H1 2011 E-Threat Landscape Report

MALWARE, SPAM AND PHISHING TRENDS

bitdefender

Author

Bogdan BOTEZATU, Senior Communication Specialist

Contributors

Loredana BOTEZATU, Communication Specialist – Malware & Web 2.0 Threats

Răzvan BENCHEA, Malware Analyst
Dragoş GAVRILUȚ, Malware Analyst

Alexandru Dan BERBECE - Database Administrator

Dan VANDACHEVICI - Spam Analyst
Irina RANCEA – Phishing Analyst

Table of Contents

Table of Contents 3
Table of Figures 4
Overview 5
Malware Spotlights 6
Malware Threats in Review 7
World’s Top Countries Producing and Hosting Malware 7
Top 10 E-Threats for H2 2010 8
Botnet Intelligence 12
Web 2.0 Malware 14
Instant Messenger Malware 15
Social Networking Threats 16
Spam Threats in Review 18
Phishing and Identity Theft 21
Vulnerabilities, Exploits & Security Breaches 22
E-Threat Predictions 23
Botnet Activity 23
Malicious Applications 23
Social Networking 24
Mobile Operating Systems 24
Windows 8 Beta 24
Disclaimer 25

Table of Figures

Figure 1: Top 10 countries producing and hosting malware 7
Figure 2: Top 10 countries affected by malware 8
Figure 3: Top 10 most active families of malware 9
Figure 4: Most active botnets in H1 2011 13
Figure 5: Malicious links delivered through YIM 15
Figure 6: Win32.Worm.Pinkslipbot in action 16
Figure 7: Greeting Cards application active around Easter. It collects personal information 16
Figure 8: Propagation mechanism of a Facebook worm. The CAPTCHA is actually the comment 17
Figure 9: The alleged execution video is only available if the user fills in some surveys 18
Figure 10: Spam breakdown by category 18
Figure 11: Pharmacy-related spam message - simple e-mail template 19
Figure 12: Russian brides spam: clean template and no images attached 19
Figure 13: Malware-bundled spam message pointing to malware 20
Figure 14: 15 million active e-mail addresses used by Facebook members ready for spamming 21
Figure 15: Top 10 phished institutions and services during H1 2011 21
Figure 16: WoW phishing email - note the various typos 22

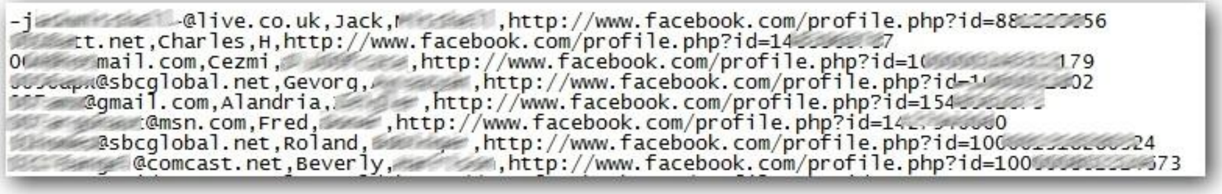
Overview

The first six months of 2011 have been placed under the sign of vulnerabilities and data breaches. While the malware landscape has witnessed little to no significant changes or epidemics, the numbers of data breaches and outages have increased considerably during the monitored period. IT security companies have been the primary targets of cybercriminals in an attempt to take them offline and, at the same time, to diminish their expertise in the eyes of their customers. Two of the most important IT security vendors that have been slammed with such attacks are HBGary and RSA, the security division of EMC.

Another major data leak followed by almost one month of outage was the Sony PlayStation Network incident, which exposed credit card details of about two million PSN users. The data leak was disclosed with a significant delay. The damage inflicted to users is yet to be estimated.

Significant outages have also happened in Egypt, following the massive wave of protests that took place on January 28. In order to prevent demonstrations and protests, the Egyptian government had all the local ISPs pull the plug on the Internet, thus rendering the bulk of electronic communications useless. The Internet blackout in Egypt has brought up endless debates on the importance of digital communications and the catastrophic results of outages.

Social networks have played a key role in maintaining a climate of insecurity. Although the number of e-threats especially designed to infect social network users (such as the infamous Koobface and Boonana worms) has dramatically decreased, cyber-criminals have focused their efforts on pushing an unprecedented number of rogue applications. The purpose of these virally/spreading applications is two-fold: on the one side, they redirect the users to websites where they are forced to fill in surveys; on the other side, these applications collect exhaustive information about their victims and their friends, which are later used in targeted spam and phishing campaigns.



```
-j[redacted]-@live.co.uk,Jack,[redacted],http://www.facebook.com/profile.php?id=88[redacted]56
[redacted]tt.net,Charles,H,http://www.facebook.com/profile.php?id=14[redacted]7
0[redacted]mail.com,Cezmi,[redacted],http://www.facebook.com/profile.php?id=1[redacted]179
[redacted]@sbcglobal.net,Gevorg,[redacted],http://www.facebook.com/profile.php?id=[redacted]02
[redacted]@gmail.com,Alandria,[redacted],http://www.facebook.com/profile.php?id=154[redacted]
[redacted]@msn.com,Fred,[redacted],http://www.facebook.com/profile.php?id=14[redacted]0
[redacted]@sbcglobal.net,Roland,[redacted],http://www.facebook.com/profile.php?id=100[redacted]24
[redacted]@comcast.net,Beverly,[redacted],http://www.facebook.com/profile.php?id=100[redacted]73
```

1.5 million leaked addresses, names and Facebook profiles available for free.

Malware Spotlights

- Autorun worms and Trojans account for the bulk of infections with almost 25 percent of the globally-identified infections. In order to protect the users from this increasingly persistent issue, BitDefender has released the USB Immunizer, a free tool that prevents Autorun malware from infecting USB and photo card storage devices.

- The web is still one of the most important vectors of infection. Attacks on high-profile websites is one of the most important methods of getting computer users infected by visiting their favorite resources. Osama Bin Laden's death and the Champions League are only two events that have brought Black-Hat SEO into the spotlight.

- Spam messages bundled with malware have witnessed a dramatic increase. While malware-bundled spam usually accounts for 1.5 percent of the total amount of unsolicited mail sent worldwide, it peaked to 7 percent and more in mid-April. Most of these messages carry variants of Bredolab and AsProx malware. The most important botnets in terms of malware spreading are Bredolab, Cutwail and AsProx.

- Spear phishing is the root of all evil: some of the high-profile data breaches that took place during the first half of 2011 have been built around phishing e-mails. The RSA incident that took place in late March was triggered by an e-mail message sent to some selected employees and carrying an excel file called "2011 Recruitment Plan"[1]. The file contained a malformed Flash applet that would install a backdoor through an Adobe Flash vulnerability (CVE-2011-0609).

- Mac OS X malware is slowly gaining ground as Apple's market share increases. During the first half of the year, BitDefender has identified multiple variants of rogue antivirus and recent discussions on underground forums hint about the development of a malware creation toolkit similar to Zeus.

[1] Full details on the data breach can be found on the RSA blog at http://blogs.rsa.com/rivner/anatomy-of-an-attack/.

Malware Threats in Review

The malware top for the first half of 2011 has suffered a variety of modifications, but the most important change 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.

World's Top Countries Producing and Hosting Malware

During the first six months of 2011, the most prolific countries in terms of malware productions have remained relatively unchanged as compared to the last half of 2010. The most important producers of malware are China and Russia with 31.30 and 21.88 percent, respectively. Ranking third, Brazil only accounts for about 8.40 percent of the globally-produced malware. Surprisingly enough, both China and Russia scored the very same percentages of malware as they did in the past semester. Brazil has ramped up production from 8.1 to 8.4 with a focus on banker Trojans built in Delphi.

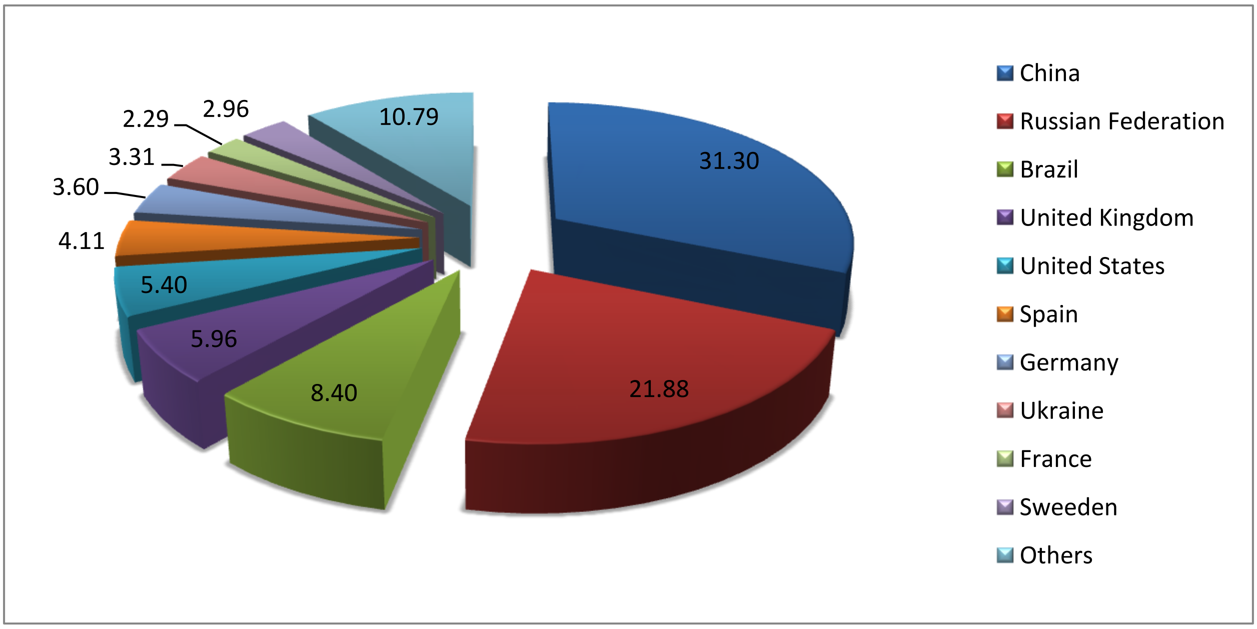


Figure 1: Top 10 countries producing and hosting malware

Other noteworthy producers of malware are the Republic of Korea (with 1.41 percent of the global amount of malware), Saudi Arabia (0.7%) and Canada (0.56%).

The most affected countries are France and the United States, which account for more than 25 percent of the global malware incidents logged by BitDefender. During the first six months of 2011, more than 500,000 computers in France have been exposed to various families of malware, ranging from average rogue antivirus scanners to devastating malware such as the Sality or Downadup families.

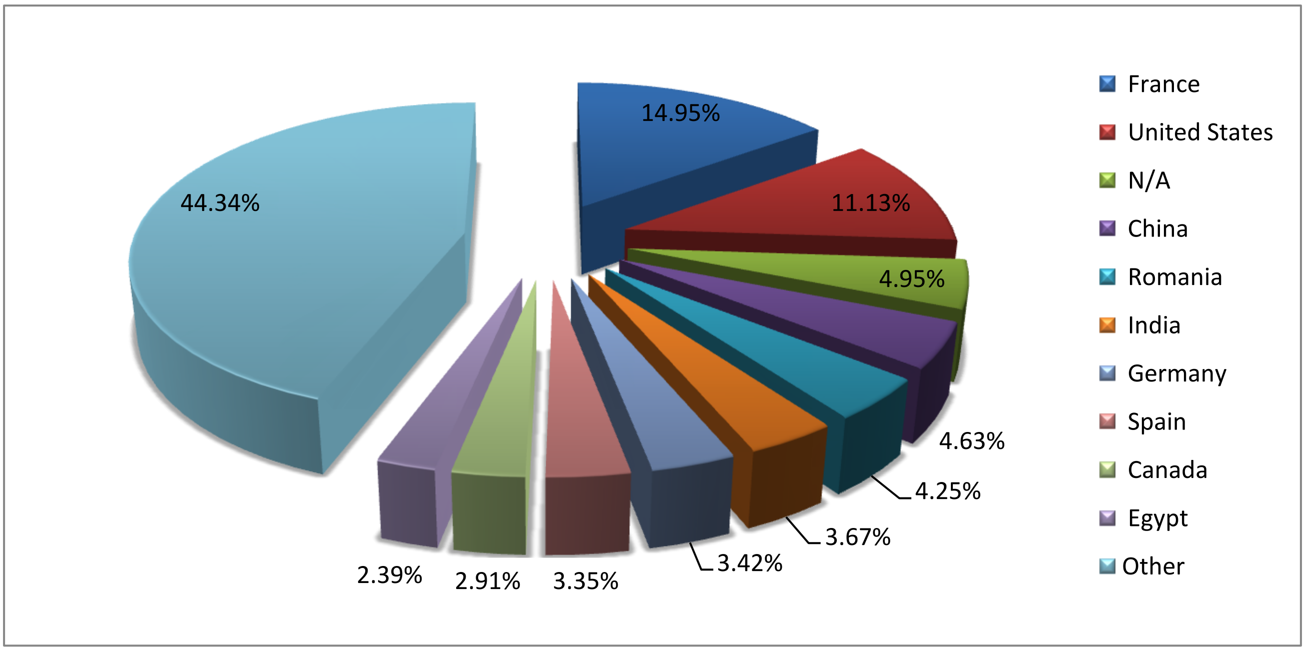


Figure 2: Top 10 countries affected by malware

Top 10 E-Threats for H2 2010

Although the number one e-threat for the first half of 2011 has remained unchanged since 2009, the top has witnessed some changes, with older malware moving to lower positions and software cracks taking a significant second place.

Multi-platform malware built in Java has also made an appearance, represented by Java.Trojan.OpenConnection.AI. This tool is a silent downloader that can fetch and execute a number of e-threats on the compromised computer. Other noteworthy presences are Exploit.CplLnk.Gen, one of the spreading mechanisms of the notorious Stuxnet worm and the Sality / Virtob combo of file infectors.

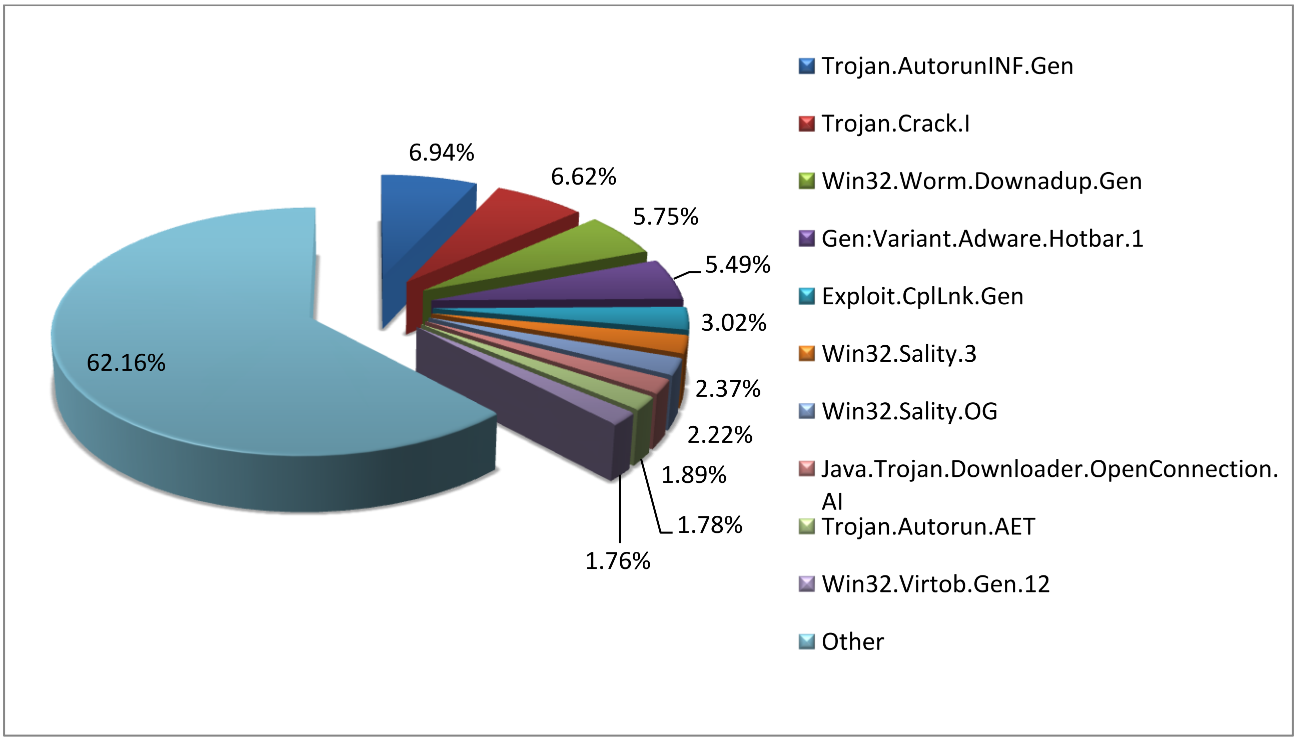


Figure 3: Top 10 most active families of malware

1. Trojan.AutorunINF.Gen

Trojan.AutorunINF.Gen is a persistent threat that has claimed the first place in the BitDefender malware top ever since the second half of 2009. With 6.94 percent of the global infections, the Autorun family still ranks as one of the most prolific breeds of malware, although its share has dropped significantly (from a whopping 10.42 in H2 2010). This generic detection deals with malformed autorun.inf files that usually accompany a couple of families of plug-and-play malware such as Win32.Worm.Downadup, Win32.Zimuse.A, Win32.Sality, Trojan.PWS.OnlineGames, Win32.Worm.Sohanad and Win32.Worm.Stuxnet.A.

Given the increased presence of the AutorunINF family of e-threats, BitDefender has released a free toll called the BitDefender USB Immunizer that protects USB sticks and CF / SD storage cards against these modified autorun.inf files. The BitDefender USB Immunizer is available for download on the product's page at the BitDefender Labs.

2. Trojan.Crack.I

Ranking second in the BitDefender malware top for the first half of 2011, Trojan.Crack.I is an e-threat that comes bundled with various “cracks” designed to defeat commercial protection of shareware applications. This e-threat is particularly present 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 running 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 it jumps straight on the second place with 6.62 percent of the global infections.

3. Win32.Worm.Downadup.Gen

Win32.Worm.Downadup hardly needs any introduction: it is the worm that has wreaked havoc in the computer industry ever since early 2008. Designed by a team of malware professionals whose identity has remained a mystery up until now, the worm has infected millions of computers worldwide. The worm uses a vulnerability in the Microsoft Windows Server Service RPC (also known as **MS08-67**) in order to propagate, but it can also "jump" from one infected flash drive to another. After it has infected the computer, the worm simply restricts access to the Windows Update service, as well as to most of the antivirus vendors' websites and then installs rogue antivirus applications. Win32.Worm.Downadup has dropped from the second to the third place in less than six months (with only 5.75 percent of the global infections), as more and more computer users are migrating from Windows XP to Windows 7, which is less vulnerable to Win32.Worm.Downadup infections.

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 ranks fourth with 5.49 percent of the global infections logged by BitDefender for the first half of 2011.

5. Exploit.CplLnk.Gen

Ranking fifth in the H1 2011 e-threat malware top, Exploit.CplLnk.Gen scores 3.02 percent of the global infections. As compared to the second half of 2010, the exploit has increased its presence with one percent, although a fix has been made available by the OS vendor. This detection is specific to lnk (shortcut) files that make use of a vulnerability in all Windows® operating systems to execute arbitrary code; this flaw has been extensively used by the Stuxnet worm to automatically execute itself as soon as an infected removable device is plugged into the computer.

6. Win32.Sality.3

Win32.Sality.3 is a specific detection that deals with file infectors in the Sality family. This family of viruses usually adds their malicious code in the last section of an EXE or SCR file. The Sality virus is able to infect executable files on local, removable and remote shared drives, which dramatically increases its destructive potential on networks.

Right after it has infected the system, the virus creates a list of exe and scr files, append their polymorphic code which has been heavily encrypted, and then modify the file’s entry point in order to execute the viral code every time the file is executed. This piece of malware also installs a rootkit driver, attempts to kill the local antivirus, and then installs a peer-to-peer (P2P) component to add the infected computer into a botnet.

Win32.Sality.3 ranks sixth in the BitDefender malware top with 2.37 percent of the total number of infections.

7. Win32.Sality.OG

Win32.Sality.OG is a variant of the Win32.Sality virus and ranks seventh with 2.22 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.

8. Java.Trojan.Downloader.OpenConnection.AI

Java.Trojan.Downloader.OpenConnection.AI is an e-threat written in Java that has been discovered in late 2010. Although it is relatively new in the e-threat landscape, this piece of malware is highly viral and can be found in the form of a Java applet on compromised or malicious websites promoted by cyber-criminals via social networks. This malicious Java applet downloads and executes arbitrary files and bypasses the Java sandbox by using the CVE-2010-0840 exploit. Java.Trojan.Downloader.OpenConnection.AI ranks eight in the BitDefender malware top with 1.83 percent of the globally-recorded infections.

9. Trojan.Autorun.AET

Ranking ninth in the H1 2011 E-Threat Landscape Report, Trojan.Autorun.AET is responsible for 1.87 percent of the infected computers around the world. This piece of malware spreads through the Windows shared folders, as well as through removable storage devices. In order to automatically execute, the Torjan uses an autorun.inf file placed in the root of the infected removable drive.

10. Win32.Virtob.Gen

Win32.Virtob ranks tenth with 1.76 percent of the global infections for the first half of 2011. This file infector is optimized for size, speed and stealth. Its code is exclusively written in assembly language and infects scr and exe files, but does not alter critical files belonging to the Windows operating system. Apart from infecting other files, the virus attempts to “call home” by connecting to an IRC server where it receives commands from its master. The virus has a backdoor component which allows an attacker to seize control over the machine and steal files, cookies, passwords or other critical information, as well as to install other e-threats.

Malware top for January – June 2011		
01.	**TROJAN.AUTORUNINF.GEN**	6.94 %
02.	Trojan.Crack.I	6.62%
03.	**WIN32.WORM.DOWNADUP.GEN**	5.75%
04.	Gen:Variant.Adware.Hotbar.1	5.49%
05.	**EXPLOIT.CPLLNK.GEN**	3.02%
06.	**WIN32.SALITY.3**	2.37%
07.	**WIN32.SALITY.OG**	2.22%
08.	Java.Trojan.Downloader.OpenConnection.AI	1.89%
09.	**TROJAN.AUTORUN.AET**	1.78%
10.	Win32.Virtob.Gen.12	1.76%
11.	OTHERS	62.16%

Botnet Intelligence

The botnet landscape witnessed a dramatic turn during the first six months of 2011, when two major botnets have finally met their end. The disappearance of these botnets, along with the termination of the Spamit affiliate business in the last months of 2010 dealt a major blow to the spam operations worldwide and changed the hierarchies of the most important botnets on the globe.

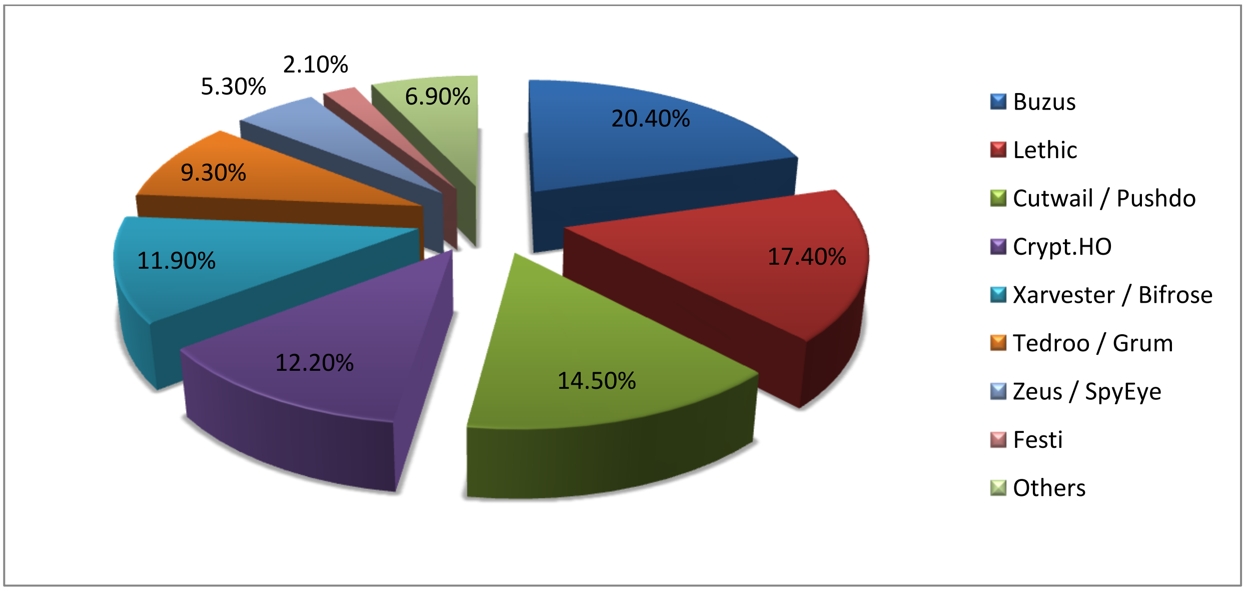


Figure 4: Most active botnets in H1 2011

The Rustock botnet, one known as the most important source of spam in the world, hit a dead end on March 11, when a coordinated action brought all the botnet's C&C servers offline simultaneously, thus disrupting communication and preventing the bots from updating. The takedown dramatically decreased the amount of spam mail sent worldwide, as Rustock was responsible for about half the amount of unsolicited mail coming from a botnet. The Spam Volume Index is now situated at 77.1 percent, a major improvement over the 85.1 percent recorded in H2 2011.

1. Buzus (a.k.a. Donbot)

Buzus has been around since 2009, but it never managed to gain a significant spot in the spam botnets' hall of fame, mostly because its abilities were no match to those of the elites of spam business such as Rustock, Pushdo and the likes. This unsophisticated bot uses plain-text communication and is capable of sending about 7,500 spam messages per hour from a single infected computer. This tireless spambot mostly deals with pharmacy and replica spam, along other minor side-businesses.

2. Lethic

Lethic is one of the botnets that has its origins in late-2007. Also small compared to the now-defunct Rustock botnet, the Lethic army of zombified computers is mostly known for its involvement in pharmaceutical and replica spam. It has survived an aggressive takedown in early 2010 which made its spam messages plummet to 0, but arose one month later when all the infected machines were able again to connect to the botnet’s C&C server located in the USA. Although its spam output can’t match the figures before takedown, it still relies important amounts of unsolicited mail.

3. Pushdo / Cutwail

Pushdo hardly needs any introduction, as it has been around long enough to show its capabilities. As one of the oldest botnets still active, Pushdo is responsible for a large share of spam mail, ranging from pharmaceuticals to “discounted OEM software”. The botnet is also famous for sending malware-bundled spam that apparently look extremely similar to announcements and alerts coming from social networking services. Pushdo supports a multi-faceted business in which customers can hire botnet power for a multitude of campaigns. The Pushdo bot is also active on instant messenger services, where it attempts to lure other contacts into downloading and installing the bot component.

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

The Maazben botnet is a constant presence in the BitDefender E-Threat Landscape Report. This medium-size botnet has been constantly growing since May 2009 and is mostly focused on promoting Casino spam to e-mail addresses belonging to Eastern-European citizens. It is one of the bots deployed by the notorious Sality family – a breed of file-infectors that also fetch and install other families of bots.

5. Xarvester / Bifrose

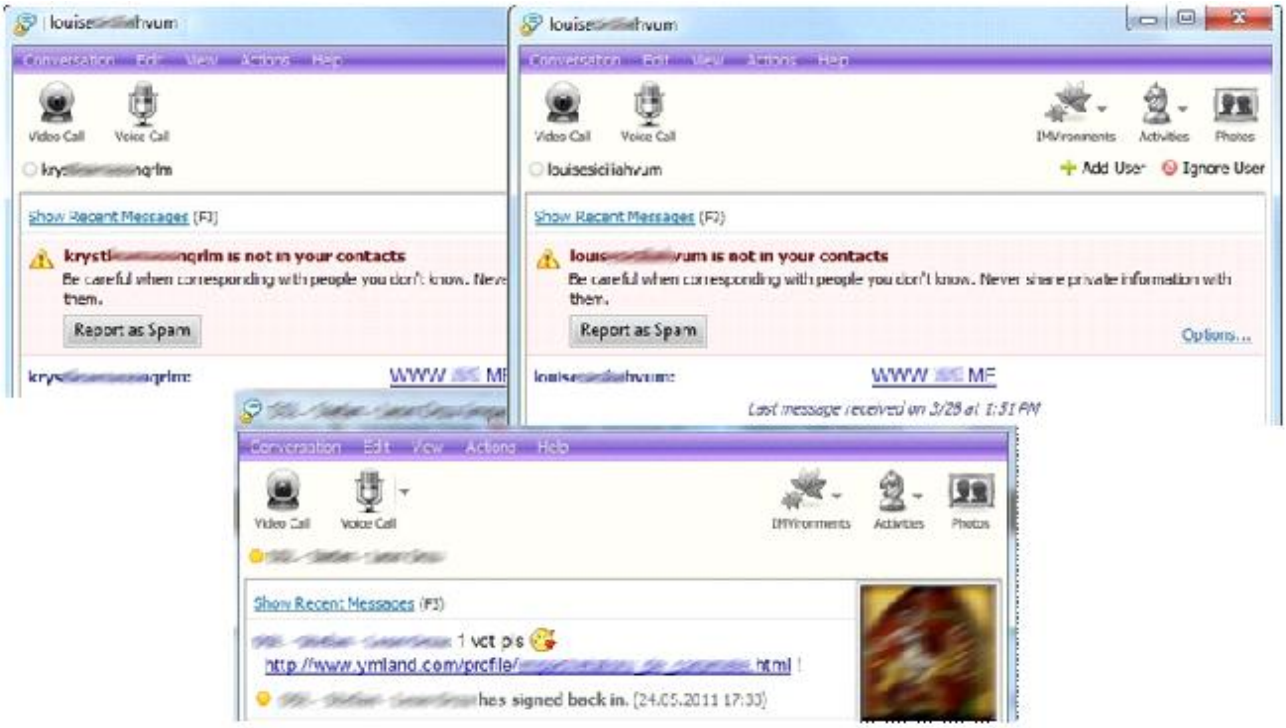
Xarvester is one of the mid-sized botnets that compensate for the lack of drones with an incredible amount of firepower. Every Xarvester bot is able to send about 25,000 messages per hour, most of these related to replica watches and pharmaceutical products. These bots share some common features with the Srizbi counterparts, which may suggest that Xarvester is a spinoff of the later.

Web 2.0 Malware

With Facebook surpassing 670 million registered members it is easy to figure that the popular social networking platform has become the number one target for cyber-criminals. Some of the most important developments during the first half of 2011 in the “social networking cyber-crime” are the emergence of a considerable number of rogue applications and the increase in links leading to surveys or malware.

Instant Messenger Malware

Instant messenger services are used by hundred millions users on a daily basis. They are flexible, easy to integrate in malware thanks to the multitude of APIs and SDKs available on the web and, most importantly, they have a viral potential.



kryst[redacted]nqrlm is not in your contacts
Be careful when corresponding with people you don't know. Neve
them.

kry[redacted]nqrlm: WWW [redacted] ME

louis[redacted]vum is not in your contacts
Be careful when corresponding with people you don't know. Never share private information with them.

louis[redacted]hvum: WWW [redacted] ME

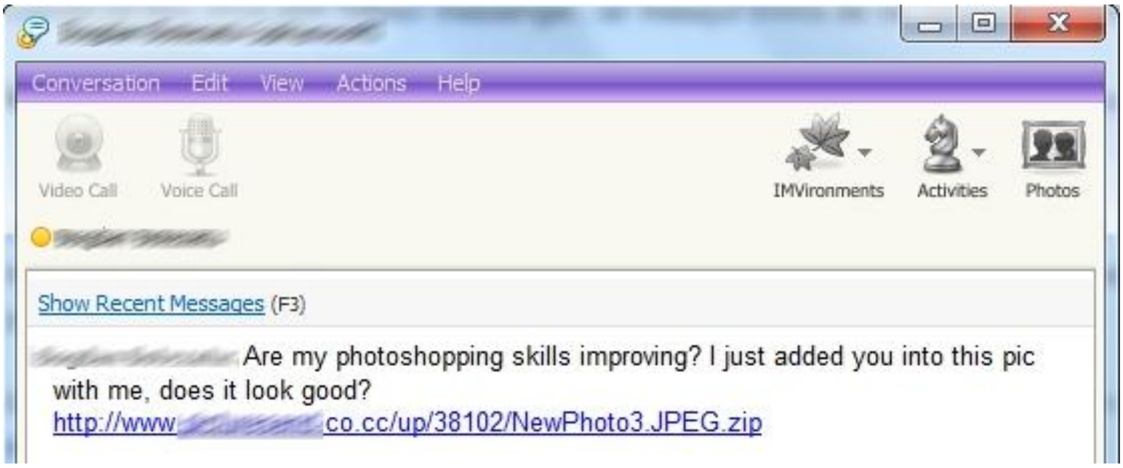
Last message received on 3/28 at 1:31 PM

[redacted] 1 vot pls
http://www.ymland.com/profile/[redacted].html !
[redacted] has signed back in. (24.05.2011 17:33)

Figure 5: Malicious links delivered through YIM

Most of the malicious links delivered through instant messaging platforms during the first half of 2011 were advertisements to online dating services or other websites with adult content. These messages are sent by computer users who have been infected with Yahoo Messenger bots, small applications written in Delphi that log into the user's account, fetch a list of messages from a remote location, and then start sending them to the user's contacts.

Instant messages with links to malware have also abounded during the first six months of 2011. The link is hosted on a .co.cc free domain and points to a .zip archive allegedly holding images. However, if the user tries to open the "image" inside, they will actually run the worm, which will continue to propagate from the freshly infected computer, but it would also fetch a modified version of Zbot from a remote location. Judging by the name of the domains called by the worm, this malware scheme seems to originate in Romania, although the malware is hosted in the United States.

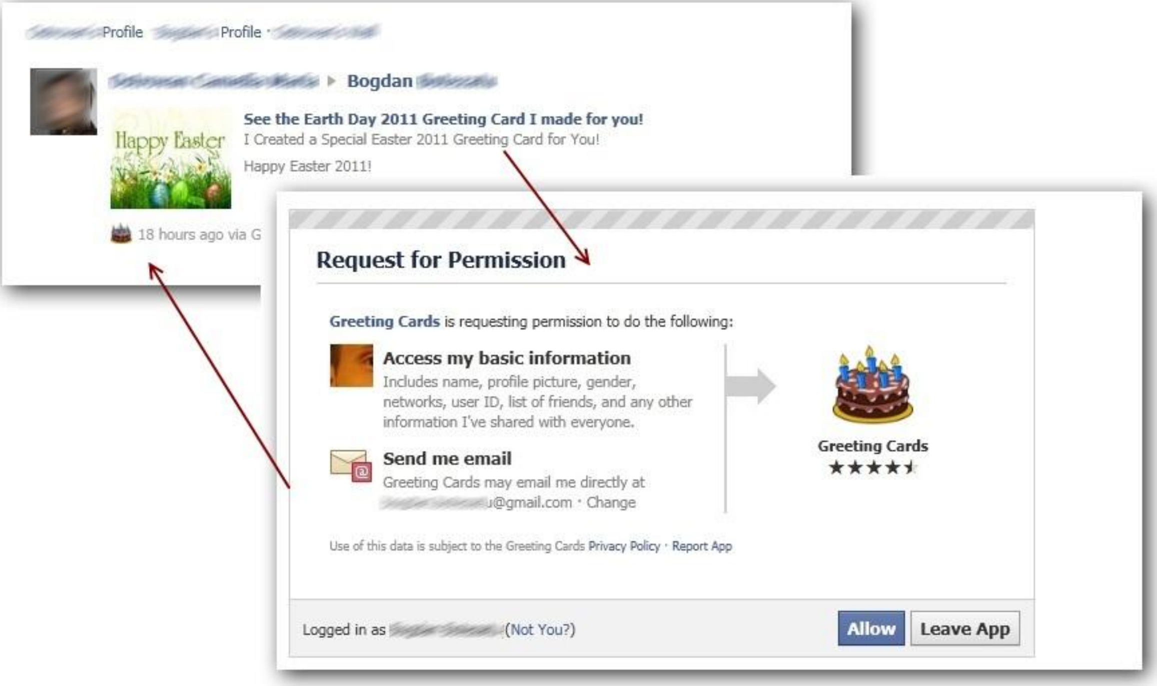


[redacted] Are my photoshopping skills improving? I just added you into this pic with me, does it look good?
http://www.[redacted]co.cc/up/38102/NewPhoto3.JPEG.zip

Figure 6: Win32.Worm.Pinkslipbot in action

Social Networking Threats

Social networks have also had their share of attention during the past six months with malicious activity spiking during the Easter holiday and around Osama Bin Laden's death. Most of these security incidents involve a rapidly-spreading worm that leads the user outside of the social network, where they are exposed to either malware or they are required to fill in a series of surveys before they are allowed to see the promised content.



[redacted] ▸ Bogdan [redacted]

See the Earth Day 2011 Greeting Card I made for you!
I Created a Special Easter 2011 Greeting Card for You!
Happy Easter 2011!

18 hours ago via G

Request for Permission

Greeting Cards is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

Send me email
Greeting Cards may email me directly at [redacted]u@gmail.com · Change

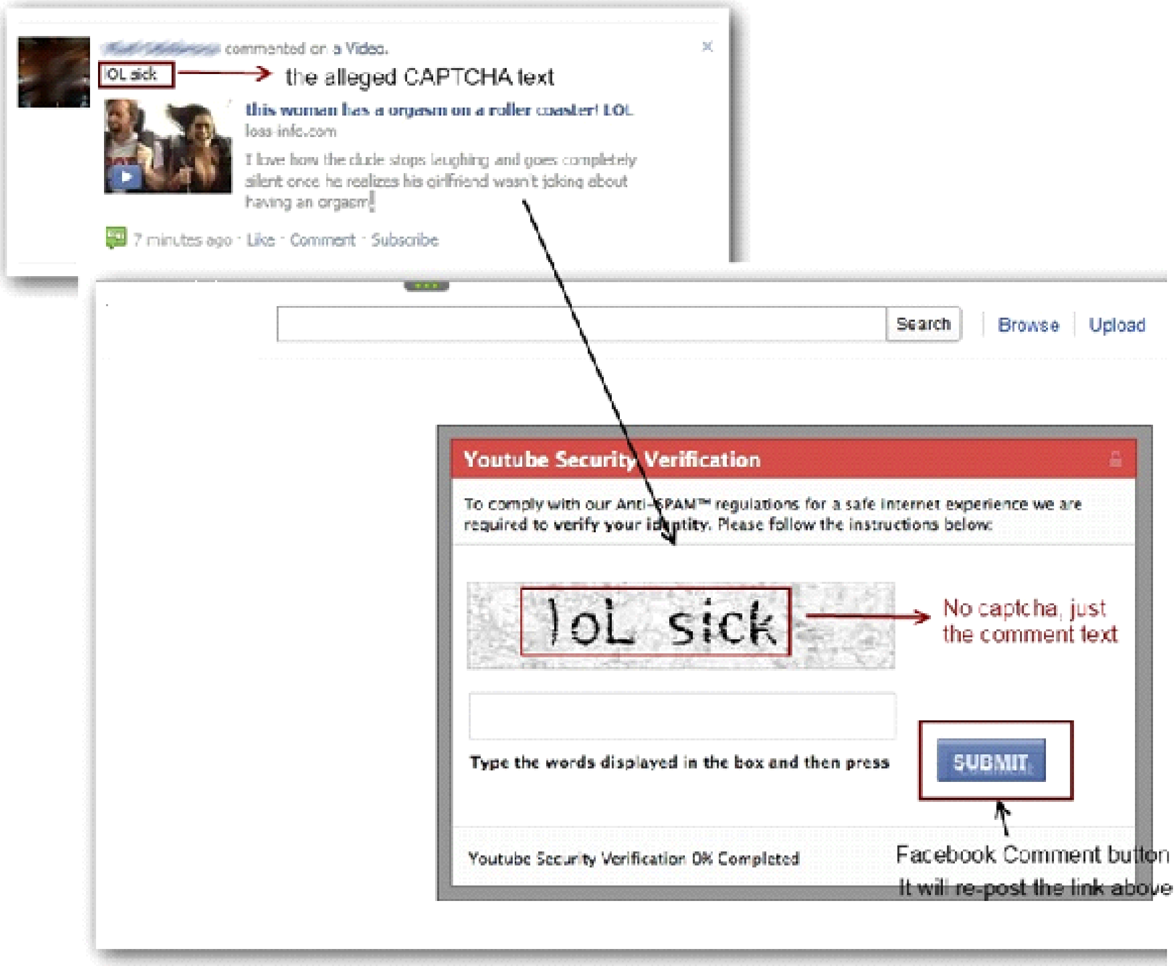
Greeting Cards
★★★★★

Use of this data is subject to the Greeting Cards Privacy Policy · Report App

Logged in as [redacted] (Not You?)

Figure 7: Greeting Cards application active around Easter. It collects personal information

Most of the rogue applications that emerged during the first six months of 2011 have 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 the 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, thus making itself visible to the victim's friends.



[redacted] commented on a Video.

lOL sick

the alleged CAPTCHA text

this woman has a orgasm on a roller coaster! LOL

loss-info.com

I love how the dude stops laughing and goes completely silent once he realizes his girlfriend wasn't joking about having an orgasm!

7 minutes ago · Like · Comment · Subscribe

Youtube Security Verification

To comply with our Anti-SPAM™ regulations for a safe internet experience we are required to verify your identity. Please follow the instructions below:

lol sick

No captcha, just the comment text

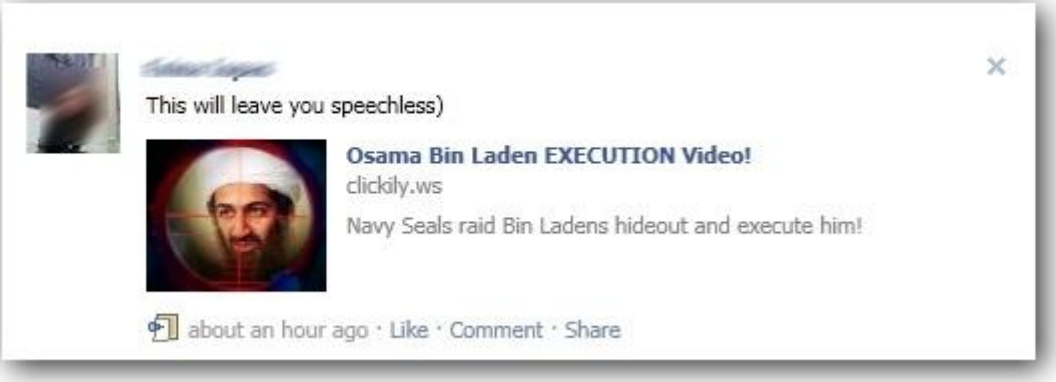
Type the words displayed in the box and then press

Youtube Security Verification 0% Completed

Facebook Comment button
It will re-post the link above

Figure 8: Propagation mechanism of a Facebook worm. The CAPTCHA is actually the comment

Osama Bin Laden's death has also brought a multitude of wall posts created by self-propagating worms. The main goal of these messages was to capitalize on the users' curiosity regarding the circumstances Osama Bin Laden passed away and lead them to pay-per-survey websites.



This will leave you speechless)

Osama Bin Laden EXECUTION Video!

clickily.ws

Navy Seals raid Bin Ladens hideout and execute him!

about an hour ago · Like · Comment · Share

Figure 9: The alleged execution video is only available if the user fills in some surveys

Spam Threats in Review

With Rustock out of the picture following the March 16 takedown, the spam landscape has witnessed significant changes. The Rustock botnet, once responsible for **half the amount of spam sent daily,** has been brought to a grinding halt. The result was visible almost immediately, as spam levels dropped significantly. The Rustock decline has complemented the disappearance of another significant spam source, namely the SpamIt affiliate program in September 2010.This affiliate program has been funding some of the world's top spammers to promote fake pill Web sites and its termination dealt a major blow to the Canadian Pharmacy business which – six months later – seems to be almost extinct.

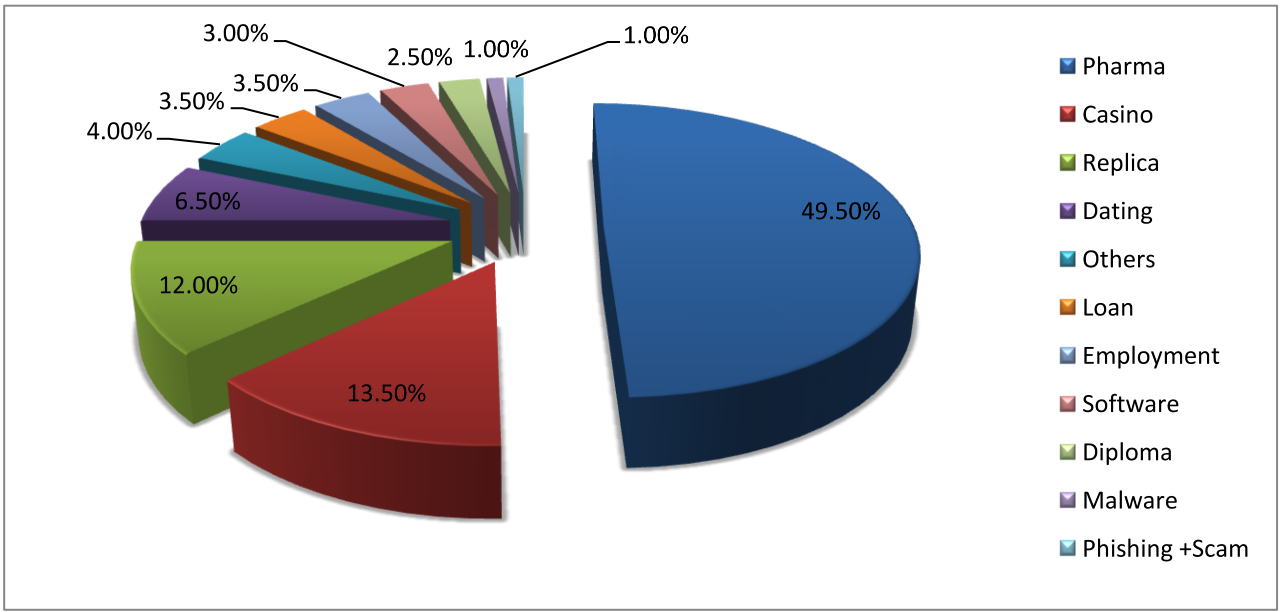
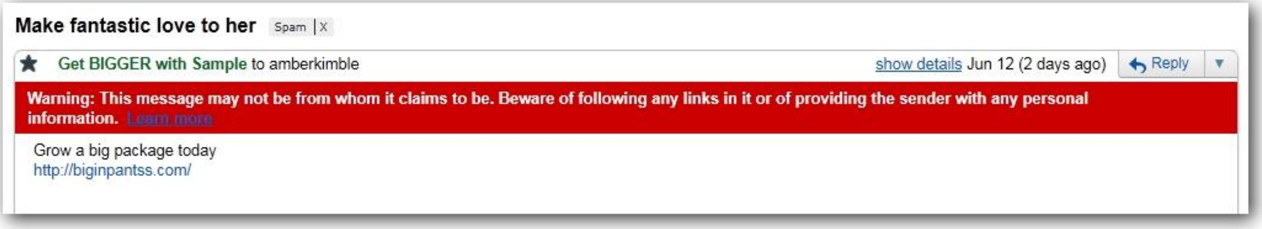


Figure 10: Spam breakdown by category

Although Rustock's disappearance has translated into a steep decline in pharmacy mail, this highly lucrative breed of spam hasn't just faded away completely. Most of the spam messages dealing with pharmacy spam are originating from Russia and China.



Make fantastic love to her Spam | X

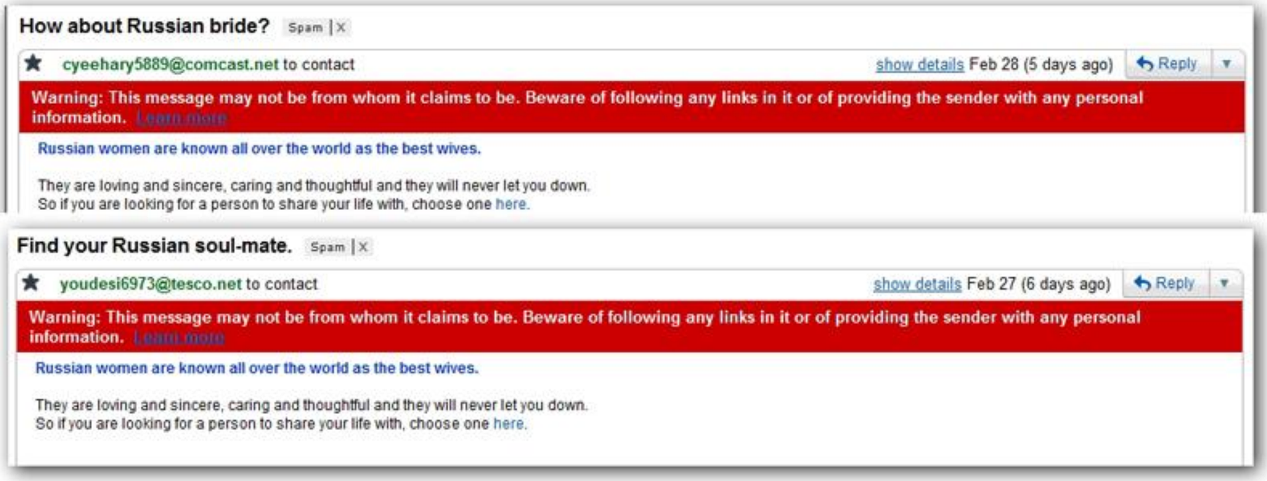
★ Get BIGGER with Sample to amberkimble show details Jun 12 (2 days ago) Reply

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

Grow a big package today
http://biginpantss.com/

Figure 11: Pharmacy-related spam message - simple e-mail template

Online dating spam has witnessed a massive increase as compared to the second half of 2010. The "Russian brides" scam is a common technique of luring unwary people from the west into visiting an online dating website with profiles of women looking for a soul-mate. As soon as they have fallen into the scam, they will be required to transfer significant sums of money into the bride's account to cover for the trip fees from Russia to the victim's location. However, as soon as the transfer has been made, the victim will never hear from the bride again.



How about Russian bride? Spam | X

★ cyeehary5889@comcast.net to contact show details Feb 28 (5 days ago) Reply

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

Russian women are known all over the world as the best wives.

They are loving and sincere, caring and thoughtful and they will never let you down.
So if you are looking for a person to share your life with, choose one here.

Find your Russian soul-mate. Spam | X

★ youdesi6973@tesco.net to contact show details Feb 27 (6 days ago) Reply

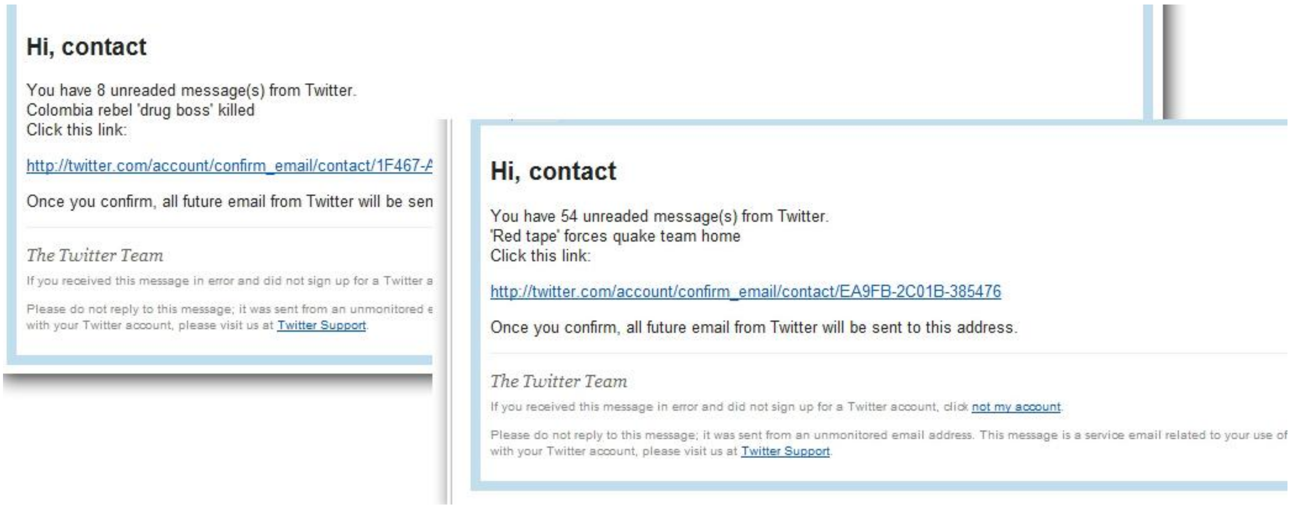
Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

Russian women are known all over the world as the best wives.

They are loving and sincere, caring and thoughtful and they will never let you down.
So if you are looking for a person to share your life with, choose one here.

Figure 12: Russian brides spam: clean template and no images attached

Spam messages accompanied by malware have also gained popularity following the termination of the SpamIt affiliate program. With little to no money left for medicine spam, botnet owners have focused their efforts into promoting a wide assortment of malware. One of the most persistent spam waves carrying malware was a Facebook password reset campaign that would end up with the victim installing a backdoor application. Other spam campaigns abusing the Facebook and Twitter brands have been launched throughout the first half of 2011.



Hi, contact

You have 8 unreaded message(s) from Twitter.
Colombia rebel 'drug boss' killed
Click this link:

http://twitter.com/account/confirm_email/contact/1F467-A

Once you confirm, all future email from Twitter will be sen

The Twitter Team

If you received this message in error and did not sign up for a Twitter a

Please do not reply to this message; it was sent from an unmonitored e
with your Twitter account, please visit us at Twitter Support.

Hi, contact

You have 54 unreaded message(s) from Twitter.
'Red tape' forces quake team home
Click this link:

http://twitter.com/account/confirm_email/contact/EA9FB-2C01B-385476

Once you confirm, all future email from Twitter will be sent to this address.

The Twitter Team

If you received this message in error and did not sign up for a Twitter account, click not my account.

Please do not reply to this message; it was sent from an unmonitored email address. This message is a service email related to your use of
with your Twitter account, please visit us at Twitter Support.

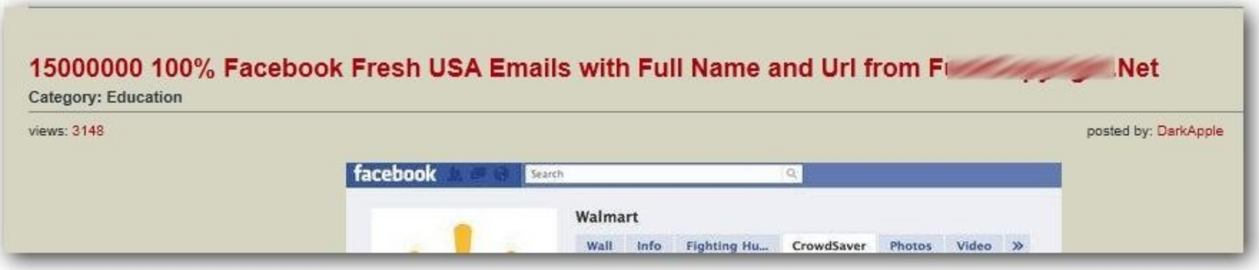
Figure 13: Malware-bundled spam message pointing to malware

Using the e-mail templates from Twitter official communications, cyber-criminals have set up spam campaigns informing the user that they have a number of unread messages which can be read by clicking on the provided link. Users following these links will end up downloading and installing a variant of the Zeus / SpyEye bot.

Spam Trends for H1 2011

The first six months of 2011 have brought a significant drop in spam messages following the takedown of the Rustock botnet in March. The spam volume index has dropped from 85.1 to 77.1 percent, which is one of the most important declines in the past years. On average, the size of a spam message is 2.5 KB with text as the format of choice for sending unsolicited mail. The Rustock takedown has also contributed to the dilution of the image-intensive spam such as the messages in the Canadian Pharmacy family.

On the other side, targeted phishing and spam attacks have increased their accuracy following the series of data breaches and corporate hacks that took place during the first half of the year. Early February has brought a series of attacks against high-profile military and political officials in the United States China and Taiwan who had their Gmail accounts compromised through carefully-planned spear-phishing. E-mail lists collected by rogue Facebook applications have also played an important role in the spam industry by allowing spammers to more accurately approach their targets and increase the possibility of selling what they are offering.



15000000 100% Facebook Fresh USA Emails with Full Name and Url from F[redacted].Net

Category: Education

views: 3148

posted by: DarkApple

Figure 14: 15 million active e-mail addresses used by Facebook members ready for spamming

Phishing and Identity Theft

The first half of 2011 has brought significant changes not only in the spam landscape, but also in phishing. While the last six months of 2010 have seen Facebook as the most phished brand on the globe, this year has brought financial institution into the spotlight once again. The phishing top for the first half of 2011 has PayPal and eBay leading with 54.74 and 12.41 percent, respectively. The gaming industry has also been an important target for cyber-criminals, especially the branches related to massive-multi-player RPGs such as World of Warcraft (ranking third with 7.29 percent) and RuneScape (ranking seventh with 3.63 percent).

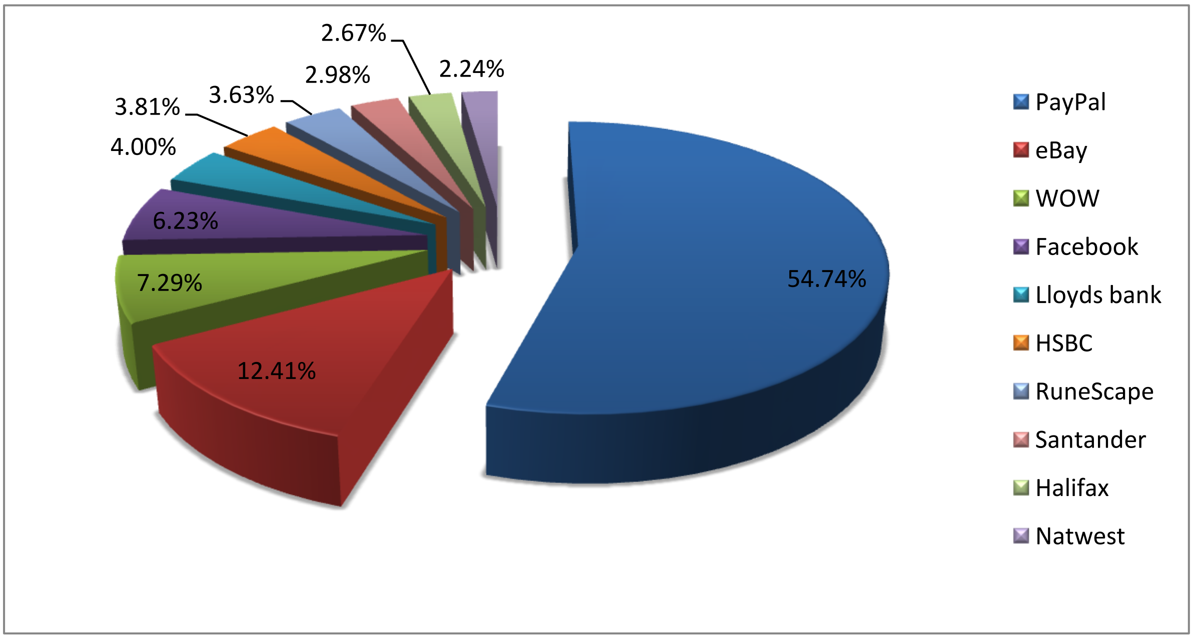
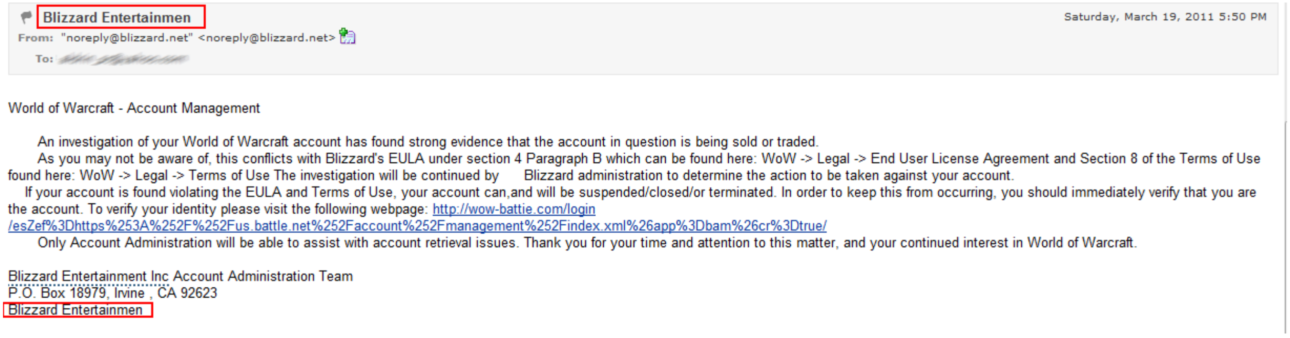


Figure 15: Top 10 phished institutions and services during H1 2011

Just like financial institutions, gaming phishing is an extremely lucrative business, as it offers the attacker access to a wide array of assets, such as the game’s serial key or even the character itself, things that can be easily sold on underground markets for real money.



Blizzard Entertainmen

Saturday, March 19, 2011 5:50 PM

From: "noreply@blizzard.net" <noreply@blizzard.net>

To: [redacted]

World of Warcraft - Account Management

An investigation of your World of Warcraft account has found strong evidence that the account in question is being sold or traded.

As you may not be aware of, this conflicts with Blizzard's EULA under section 4 Paragraph B which can be found here: WoW -> Legal -> End User License Agreement and Section 8 of the Terms of Use found here: WoW -> Legal -> Terms of Use The investigation will be continued by Blizzard administration to determine the action to be taken against your account.

If your account is found violating the EULA and Terms of Use, your account can,and will be suspended/closed/or terminated. In order to keep this from occurring, you should immediately verify that you are the account. To verify your identity please visit the following webpage: http://wow-battie.com/login /esZef%3Dhttps%253A%252F%252Fus.battle.net%252Faccount%252Fmanagement%252Findex.xml%26app%3Dbam%26cr%3Dtrue/

Only Account Administration will be able to assist with account retrieval issues. Thank you for your time and attention to this matter, and your continued interest in World of Warcraft.

Blizzard Entertainment Inc Account Administration Team
P.O. Box 18979, Irvine , CA 92623
Blizzard Entertainmen

Figure 16: WoW phishing email - note the various typos

Vulnerabilities, Exploits & Security Breaches

Year 2011 has been extremely rough with a multitude of high-profile businesses around the world. Following the WikiLeaks incidents in November last year, when Facebook and Moneybookers have ended their relationship with the website, cyber-activist group Anonymous have started a series of attacks against these websites as well as against others.

The series of attacks started with a raid against HBGary Federal following the official announcement of the company that it had infiltrated the Anonymous group. The cyber-activists responded with website defacement and a subsequent series of attacks which revealed 68,000 highly confidential e-mails that exposed details about a high quality offensive application.

On April 2 2011, the group of activists launched one of the largest attacks in history against media giant Sony. This attack, part of the Operation payback was allegedly their response to the legal action against George Hotz (known as GeoHot), a software developer who created and maintained a popular tool that allows unofficial software to run on the PlayStation 3 console. The attack took down the PlayStation Network and other related PlayStation websites. Subsequent attacks against the PlayStation Network have been carried by Anonymous spinoff group LulzSec, who managed to expose credit card details belonging to 1.5 million PSN users.

Another high-profile hack was announced on June 2nd, when Google revealed that group of unidentified Chinese hackers phished several e-mail credentials belonging to US government representatives, Chinese political activists, military personnel, journalists and other Asian officials. The attackers have carefully monitored their victims for a while, and then carried individual spear-phishing attacks that allowed them to seize control over the Gmail inboxes and syphon out work-related e-mail they have forwarded from their business inbox to the Gmail account. The impact of the attack has yet to be evaluated.

E-Threat Predictions

Without any doubts, the past six months have unfolded under the sign of the high-profile corporate data breach. These incidents have revealed the disastrous consequences of downplaying the need for security at the corporate level and gave a new dimension to the term **cyber-warfare**. Distributed denial of service and massive data leaks have been two of the most important threats to corporate networks and governments. Unlike other attacks against companies, these particular examples have had dramatic consequences not only for the company itself, but also for its customers whose data have been exposed.

Botnet Activity

Botnets are some of the most important tools used by cyber-criminal gangs. They have played a key role ever since the Internet boom and they will continue to be a valuable asset. However, the recent changes in the industry, such as the disappearance of the SpamIt affiliate program will force botmasters to find new approaches to capitalize on the infected computer.

The rest of 2011 will see botnets as one of the most important prerequisites for distributed denial of service attacks against companies and governments. The conventional botnets created after successful infection with bot software will be complemented by computer users who voluntarily enrol their machines to provide the necessary bandwidth for DDoS attacks.

Malicious Applications

During 2011, malware authors will focus on developing new e-threats spun off from leaked source-code from high-profile malware projects such as the Zeus crimeware kit. For the past six months, we have seen new families of malware that borrowed features from older versions of Zeus, and we expect this trend to continue throughout the second half of the year.

Mac OS X users will also have a rough semester ahead. As the company's market share surpassed the 10 percent mark, the OS X platform has become a viable target for cyber-crooks. We have already seen advanced Rogue AV applications such as the MacDefender. A new and complete crimeware toolkit for MacOS X is rumoured to be in the works, with plenty of features taken from the Wayland-Yutani project.

Social Networking

Social networking will continue to be the favourite destination for cyber-criminals. With a victim base of more than 670 million users, Facebook itself is a mine of personal information that can be used for a variety of purposes. The recent phishing incidents involving the US and Asian military officials have supposedly been carried out with data collected from social networks.

Rogue applications have also dramatically increased over the past six months. Profile Creepers and Top Profile Viewers are only two of the multitude of applications that funnel data from profiles to third parties looking for illicit gains. BitDefender estimates that 2011 will bring even more rogue applications that will try to force users into installing adware or disclosing their personal information.

Mobile Operating Systems

The rise of the Android platform has also brought an increased wave of malicious applications aimed at the mobile users. Google Android is an open-source platform that makes it extremely easy for a software developer to create and distribute third-party applications. We have already seen a flurry of malicious apps such as the Geinimi Trojan, as well as a series of banking-related apps that were actually used for phishing. BitDefender expects to see an increase of malicious apps during the next six months, especially in regions such as China, where there are no official Android Markets available and users tend to download applications from high-risk software repositories.

Windows 8 Beta

The upcoming release of Windows 8 from Microsoft will likely cause a series of malware infections. Widespread interest in early previews and betas will likely force users into downloading illegal copies of the software and cracks via peer-to-peer networks, which might result in total system compromise. In order to avoid this kind of incidents, you are advised to only download software from the vendor's website and never use cracks, tweakers or other any third-party applications that might interfere with the proper functionality of the software.

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.