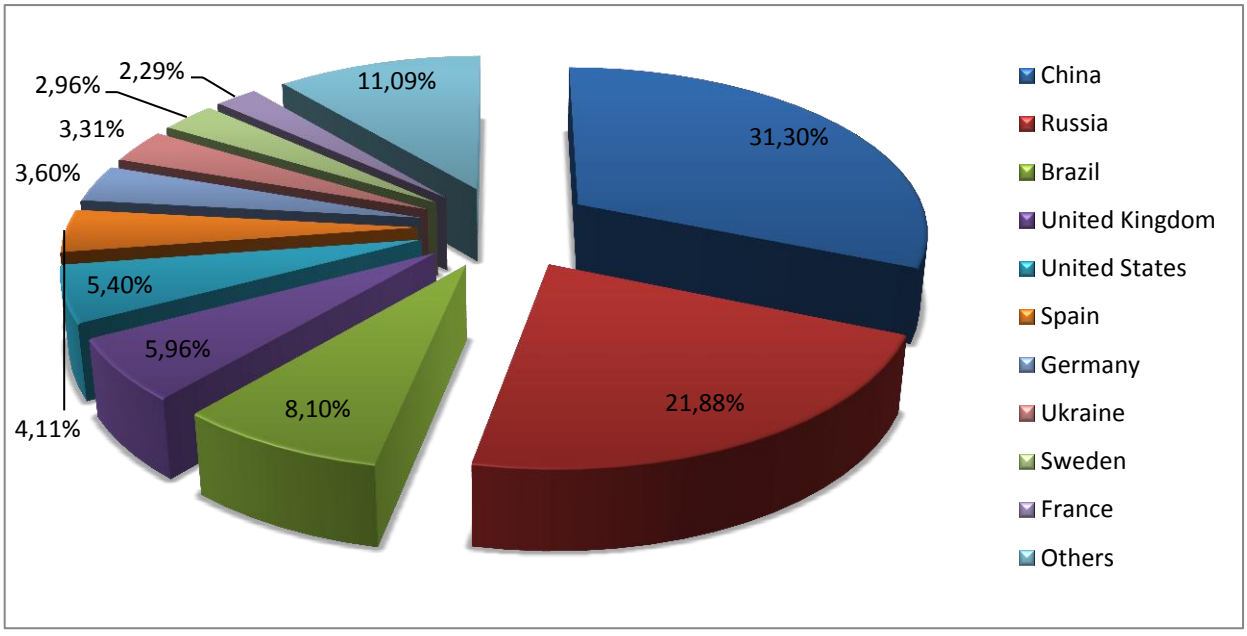

Figure 1: Top 10 countries producing and hosting malware

A closer look on the files hosted in China reveals that the most frequently encountered e-threats are password stealers for online games and a wide range of downloader Trojans which are used to install

additional malware onto the compromised systems. The malware identified in Russia is mostly related to Rogue Antivirus, or more complex e-threats, such as the Zeus bot, peer-to-peer worms and backdoors. Brazil's malware industry is almost exclusively based around Banker Trojans and information stealers used for man-in-the-middle and man-in-the-browser attacks. Interesting enough, Brazil is the prime target for the notorious compile-a-virus malware called Win32.Induc.A, a side effect of using the Delphi RAD tool (versions 4 through 7) to write Banker Trojans.

During the second half of the year, the most affected countries by malware have been France, the United States and China, where BitDefender logged most of the malware-related incidents.

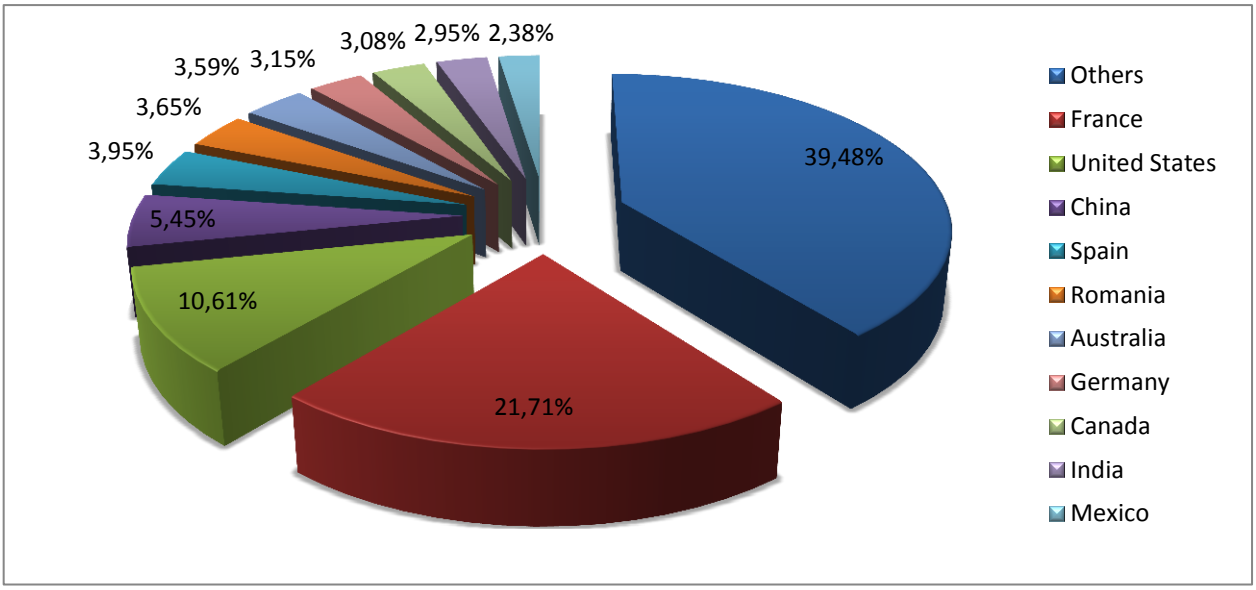

Figure 2: Top 10 countries affected by malware

Top 10 E-Threats for H2 2010

The international malware top for the second semester shows little modifications as compared to the first half of 2010, with Trojan.AutorunInf, Win32.Worm.Downadup and Exploit.PDF-JS ranking as top three global e-threats. As a side note, both Trojan.AutorunInf and Win32.Worm.Downadup are two pieces of malware that have their roots in the Windows XP era, and which could be easily mitigated by simply upgrading the operating system.

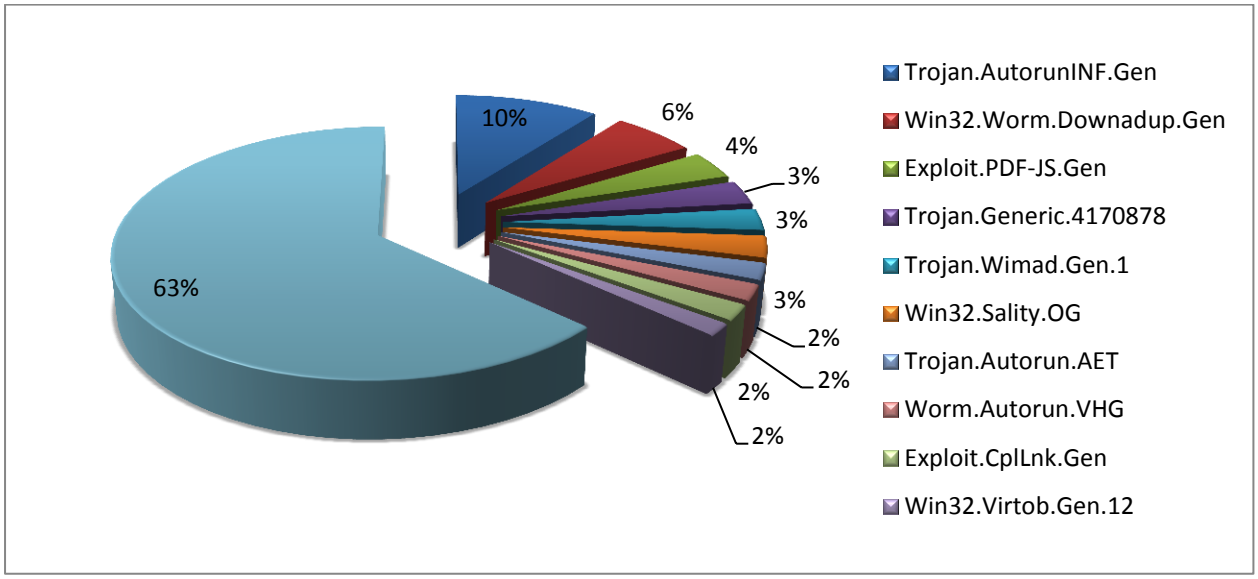

Figure 3: Top 10 e-threats for H2 2010

1. Trojan.AutorunInf.Gen

The **top** ranking e-threat, **Trojan.AutorunInf.Gen** holds 10.42 percent of the worldwide infections. This e-threat is a specially crafted autorun.inf file that automatically launches malware from infected removable storage devices without the users' interaction. Some of the most well-known families of plug-and-play malware that rely on autorun.inf files to automatically execute when an infected flash drive is plugged in are Win32.Worm.Downadup, Win32.Zimuse.A, Win32.Sality, Trojan.PWS.OnlineGames, Win32.Worm.Sohanad and Win32.Worm.Stuxnet.A.

2. Win32.Worm.Downadup

Win32.Worm.Downadup (also known as the Conficker or Kido) hardly needs any introduction. During the past three years, it managed to become the living nightmare of any system administrator, and although the last year hasn't brought any development, the worm is still active and wreaking havoc amongst a considerable number of computers.

On the technical side, the worm exploits the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (**MS08-67**) in order to propagate. After it has successfully infected the computer, it restricts users' access to the Windows Update service, as well as to security vendors' web pages. The latest variants of the worm can download and install rogue antivirus and other e-threats.

3. Exploit.PDF-JS.Gen

BitDefender's third e-threat for the second half of 2010 is **Exploit.PDF-JS.Gen**, which holds 3.66 of the total number of infections worldwide. This generic detection deals with malformed PDF files exploiting different vulnerabilities found in Adobe PDF Reader's Javascript engine in order to execute malicious code on users' computer. Upon opening an infected PDF file, a specially-crafted Javascript code triggers the download and automatic execution of malicious binaries from remote locations.

PDF exploits have been extremely popular during this semester, when they peaked with the series of spamvertised PDF files posing as invitations to the Nobel Prize. Upon opening the PDF file, the above-mentioned JavaScript code drops a malicious file embedded into the PDF document and executes it.

4. Trojan.Generic.4170878

Trojan.Generic.4170878 holds the fourth place with 3.14 percent of the number of recorded infections for the second half of the year. It is a backdoor that provides cybercriminals with remote access to the infected system. Data gathered by the BitDefender labs revealed that the Trojan usually comes bundled with the so-called "cracks" and "keygens" that are used to circumvent the protection algorithms of commercial software applications.

5. Trojan.Wimad.Gen.1

The fifth place in the BitDefender malware top for the second half of 2010 is taken by Trojan.Wimad, This e-threat is disseminated via Torrent websites, camouflaged as episodes of your favorite series or as a not-yet-aired but soon-to-be blockbuster. These counterfeit video files connect to a specific URL and download malware "advertised" as the appropriate codec required in order to play the file. Trojan.Wimad.Gen.1 is mostly active before or immediately after box-office premieres.

6. Win32.Sality.OG

The sixth place with 2.83 percent of the infections triggered globally is taken by Win32.Sality.OG. This malicious e-threat is a polymorphic file infector that appends its encrypted code to executable files (.exe and .scr binaries). It deploys a rootkit and kills antivirus applications running on the computer in order to hide its presence on the infected machine. After it has successfully defeated local security, the virus tries to deploy a keylogger that would intercept all passwords and login accounts, and then send them to a pre-defined e-mail address. More than that, Win32.Sality.OG has backdoor features, which means that the remote attacker can seize full control over the remote machine.

7. Trojan.Autorun.AET

Trojan.Autorun.AET is a piece of malware that spreads through the Windows shared folders, as well as through removable storage devices. This e-threat ranks seventh with 2.14 percent of the worldwide infections. This is one of the Trojans that exploit the Autorun feature implemented in Windows for automatically launching applications when an infected storage device is plugged in. It is also representative for the generation of computers running Windows XP and Vista SP1, since Microsoft pulled this feature out for any removable media except for CD and DVD-ROM storage devices.

8. Worm.Autorun.VHG

Worm.Autorun.VHG is an Internet /network worm that exploits the Windows MS08-067 vulnerability in order to execute itself remotely using a specially crafted RPC (remote procedure call) package. This method of propagation has also been used by Win32.Worm.Downadup, which means that this specific worm also targets computers running the Windows XP operating system without the security patches in place. The worm ranks eighth with 2.05 percent of the global infections.

9. Exploit.CplLnk.Gen

The ninth place in the malware top goes to Exploit.CplLnk.Gen (2.01%) - a detection specific to lnk (shortcut) files that makes use of a vulnerability in all Windows® operating systems to execute arbitrary code. This exploit has seen a significant boost these past few weeks as it managed to become one of the top 10 e-threats in less than 5 months. It is also one of the four zero-day exploits that have been intensively used by the Stuxnet worm to compromise local security.

10. Win32.Virtob.Gen.12

Ranking 10th with 1.59 percent of the global number of infections worldwide, Win32.Virtob.Gen.12 is a file infector whose code is entirely written in assembly language. Upon execution, it starts infecting .scr and .exe files, but it spares critical system files and dll s. The highly encrypted viral code is continuously attempting to connect to an IRC server. When a connection has been established, it awaits for the remote attacker's instructions. The virus also opens a backdoor for the remote attacker to take control of the infected system.

Malware top for July – December 2010		
01.	TROJAN.AUTORUNINF.GEN	10,42%
02.	Win32.Worm.Downadup.Gen	6,00%
03.	EXPLOIT.PDF-JS.GEN	3,66%
04.	Trojan.Generic.4170878	3,14%
05.	TROJAN.WIMAD.GEN.1	2.84%
06.	WIN32.SALITY.OG	2.83%
07.	TROJAN.AUTORUN.AET	2.14%
08.	Worm.Autorun.VHG	2.05%
09.	EXPLOIT.CPLLNK.GEN	2.01%
10.	Win32.Virtob.Gen.12	1.59%
11.	OTHERS	63.32%

Tools of Corporate Espionage: Win32.Stuxnet.A

The Stuxnet worm has undoubtedly been the most spectacular e-threat in the past years. As one of the most complex pieces of malware to date, Win32.Worm.Stuxnet.A is touted to have been created in order to disturb the activity of a nuclear facility in Teheran.

The worm has been initially spotted in June 2009, but it has been considered yet another variant of the Zlob Trojan. During the year that elapsed between its emergence and its identification, Win32.Worm.Stuxnet.A has gathered the necessary data for its masters to get a glimpse at the power plant's critical processes and systems.

The worm is built on a variety of technologies, ranging from rootkit protection to a series of critical 0-day exploits that allows it to breach the local security. The rootkit driver accompanying the worm prevents the user from seeing the malicious files; however, this sophisticated e-threat has yet another layer of protection to ensure that it is not caught: a valid digital signature.

The digital signature is a fundamental concept in the information security field, as it ensures the recipient the validity of a message or document. Since the binary files signed with a valid digital certificate are proven to be safe, some antivirus vendors tend to skip them from scanning, which allowed Stuxnet to also infect systems running security software.

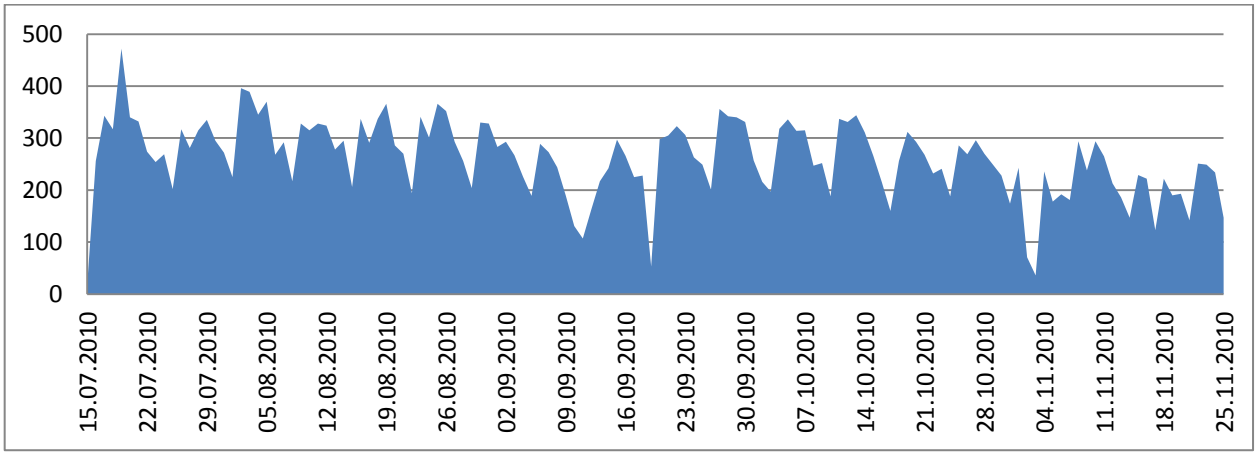

Figure 4: The evolution of Stuxnet in the second half of 2010

Stuxnet's payload is primarily targeted at interfering with the behavior of computer systems that control ultra-high-speed electric engines. The worm's components come packed in a single DLL file, which makes it extremely viral even in environments with no connection to the Internet.

Win32.Worm.Stuxnet.A is currently spreading via infected memory sticks, as well as through the Windows shared folders. In order to "jump" from one computer to another, the Stuxnet worm enumerates all the user accounts present on the system and tries to access all the shared folders on the network for every user. This approach relies on the Windows Server Service RPC Handling Remote Code Execution Vulnerability (**MS08-67**) that has been previously used by Win32.Worm.Downadup to infect about 5 million computers.

If it manages to copy itself on a computer on the network (usually in the folder that hosts the operating system[3]), it creates a .job file pointing to a file named defrag[number].tmp. The job file ensures that the malware gets executed two minutes after the Worm has been copied on the local computer.

Win32.Worm.Stuxnet.A is more than a simple e-threat whose infection potential got out of proportion. It is a highly-advanced piece of malware written by a team of professionals with in-depth knowledge of both operating systems and industrial process control software.

[3] In order to copy itself in the directory hosting the operating system, the worm exploits a vulnerability in the print spooler service. This vulnerability has been discovered in early 2009, but it hasn't been exploited by any other e-threat to date.

Botnet Intelligence

During the past 6 months, botnets have played a significant role in the global malware landscape. From spam sending to vengeful attacks against companies, botnets have done it all. However, while the first half of the year has been quite favorable for the development and exploitation of botnets, the second semester saw some of the most important spam networks taken down by authorities or crippled by the sudden desappearence of their affiliate programs.

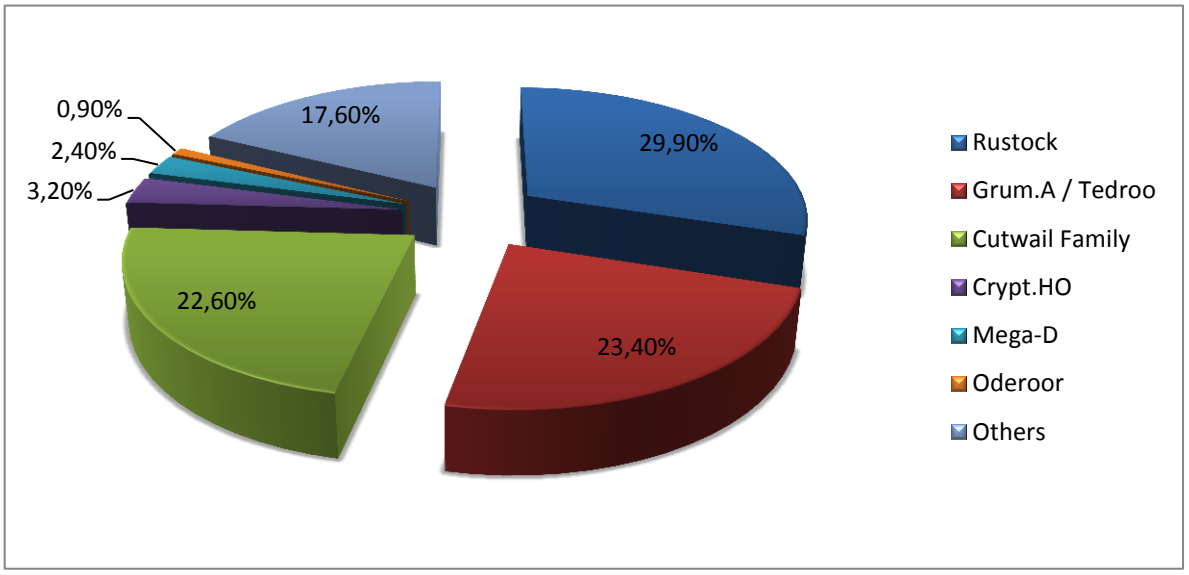

Figure 5: Botnet activity between July and December

1. Rustock

The second half of 2010 shows Rustock as the world's most proficient bot, but – unlike the first half – its activity has considerably reduced as of mid-September. If Rustock owned about half the spam market alone during the first six months of 2010 and continued to dramatically increase between July and September, it has minimized its presence during the last quarter of the year.

Overall, Rustock remains one of the most sophisticated spam bots ever. Protected by a rootkit driver, each bot is capable of sending more than 25,000 messages per hour. In order to detect whether the infected machine is connected to the Internet, the bot performs DNS MX queries on popular websites. It then queries a list of domain names to locate its command and control center. After it has located the C&C center, it tries to log in via a POST request and then downloads the templates and email addresses that will be used for spamming. Spam mail coming from Rustock is easy to tell, as it never comes bundled with malware, but rather focuses on male enhancement pills and other pharma-related messages.

2. Grum (a.k.a. Tedroo)

During the past six months, Grum's activity has witnessed an impressive comeback, which translates in a whopping 23.4 percent of the spam market. Just like Rustock, the Grum bot deploys a kernel-mode rootkit and starts pumping up to 4000 spam messages per hour. Although it is less capable of sending spam as compared to the Rustock bot, Grum can download a multitude of spam templates from multiple download locations. Usually, the unsolicited mail sent by Tedroo advertises pharmaceutical products, but occasionally, the botmasters run their own infection campaigns by sending out links to bots in messages mentioning international celebrities.

3. The Cutwail Family

The Cutwail botnet has gained considerable ground throughout 2010, reaching the third place in the spam industry. During the first half of 2010, the Cutwail bot is the spamming component of the Pushdo botnet, which ranked second in our previous E-Threat Landscape Report. Upon infection, the local computer is instructed to download the Cutwail rootkit dropper and the spammer component. Apart from the already "traditional" rootkit driver to hide its presence, the bot comes with extra layers of protection, such as the ability to launch, send a burst of messages, and then terminate itself. When it starts again (which happens almost immediately), the bot gets a new process identifier (PID), and becomes almost impossible to kill.

Although impressive enough, the Cutwail bot is more than a spam-sending machine. Every new version of the bot is upgraded with new features, such the ability to send itself through instant messaging applications, to open backdoors or to install additional malware. Also, while other botnets usually experience severe difficulties when C & C servers get shut down, the Cutwail bots get upgraded via the fail-safe mechanism offered by Pushdo / Kobka.

4. Crypt.HO (a.k.a. Maazben)

The Maazben botnet seems to have become larger during the past six months, although the number of Maazben bots may look ridiculous as compared to the top 3 botnets presented above. The botnet started to get shape in May 2009 and ever since, it has constantly managed to add new zombified computers to its infrastructure. Despite its significant number of infected drones, Maazben keeps a low profile by sending moderate number of spam messages. At the moment, Maazben is one of the very few botnets that send Casino-related spam.

5. Mega-D (a.k.a. Ozdok)

Once known as one of the largest botnets in the world, the Mega-D network has gained unwanted attention from the authorities. After a couple of failed attempts to terminate the botnet by taking down the C & C servers, security researchers found a flaw in the bot's proprietary communication protocol, which allowed a third party to download the spam templates and train spam filters on them before these spam waves get sent to their victims. The second half of 2010 saw the Mega-D botnet lose its drones, but the real hit came in November 2010, when its alleged operator was arrested for CAN-SPAM act violations.

6. Oderoor (a.k.a Bobax)

Oderoor is the oldest (and, back in 2008, the largest) botnets in the world. It has become popular during mid-2008, but it appears that it has been active since 2005. The Oderoor C&Cs have taken a huge blow by having its C&C servers shut down. At the moment, Oderoor barely gets one percent of the spam market

Web 2.0 Malware

Social networks, blogging and micro-blogging platforms play a significant role in users' lives. Social networking accounts are packed full with valuable information for cyber-criminals and include home addresses, e-mails and lists of contacts, along with significant intelligence on users' habits and routines. More than that, the social network space offers the malware author exposure to about **half a billion members**, a market place that is much larger than the entire population of the United States of America.

Instant Messenger Malware

Ever since the beginning of the year, malware authors have focused their attention towards instant messenger users. E-threats such as Win32.Worm.Palevo.DS, Win32.Worm.IM.J or the rootkit-based Backdoor.Tofsee have traditionally tried to infect the user and use their resources for a wide range of criminal purposes, such as DDoS-ing, sending spam or credit card fraud. However, although these e-threats are still making victims, the last half of the year brought a significant shift in the way cyber-criminals tackle Instant Messenger users.

Some of the Instant Messenger malware identified during the last six months of 2010 include Worm.FaceBlocker (also known as the Ymfoca worm) and a wide assortment of other bots that do not send infected links, but rather links to rogueware products.

One of the most interesting pieces of malware that spreads via IM is the Worm.FaceBlocker, an e-threat that sends infected links via Yahoo Messenger. If the user follows these links and gets infected, they will also start spreading the messages, but will also have access to the Facebook website conditioned by the participation in surveys. Judging by the prices displayed in the affiliation program, every survey brings the attacker $1.Multiply it by thousands of infected users who fill in an average of 3 surveys per day: that's what infected computers are worth to the attacker.

Social Networking Threats

Social networks have been particularly important for malware authors during the past six months. Taking advantage of the enormous number of active users, cyber-criminals have launched numerous malicious campaigns via the Facebook platform. If most of these campaigns carried via Facebook during the first half of 2010 were related to malware and adware (such as the Koobface worm and various multimedia players, respectively), the second half of the year has been dominated by rogue Facebook applications written by third parties and leading to surveys. Most of these applications require access to users' personal data, as well as permission to post everything on the users' behalf.

Figure 6: Rogue application asking for full control over user's data and actions

Using inciting messages to lure users into clicking the links, these messages take the unwary social networker to websites that ask the victim to fill in surveys as a security check before accessing the actual content. Of course, once the user complies with the request, they will be presented more surveys instead of the promised content.

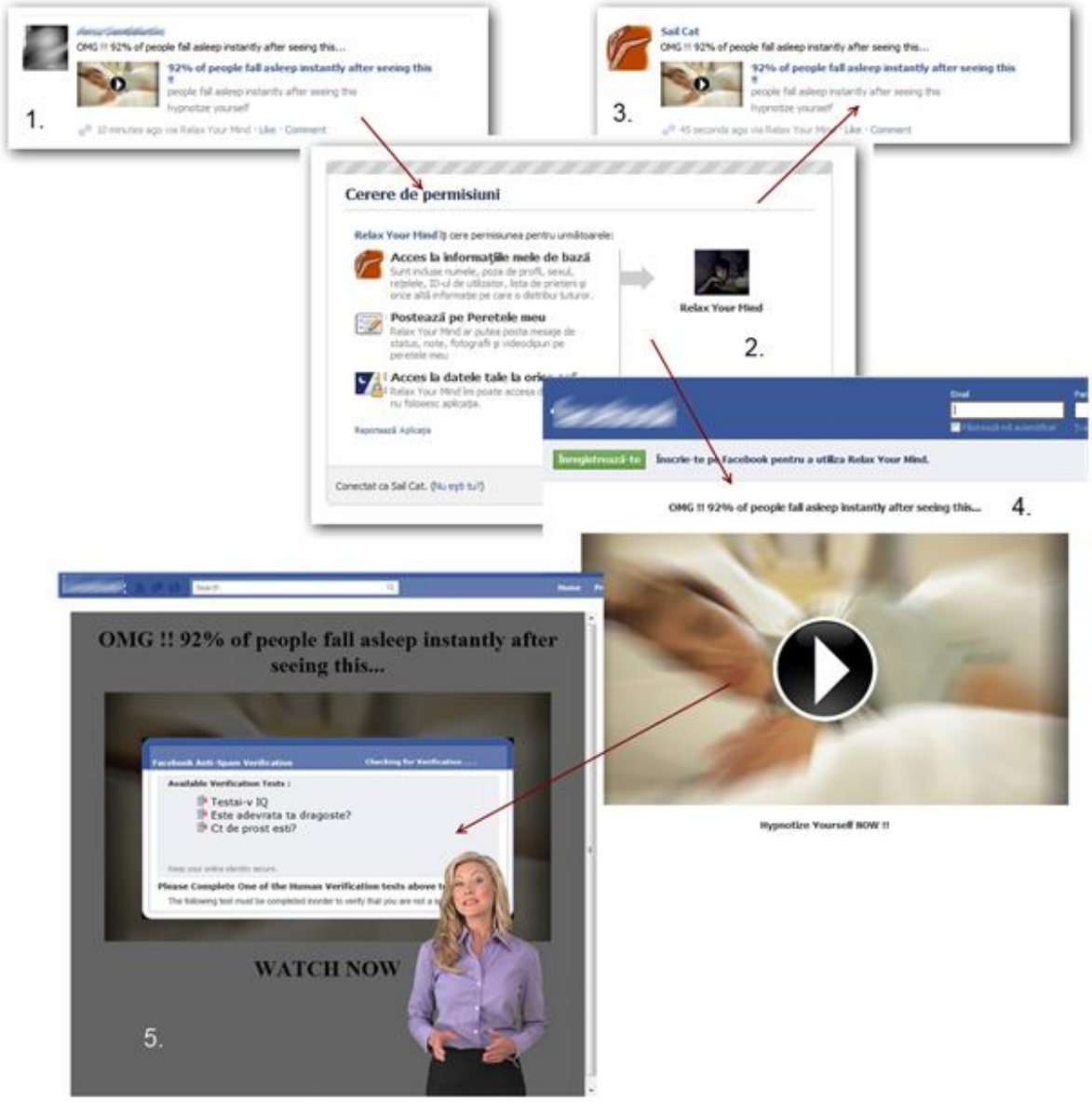

Figure 7: The scheme of a worm spreading on Facebook

The infection scheme of such campaigns is simple:

1. The infected user unwarily posts the message and link to their wall. It will be visible to all friends, luring them into further clicking on the link.
2. Friends clicking on the link will be required to allow the malicious application perform some tasks on the user's behalf, such as accessing the basic information and posting on the respective user's wall, among others.
3. The same message appears immediately on the user's wall, right after they have authorized the application for the above-mentioned tasks, thus spreading the infection further.
4. The application takes the user to a page that displays an alleged Flash player with the "incredible video", which turns to be a JPEG image linking to a domain outside of the social network.
5. As the user arrives on the external domain, they will be asked to fill-in surveys in order to be granted access to the promised video.

During the last months of the year, Java-based malware has witnessed a dramatic increase on Facebook and Twitter. Taking advantage of the fact that Java is a multi-platform environment that can run on Windows and Mac OS X, **Java.Trojan.Boonana.A**, initially runs as a Java applet that acts as a downloader for other malicious files. After it has successfully started, the Trojan hijacks all social networking accounts to post on the user's behalf and periodically checks with the C & C server to run whatever actions the botmaster has instructed it to perform.

Facebook was not the only major social network targeted by cyber-crooks. Late September saw a large-scale attack using specially crafted tweets that exploited a vulnerability in the way the social networking platform treated JavaScript.

Figure 8: Tweets containing malicious JavaScript code

When moving the mouse over the compromised link, the user involuntarily gets redirected to an arbitrary website - usually domains used by rogue antivirus to launch "scan simulations".

While Twitter rapidly fixed the glitch and removed the offending accounts, a new malicious scheme was built for Twitter users who panicked that their accounts might have been hacked into. A large number of tweets announced an alleged step-by-step guide on how to “unhack” your own Twitter account. However, in order to access the respective content, the user was asked to complete a survey.

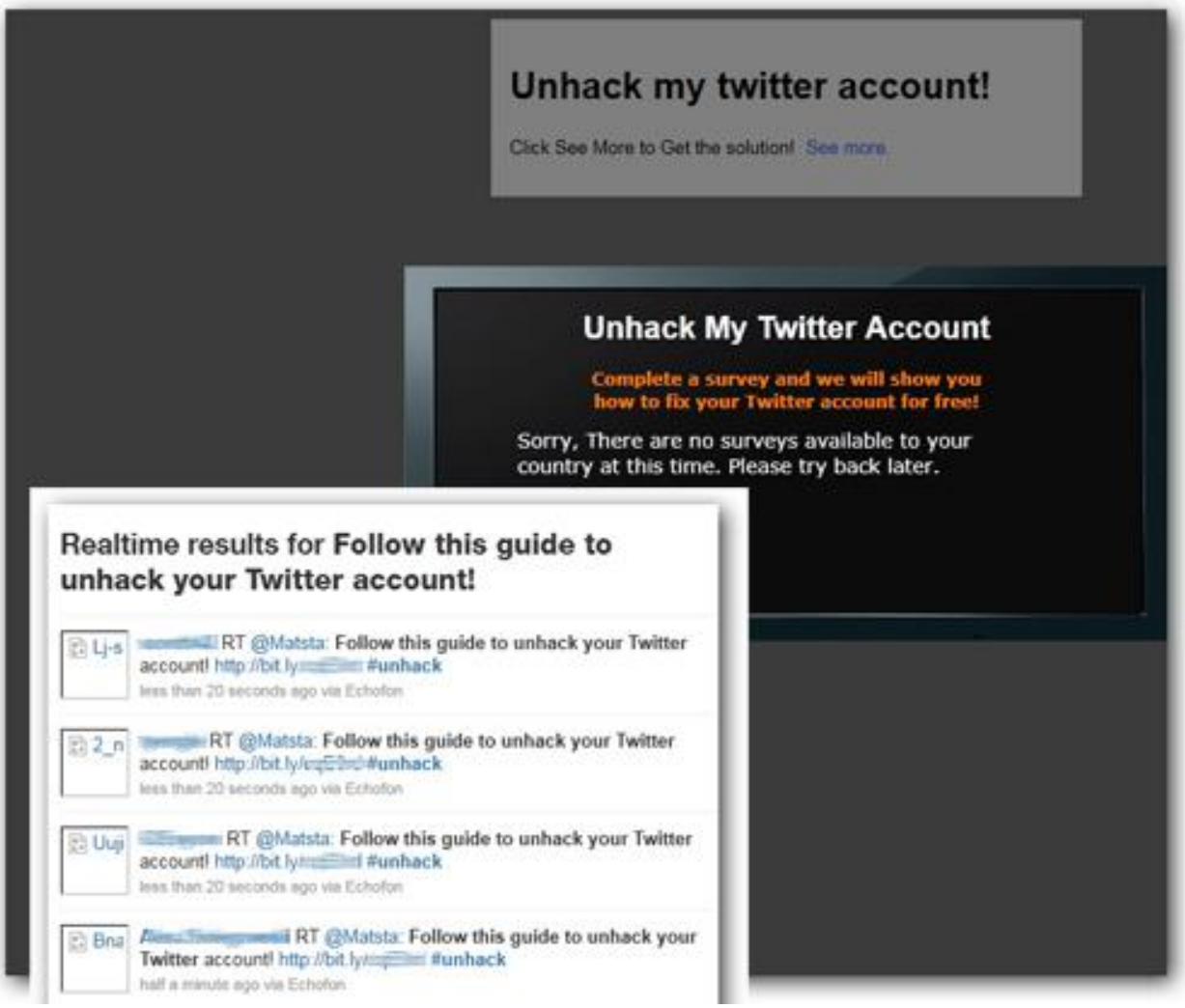

Figure 9: Twitter glitch exploited by quick cash makers

Social networking spam has been another major party-wrecker during the second half of 2010. Most of the spam waves carried via social networking platforms were related to the activity of malicious applications posting objectionable content on users’ behalf. Some of the spam messages are directed at selling products and services, while others are aimed at collecting information about the victims and their circle of friends.

Figure 10: Sexual enhancement ads spammed throughout Yahoo! Groups

Spam Threats in Review

During the second half of 2010, the spam industry has taken an important blow, as one of the most important affiliate programs shut their doors for good. The domain **spamit.com**, a notorious hub for underground spammers ready to turn their botnets into fully-fledged cash cows, was especially known for its involvement with Canadian Pharmacy.

One of the most remarkable aspects in the spam landscape for the second half of the year is the significant decrease of pharmaceutical spam, from a whopping 66 percent of the global amount of spam in H1 to 48 percent in H2. With Canadian Pharmacy almost extinct as of October 10 and with other botnets such as Pushdo and Mega-D severely crippled by C & C takedowns, the overall spam volume index has dropped considerably, but maintained the same breakdown as seen in the previous semester.

What is particularly important is the increase in casino spam, a strong indicator of the fact that the Crypt.HO / Maazben botnet has been hard at work and ramped up spam distribution probably to compensate for Rustock and Grum bots that have got nearly silent as of early October.

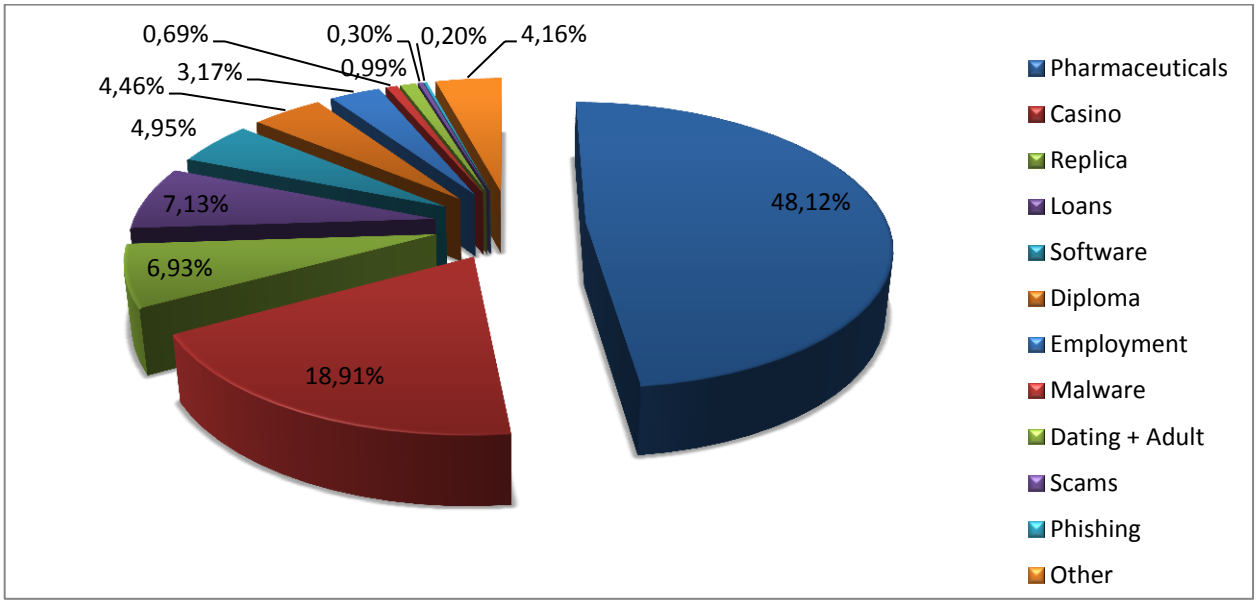

Figure 11: Spam breakdown by type

Although it has diminished in number of messages per day, pharmacy spam hasn't gone completely extinct, but rather suffered a transformation. The new spam messages advertise the same old knock-off pills made in China, but the familiar templates ripped off from legit newsletters have turned into the new layouts similar to the image below:

Figure 12: New message templates for medicine spam

Casino and online gambling spam ranked second during the past six months, a significant increase from the modest fifth place it occupied during the first half of the year. Replica spam has moved down one place. While most of the templates we have seen during the first half were graphics-intensive, the current replica spam campaigns mostly rely on text-based messages accompanied by one hyperlink.

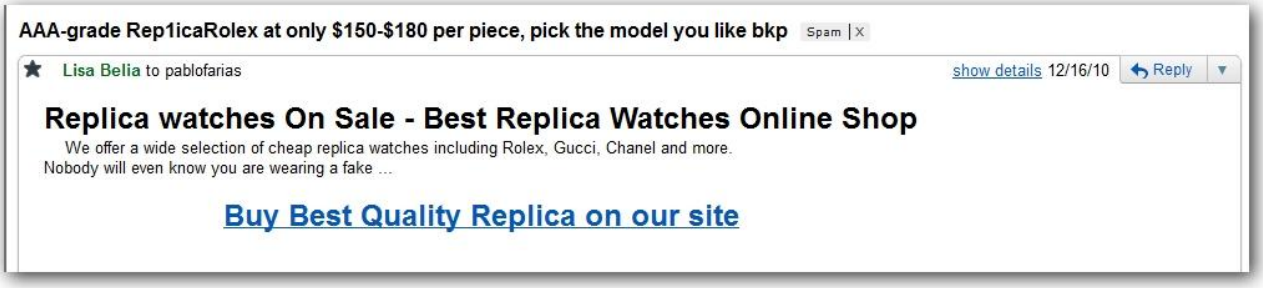

Figure 13: Replica spam using simple HTML templates

Spam messages accompanied by malware have declined during the last half of 2010. Among the most intensively spammed malware there are the Zeus bot, various variants of Bredolab, as well as a large number of malicious PDF files exploiting various vulnerabilities in the Adobe Reader PDF viewer.

Spam Trends for H2 2010

During the last 6 months of 2010, spam has dropped from 86.2 to 85.1 percent of all the e-mail messages sent globally. On average, a spam message is 4 KB, with text as the format of choice for sending unsolicited mail. Depending on the spam campaign specifics, the message size varied between 3 and 9 KB per email.

The third quarter of 2010 saw a massive flux of Canadian Pharmacy spam, including large image-based messages, which completely dropped off the radar as of October, along with the termination of the SpamIt affiliate service. Most of the pharmaceutical spam sent during the last quarter of the year is related to weight loss medicine and sexual enhancements sold by an emerging business called US Drugs. The majority of spam messages advertising such products are sent in plain text and accompanied by hyperlinks to 5-letter random domain names registered in Russia which act as proxies and redirect the user towards clone websites.

Phishing and Identity Theft

Traditionally, phishing mostly targets banking services or other financial institutions. However, unlike the first half of 2010, when Paypal was the prime target of cyber-criminals, phishing took an interesting turn towards social networks and online gaming communities. The BitDefender phishing top places Facebook as number one identity abused by phishers.

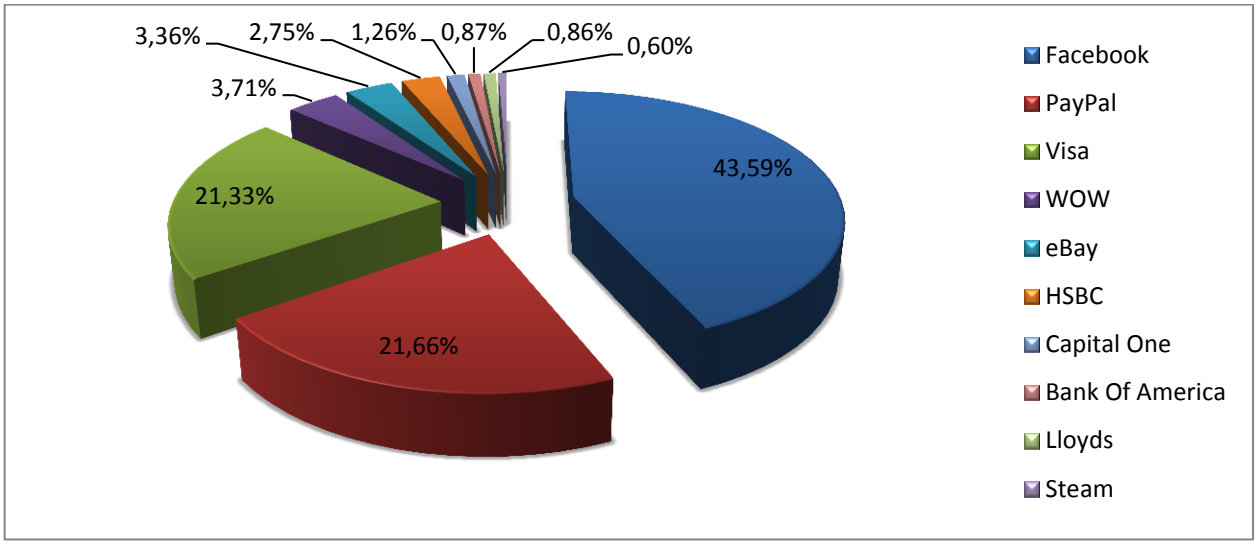

Figure 14: Top 10 phished institutions and services during H2 2010

This rapid escalation from the fourth place straight to the top reveals the fact that phishers put a lot of value to personal data, which may be used for a wide range of purposes, such as building customer profiles based on interests, building personal information databases to be sold to third party spammers or carrying further spear-phishing attacks against victim's friends and friends of friends.

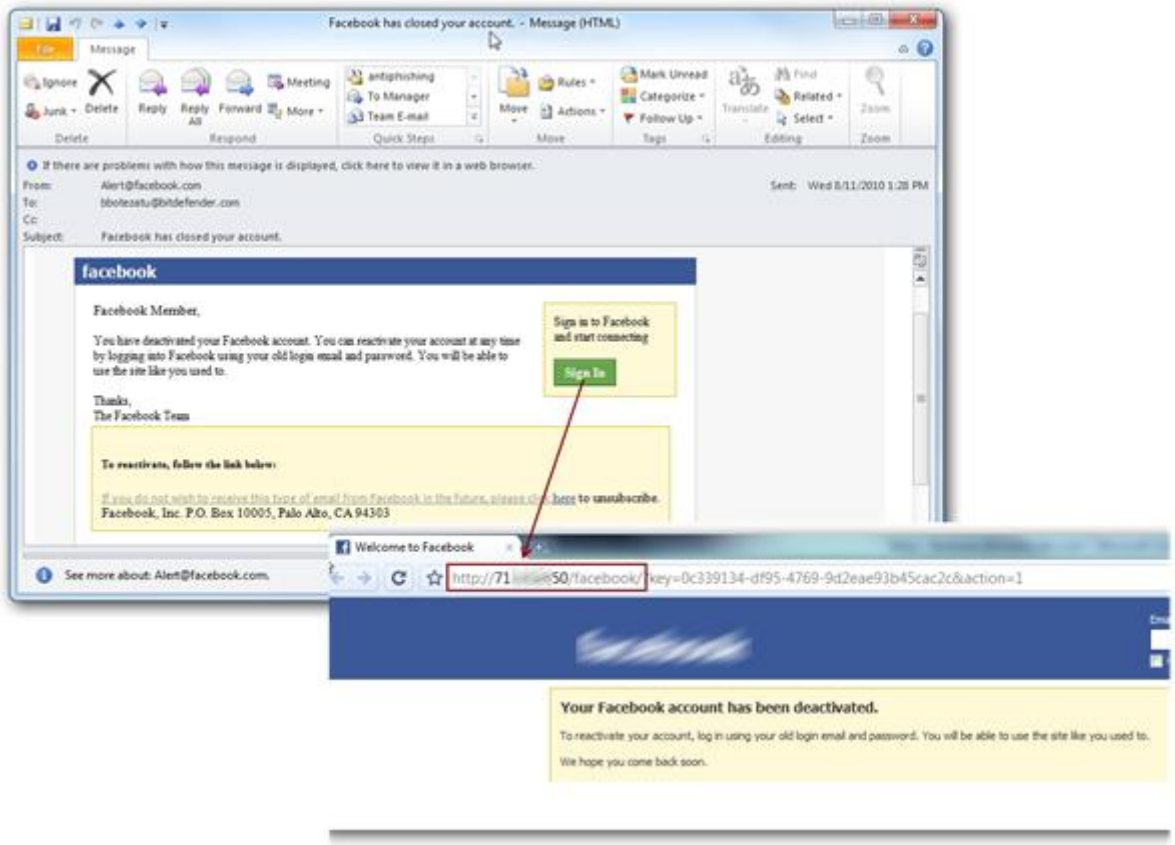

Figure 15: Phishing message playing the account deactivation trick

Payment processing service PayPal ranks second in the top of the most phished brands for the second half of 2010. Amongst the multitude of spam waves targeting the system is a message originating from Romania that asks the user to confirm their data in order to unblock the account and be able to get payments in due time.

Figure 16: PayPal Phishing Page hosted on fast-flux servers

Although the primary targets of cyber-crooks during the last half of 2010 have been social networks and payment processors, online gaming communities such as Steam® and World of Warcraft® have also been intensively exploited. Online gaming accounts are particularly marketable, as they contain either serial numbers for games that can be re-sold through the notorious “OEM Software” portals, or their resources (virtual gold and items) can be transferred to other players in exchange of real-world money.

Vulnerabilities, Exploits & Security Breaches

Just like the first semester of 2010, the second half of the year was extremely rich in 0-day exploits and security breaches. These flaws range from the “usual” Adobe 0-day exploits affecting the Reader and Acrobat applications prior to version X[4] to extremely sophisticated code taking advantage of multiple vulnerabilities, as it was the case with the Stuxnet worm. August saw no less than 14 security bulletins for Microsoft products, of which 6 have been labelled as Critical, an all-time record of hotfixes to be issued on Patch Tuesday.

[4] Version 10 of the popular PDF reader application has been sandboxed in order to isolate the Reader’s processes from one another, as well as from the other processes on the system. By isolating them, the application runs everything in an extremely confined environment with a minimum of privileges on the respective machine.

Overview of Exploits

Early September brought into the spotlight a couple of 0-day flaws that have been simultaneously exploited in the Stuxnet corporate espionage tool. Apart from the notorious (and already patched) MS08-067 vulnerability used by the Conficker worm, Stuxnet brought into the game a new LNK (Windows Shortcut) flaw identified by BitDefender as Exploit.CplLnk.Gen, a zero-day bug in the Print Spooler Service that allows arbitrary code to be transferred and executed on a remote machine and two other flaws that allow elevation of privileges for malicious code to run as administrator. The impressive number of infections worldwide has propelled the Control Panel link exploit to the ninth place in the BitDefender H2 2010 malware top.

Popular media player Winamp has also been slammed with four critical vulnerabilities in the 5.x branch, which allow a remote user to successfully open a backdoor. The exploit code is embedded into a malformed MTM file and only triggers when the specific file gets loaded into the playlist or its properties are viewed.

Internet browsers have also had a hard time during the second half of the year. Most of the exploit packs that sell on underground forums, such as Eleonore and Crimepack, are equipped with malicious code to exploit flaws in Internet Explorer[5] and Firefox[6] browsers.

Late October also brought a series of exploits designed for Mozilla Firefox versions 3.5 and 3.6. The exploit code has been planted via iFrame injections on a series of high-profile websites such as the Nobel Prize webpage, among others. This specific exploit involves triggering a use-after-free error, a technique that has been successfully used by attackers in the IE8 Exploit in January, commonly known as Operation Aurora.

Another important 0-day bug on the Windows platforms has been discovered in late November and affects the Windows kernel itself. The vulnerability allows an attacker to bypass the User Account Control on systems running Windows Vista and Windows 7. A working proof of concept example, along with a step-by-step exploitation how-to has been available on an extremely popular programming forum for a couple of hours.

The exploit code relies on takes advantage of a programming flaw in the NtGdiEnableEudc() function in wi32k.sys. The proof of concept code author iterates through the open processes via IoGetCurrentProces() and looks for services.exe. When it is found, it copies its security token and overwrites the security token of another process (in this case, the piece of malware).

---

[5] These crimepacks include two exploit codes for Internet Explorer: MS09-002 (Internet Explorer 7 exploit 1/2009) and MDAC – ActiveX (Internet Explorer exploit, 3/2007).

[6] The only exploit for Firefox included in the Eleonore pack targets a vulnerability from 2005. New browsers are not vulnerable anymore to the Eleonore code.

Other Security Risks

In August security researchers have discovered a vulnerability in the way a multitude of applications are designed. This DLL loading flaw – also known as “binary planting” – affects the way applications try to load one or more DLL files from folders outside of the Windows directory. Shortly put, an attacker can run malicious code when a vulnerable file type is opened from within a directory controlled by the attacker.

This kind of exploitation is particularly possible when users run or load files from an extracted archive, a remote network share or a USB drive, even if the file opened by the user does not contain executable code.

To date, multimedia players are the most likely to be exploited, since the user perceives avi and mp3 file formats as safe. However, when loading them from a remote shared folder, the multimedia player will first look for and load one or more DLL files from the same directory as the opened file.

E-Threat Predictions

Year 2010 has been full of unexpected surprises in terms of security. The e-threat landscape has witnessed new and unusual activity, such as the advent of the Stuxnet worm. Also, the recent events related to the Wikileaks scandal has triggered a massive wave of protest from select groups of internet users, who turned their Low-Orbit Ion Canons against the institutions that withdrew support for Wikileaks or publicly condemned their actions.

The massive wave of distributed denial-of-service attacks has paralyzed network activity for Internet service providers, payment processors and government websites. Unlike regular DDoS attacks which rely on infected computers to launch the bulk of packets against their victim, this was a voluntary, coordinated effort of millions of users who willingly surrendered their computers to unknown persons to provide the necessary attack power.

Botnet Activity

For years, botnets have represented the backbone of the malware industry. These hordes of zombified computers can be used to send spam, launch DDoS attacks, provide 0-cost webhosting for phishing pages and malware, or to offer proxies for credit card fraud. The recent termination of the SpamIt service has dramatically reduced the amount of spam sent throughout the infected bots, yet it has not disturbed the botnet infrastructure in any way.

Throughout 2011, new spam affiliate programs will emerge, while the existing ones will consolidate, and spam production will ramp up to “normal levels”, with medicine spam as top product.

Along with conventional botnets comprised of infected computers, new threats will emerge from botnets created with users’ consent. These networks of computers will likely focus of performing DDoS attacks as forms of social protest against institutions that regulate the use of the Internet.

Malicious Applications

During 2011, malware authors will pay special attention to making their creations as stealthy as possible. The highly successful debut of malware signed with genuine stolen digital certificates or with counterfeit ones (as seen in Stuxnet and various variants of ZBot) will likely continue in 2011. Since some security solutions traditionally skip digitally-signed binaries from scanning, this approach allows the malware to install kernel-mode drivers even on Windows Vista and Windows 7.

Rogue everything: rogue antivirus software is hardly news. Since 2008, rogue AV hasn’t evolved much and users have started to tell the difference. 2011 will bring an even larger offering of utilities, ranging from rogue disk defragmenters to tune-up applications.

Social Networking

Social networking is becoming a global phenomenon: in less than 6 months, Facebook’s user base jumped from 400 to 500 million of active accounts, which post and update a great pool of personal data. Phishers may corroborate data from the social networking profiles with current workplaces and whereabouts to launch high-profile social engineering attacks and plant advanced persistent threats in corporate networks and use them for industrial espionage or for illegal purposes. BitDefender estimates that 2011 will bring a larger number of rogue applications and plugins for social networks, which will try to capitalize on the user by redirecting them to surveys or persuading them into installing adware.

Other Threats

Widespread access to HTML 5 as an incipient technology will offer the user new ways to interact with the online media. Since HTML 5 is currently implemented across all major browsers, it might become universally exploitable regardless of the operating system platform the browser runs on.

0-day exploits will also play a key role in the malware distribution circuit for 2011. With cyber-crime packs such as Eleonore, Crime Pack, Fragus, Siberia and the upcoming Ares exploit kit licensed to thousands of users, malware creation has become accessible to anyone, regardless of their level of technical knowledge.

Cross-platform malware: the emergence of the Java-based Boonana Trojan (Java.Trojan.Boonana.A) that affects both Mac OS X and Windows users has proven to be a successful experiment in writing one piece of malware for two of the most prominent operating systems in the world. It is likely that the number of multi-platform worms and Trojans will continue to grow during 2011.

Mobile Operating Systems

Smartphones are rapidly gaining market share and the increased presence of hotspots in urban areas is already offering unlimited Internet connectivity to mobile users. This will increase the number of phishing attempts taking advantage of the limited screen space on the mobile phone's display to trick the user into disclosing sensitive information while shopping or performing e-banking transactions.

The rapid rise of Google's Android operating system and the availability of an intuitive software development kit will simplify malware writers' efforts to create rogue applications for both Android-based phones and the upcoming Android-based tablet PCs.

Malware targeting Android phones is already here. There are a number of fake applications that dial to premium-rate numbers, as well as a botnet-capable latest e-threat dubbed "Geinimi" that steals personal data and contacts. Since Android is an open-source operating system which is also extremely flexible it won't take long for malware authors to bring up malware that takes full control over the infected phone.

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.