# H1 2010 E-Threat Landscape Report

## MALWARE AND SPAM TRENDS

# Author

**Bogdan BOTEZATU**, Communication Specialist

# Contributors

**Loredana BOTEZATU**, Communication Specialist – Malware & Web 2.0 Threats

**Daniel CHIPIRIŞTEANU**, Malware Analyst
**Dragoş GAVRILUŢ**, Malware Analyst

**Alexandru Dan BERBECE** - Database Administrator

**Adrian MIRON** - Spam Analyst
**Irina RANCEA** – Phishing Analyst

# Table of Contents

# Overview

While 2009 was exclusively under the fateful auspices of the Conficker worm, 2010 shifted the malware balance towards e-threats using Web 2.0 services as main infection vector. With the Facebook® user base easily surpassing the population of the United States of America, it's not hard to imagine that malware authors have strengthened their efforts towards breaching the social networks's security in order to lay their hands on a massive amount of personal information.

Black-hat SEO has been yet another important vector for disseminating malware during the first half of 2010. Popular events, such as Mother's Day, Valentine's Day, or even natural disasters, such as the Guatemala tornado and the appearance of sinkholes, have been thoroughly capitalized by malware creators via various JavaScript attacks in an attempt to roll out Rogue AV or to deploy backdoors on unwary users' machines. The web remains the vector of choice for spreading malware, especially when paired with high-profile and extremely well populated social networks.

Critical 0-day exploits on popular software such as the Internet Explorer browser from Microsoft® or Adobe® Reader®, Adobe® Flash Player® and even Adobe® Photoshop® CS 4 have also played a key role in the malware landscape for the first half of 2010. Some of the Internet Explorer exploits have even been used to attack major companies such as Google, Adobe® and Rackspace®.

Ransomware Trojans have witnessed a spike throughout the first half of 2010. Most of the identified families of ransomware would target peer-to-peer users with alleged claims of copyright infringement lawsuits. One of the most eloquent examples of Torrent-based ransomware is Trojan.Maer.A, an e-threat which will be discussed later in this material.

File infectors and data-destruction viruses have made a comeback during the first three months of 2010. Although their stay in the wild was extremely short, their destructive potential overcompensated and resulted in significant damage, both in terms of money and in respects of user data.

For the first half of 2010, phishers have mostly focused on impersonating Paypal and eBay. The HSBC Bank ranks third, while Poste Italiene and EGG conclude the list of the most abused online identites

Pharmacy spam kept an ascending pace during H1 2010 and accounted for 66 percent of the global amount of spam. By contrast, during the latter half of 2009, pharmacy spam "only" reached 51 percent.

# Malware Spotlights

- Social networks and Web 2.0 services have become one of the most valuable channels of malware dissemination during the last six months. Malware authors usually rely on worldwide events and popular showbiz names to entice unwary users into downloading and running malware. The FIFA World Cup and the massive floods in Guatemala are only two of the many events used for Black-Hat SEO optimization to improve the ranking of various malware-serving websites.

- **Trojan.AutorunInf.Gen** is the number one enemy for the January – June 2010 timeframe. It accounts for 11,26 percent of the worldwide malware infections. The autorun technique is massively used by worm writers as an alternate method of spreading their creations via mapped network drives or removable USB / SD / CF media. Some of the most notorious families of malware using the Windows Autorun feature are Downadup, Palevo.

- Instant messaging worms have taken the malware game to a whole new level. Worm.P2P.Palevo.DP hit unprotected Yahoo!® Messenger and Windows Live® Messenger (formerly MSN® Messenger) users in early May 2010. The aggressively-spreading worm came with a bot component as payload, which was able to spam the worm further, as well as to download various pieces of malware on the breached machine. One week later, **Backdoor.Tofsee** slammed both **Skype™** and **Yahoo!® Messenger** users: this highly complex piece of malware featured a rootkit component[1] to protect its code against removal and analysis.

- MBR worms have made a comeback with upgraded viral mechanisms. Late January saw the emergence of Win32.Worm.Zimuse.A, a deadly combination of virus, rootkit and worm. Upon infection, the worm would start counting down the days. 40 days from the infection[2], it would overwrite the hard disk drive's Master Boot Record, thus rendering the OS unable to boot.

- Rogue antivirus software has been equipped with extra features aimed at forcing users into purchasing the useless applications. For instance, newer breeds of Rogue AV would seize complete control over the users' computer by limiting their access to some of the applications installed locally (ransomware behavior), or by sending significant amounts of data to their home base.

---

[1] For more details on Backdoor.Tofsee, please visit the Malware City description at http://www.malwarecity.com/blog/malware-alert-rootkit-based-skype-worm-opens-backdoors-810.html

[2] http://www.malwarecity.com/blog/malware-alert-win32wormzimusea-the-hard-disk-wrecker-736.html

- Phishing messages now account for only one percent of the worldwide spam – way down from the 7 percent recorded during the latter half of 2009.

# Malware Threats in Review

While the second half of 2009 was undoubtedly dominated by the Downadup worm, the main threats for H1 2010 are autorun-based e-threats. Ranking first in the malware top for the first half of 2010 is Trojan.AutorunInf.Gen, a generic detection that intercepts highly obfuscated autorun.inf files belonging to a wide assortment of malware families.

## World's Top Countries Hosting Malware

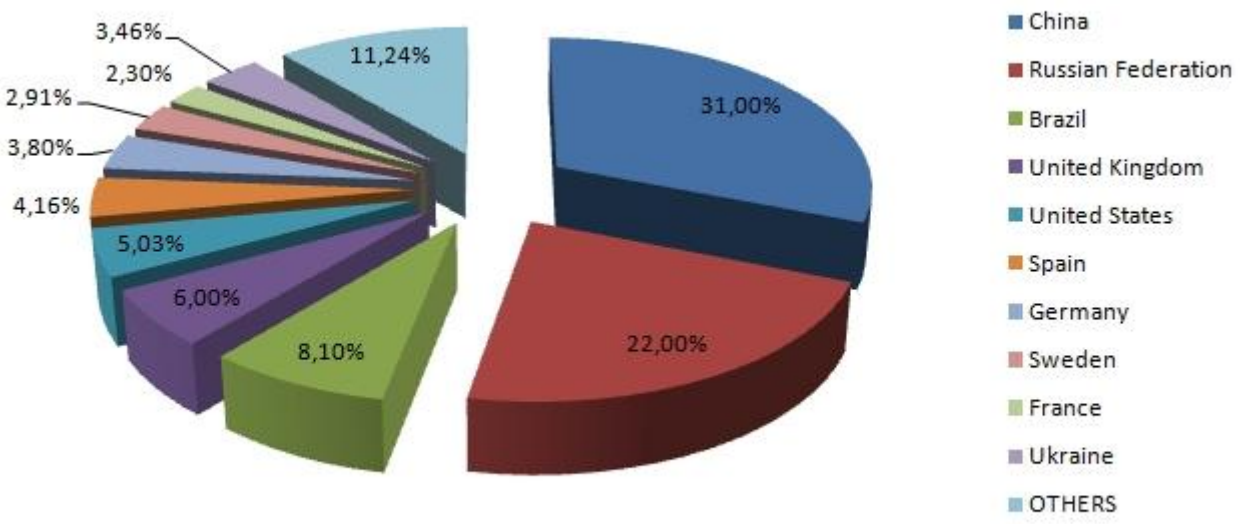



**Figure 1: Malware breakdown by country**

This report shows the breakdown of the top 10 countries hosting malware. During the last six months, China has been the most active country in terms of malware propagation, followed by the Russian Federation. Both countries are known for their lax legislation regarding cybercrime, as well as for the plethora of "bulletproof hosting" companies – such as the officially dead Russian Business Network (but extremely active in practice), Troyak (taken down in March 2010) or PROXIEZ-NET (gone as of May 2010).

If both the Russian Federation and China are the main hosters for Zeus C & C panels / exploit packs, and medicine spam mass-mailers, Brazil – ranked third – has an industry of its own: the highly

dangerous banker Trojans, usually written in Delphi[3]. The other countries in the top host diffuse malware.

| Malware top for January – June 2010 | | |
|---|---|---|
| 01. | TROJAN.AUTORUNINF.GEN | 11.26% |
| 02. | Win32.Worm.Downadup.Gen | 5.66% |
| 03. | EXPLOIT.PDF-JS.GEN | 4.80% |
| 04. | Trojan.Clicker.CM | 3.18% |
| 05. | WIN32.SALITY.OG | 2.9% |
| 06. | TROJAN.WIMAD.GEN.1 | 2.68% |
| 07. | EXPLOIT.PDF-PAYLOAD.GEN | 2.32% |
| 08. | Trojan.Autorun.AET | 2.08% |
| 09. | WORM.AUTORUN.VHG | 1.90% |
| 10. | Trojan.FakeAV.KUE | 1.76% |
| 11. | OTHERS | 6.46% |

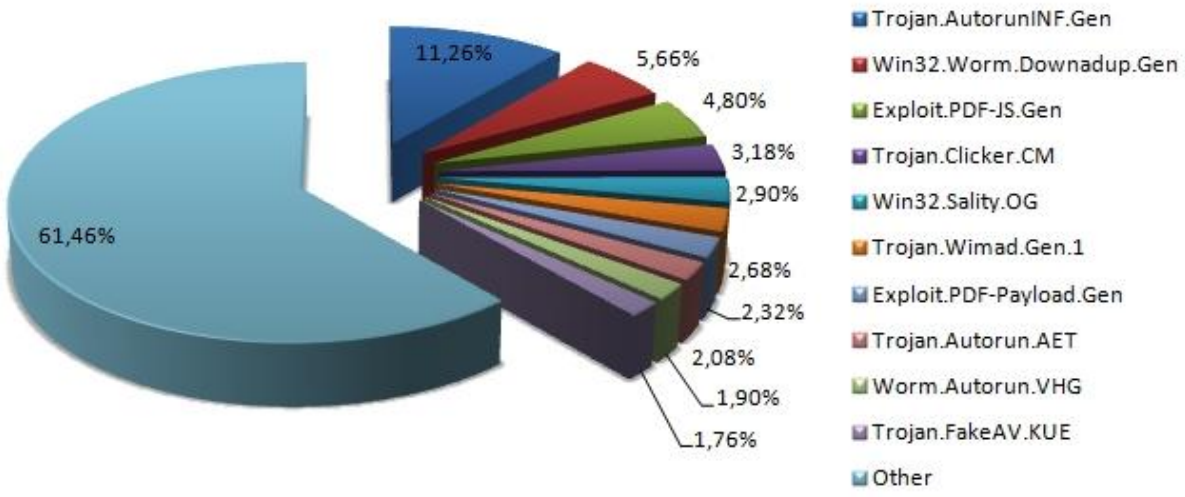



**Figure 2: Top 10 malware threats for H1 2010**

[3] For more details on the Brazilian Bankers, Man-in-the-Middle and Man-in-the-Browser attacks, please read the original article on Malware City at http://www.malwarecity.com/blog/banker-trojans-whos-been-spying-on-you-lately-781.html

## 1. Trojan.AutorunINF.Gen

Trojan.AutorunINF.Gen ranks first in the BitDefender half-yearly malware top with more than 11 percent of the total number of infections. Initially designed to simplify the installation of applications located on removable media, the Windows Autorun feature has been used on large scale as a means of automatically executing malware as soon as an infected USB drive or an external storage device has been plugged in. Unlike legit autorun.inf files, those used by miscellaneous malware usually come obfuscated, as depicted in the image below.

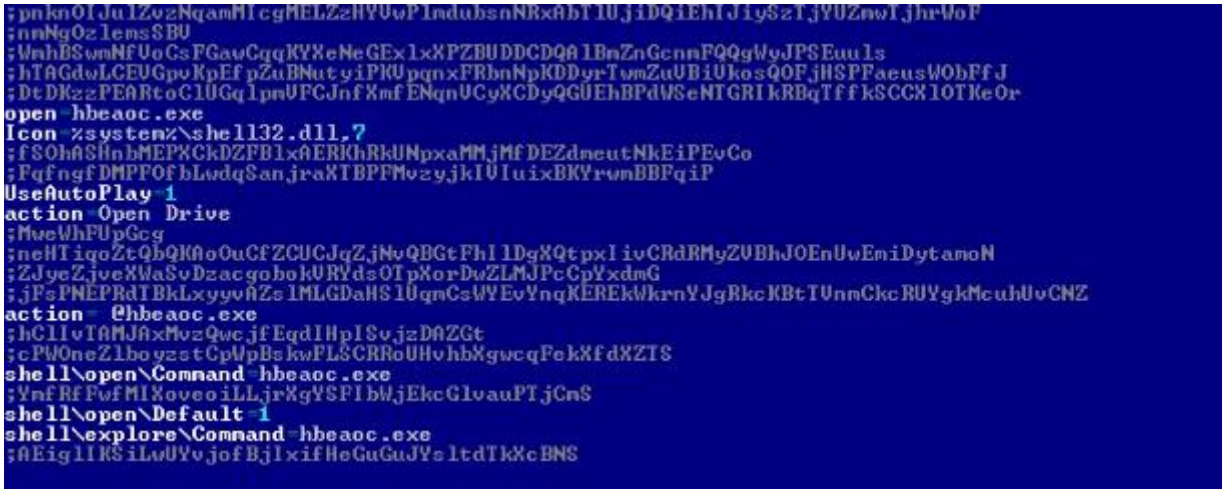



**Figure 3: Obfuscated, malicious autorun.inf file. The necessary parts of the autorun.inf file have been outlined in white.**

Some of the most representative pieces of malware abusing the autorun feature are Win32.Worm.Downadup and the new generation of peer-to-peer worms in the Palevo family.

Before the arrival of the second service pack for Vista, Windows-based operating systems would follow any autorun.inf file instructions and blindly execute any binary file the autorun file pointed to. Because of the risk the users were exposed to, Microsoft subsequently deactivated the autorun feature for all the removable devices except for the drives of type DRIVE_CDROM[4].

## 2. Win32.Worm.Downadup.Gen

Ranking second in the global infections top for H1 2010, **Win32.Worm.Downadup.Gen** hardly needs any introduction: during the last eighteen months it has managed to infect an unprecedented number of computers worldwide and it has made the headlines of about any computer magazine. The worm has obviously been engineered by a team of professional cyber-criminals, given the fact that it uses less-known Windows APIs and that it is extremely resilient to

[4] CD-ROM and DVD-ROM drives are read-only by default and can't be infected after they have been written to.

disinfection. For instance, the worm protects itself from deletion by removing all NTFS file permissions to all system users, except for the **execute** and **directory traversal** ones[5].

## 3. Exploit.PDF-JS.Gen

This conglomerate of PDF exploits ranks third in the BitDefender half-yearly top with 4.80 percent of the total number of infections. This generic detection deals with specially crafted PDF files exploiting different vulnerabilities found in the Javascript engine of Adobe® Reader® in order to execute malicious code on user's computer. Upon opening an infected PDF file, a specially crafted Javascript code triggers the download of malicious binaries from remote locations.

## 4. Trojan.Clicker.CM

**Trojan.Clicker.CM** scores 3.18 percent of the total number of infected computers. During the first six months of 2010, Clicker.CM has been mostly detected on websites hosting illegal applications such as cracks, keygens and serial numbers for popular commercial software applications. The Trojan is especially used to force advertisements as popup windows in order to boost cyber-crooks' advertisement revenue.

## 5. Win32.Sality.OG

The fifth place, with 2.90 percent of the infections triggered globally, is taken by **Win32.Sality.OG**. This e-threat is a polymorphic file infector that appends its encrypted code to executable files (.exe and .scr binaries). It deploys a rootkit and it kills antivirus applications running on the computer so as to hide its presence on the infected machine.

## 6. Trojan.Wimad.Gen.1

Ranking sixth in the BitDefender malware top for the first half of 2010, Trojan.Wimad.Gen.1 exploits a feature built in ASF and WMV files, which allows their creator to specify a URL where the appropriate codec is to be found if it is not installed on the system. However, as the Windows Media® Player attempts to play the file, it tries to download and install the specified codec which – most of the times - turns out to be an adware video player or a rogue antivirus delivered under the guise of a Flash update.

[5] For more information on the Downadup worm, as well as for our free disinfection tool, please visit http://www.bitdefender.com/VIRUS-1000462-en--Win32.Worm.Downadup.Gen.html

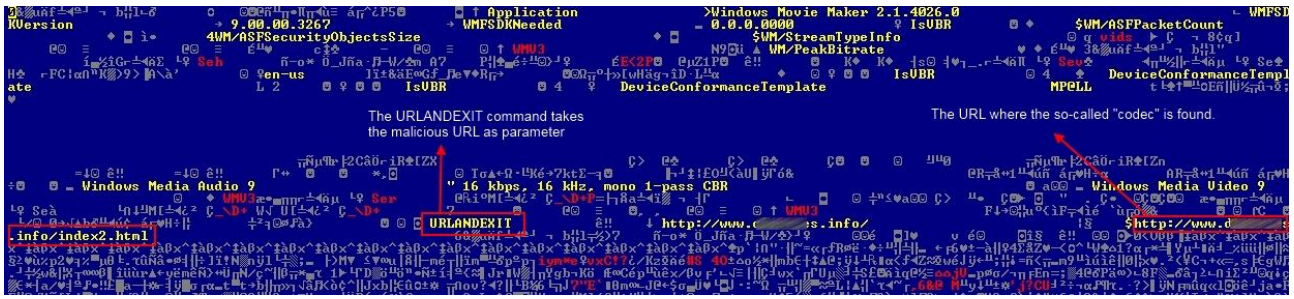



**Figure 4: URLANDEXIT and the redirect link**

Most of the video files that abuse this feature are shared via peer-to-peer and torrent websites and usually impersonate either block-buster titles or highly-anticipated episodes of miscellaneous series.

## 7. Exploit.PDF-Payload.Gen

**Exploit.PDF-Payload.Gen** ranks seventh in the malware top for H1 2010 with 2.32 percent of the total number of infections. It is a generic detection dealing with specially-crafted Portable Document Format (PDF) files that attempt to exploit vulnerabilities in Adobe® Reader®.

## 8. Trojan.Autorun.AET

**Trojan.Autorun.AET** is a piece of malware that spreads through the Windows shared folders, as well as via removable media (network attached storage devices or mapped drives). The Trojan exploits the Autorun feature implemented in Windows operating systems to automatically execute itself when an infected device is plugged in. It ranks eight and it accounts for 2.08 percent of the worldwide infections.

## 9. 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 (an approach also used by **Win32.Worm.Downadup**). The worm ranks ninth with 1.9 percent of the global infections.

## 10. Trojan.FakeAV.KUE

**Trojan.FakeAV.KUE** concludes the H1 2010 malware top with a percentage of 1.76 of the total number of infections. This detection blocks the JavaScript code that is used inside webpages to trigger fake alerts and animated scan simulations. These scripts are hosted on malicious sites, as well as legit web services that have been compromised.

## Traditional Botnets

Botnets are the ultimate tools of trade for malware authors, since they can be practically used for anything related to malware, from sending spam to performing massive DDoS attacks. Parts of botnets are sold or lent on a project basis to different groups of cyber-criminals in order for such groups to carry out their own projects.

During the first half of 2010, the most important botnets in terms of size and activity have been Rustock (which almost doubled in size as compared to H2 2009), Kobcka (14.5%) and Kolab (11.2%).

While Rustock is shielded by multiple layers of protection, including a rootkit driver and massive code encryption, the Kobcka bots stealthily download their spam components (the Cutwail bots) at runtime and inject them into critical processes such as svchost.exe. This approach allows the Kobcka botnet to ensure that the Cutwail bots are loaded even if all the existing Cutwail C & C servers have been taken down.

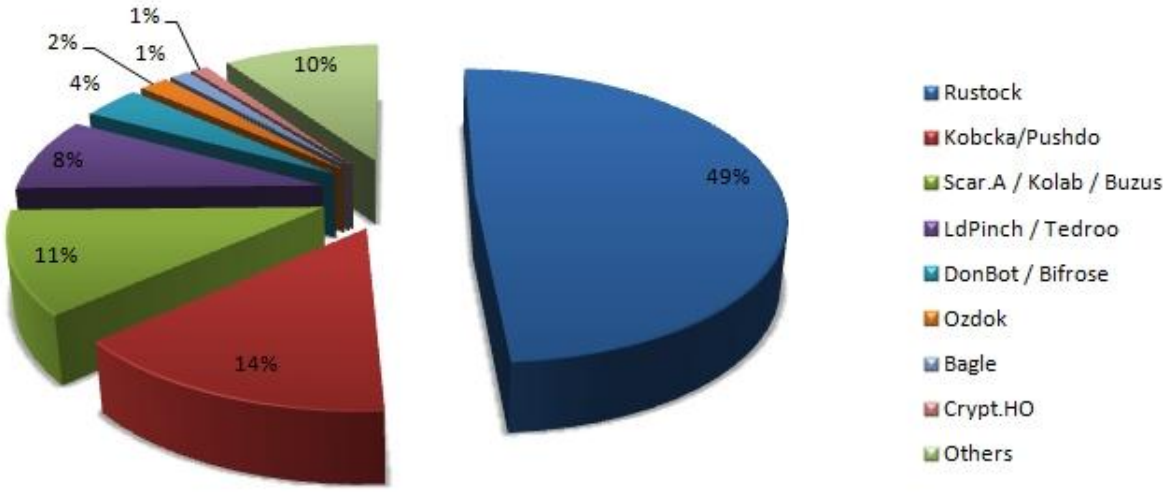



**Figure 5: Botnet activity by bot family**

## Web 2.0 Botnets

For years, the use of Web 2.0 botnets was thought to be a less practical approach than the IRC-based one, simply because each bot would require a separate account registered with the Web 2.0 service provider.

However, recent developments that started in August 2009 and continued throughout the first half of 2010 revealed that malware authors are ready to bridge the potential technological shortcomings and move the botnet front in the cloud. This year saw the emergence of the first viable botnet based on Twitter, though minimalistic enough to be called a proof-of-concept.

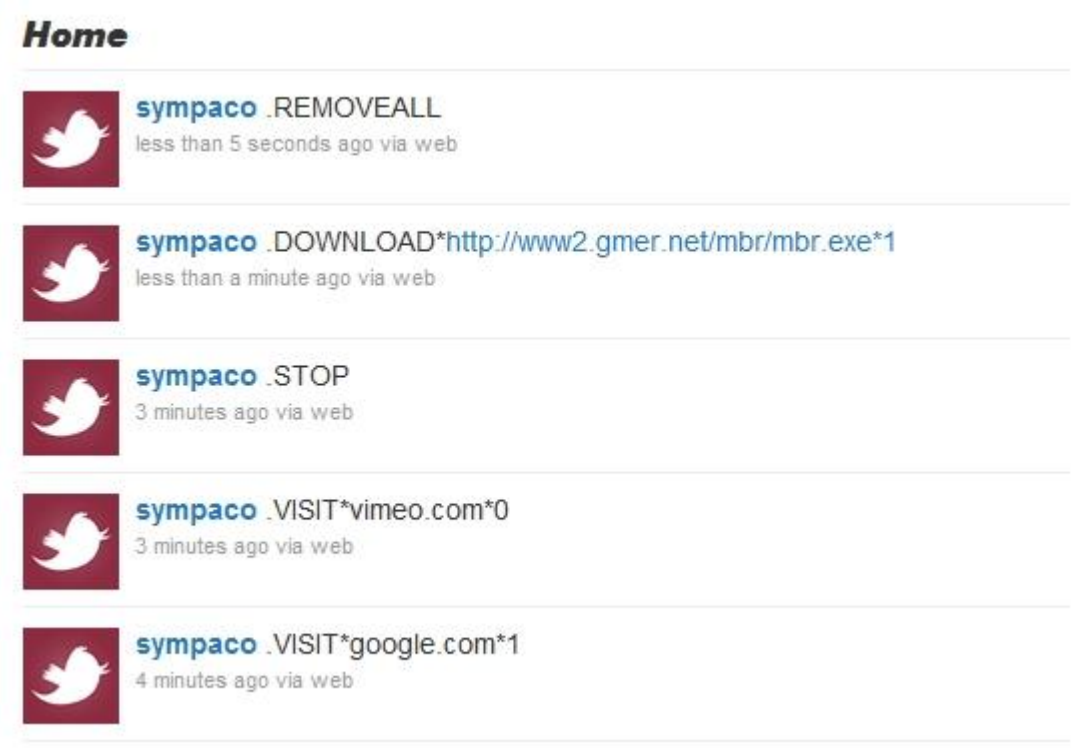



**Figure 6: "Rogue" Twitter account used to send commands. Please note that this is a research account and has nothing to do with a botnet in the wild.**

The bots used to subvert Windows-based machines have been created using a DIY tool called TwitterNET, where an attacker can specify the Twitter username the bots should monitor for issued commands. A second iteration of the self-development toolkit is also in the wild and comes with extra configuration options as far as the issued commands are concerned.

There are two major issues that required for the mentioned SDK upgrade:

A) The weakest link of a Twitter-based botnet infrastructure is the single-point-of-failure C & C (the herder's username); if it gets suspended, the whole botnet would aimlessly look for commands that will never be issued;

B) Such usernames are easily identifiable. Figure 6 shows how suspicious an attacker's account would look after issuing several commands. A Twitter search for ".REMOVEALL" would reveal all the compromised accounts which would subsequently be suspended.


**Figure 7: The second version of the TweBot Builder supports custom commands**

Botnets based on Youtube have also been spotted by analyzing the "background noise[6]" left as comments for specific videos. However, the scale of such botnets is dramatically limited by the fact that – to our knowledge - there is no publicly-available DIY bot creator.

## Web 2.0 Malware

During the first six months of 2010, most malware has been disseminated via the Internet, with cyber-criminals paying special attention to Web 2.0 services such as social networks, instant messaging and peer-to-peer file-sharing websites.

### Instant Messaging Malware

May 2010 brought a series of e-threats targeting unprotected users of Yahoo!® Instant Messenger and Skype™. Initially spotted in Romania, the Delphi worm **Win32.Worm.IM.J** was more than a YIM worm spreading at will - the built-in downloader component opens the door to other high-risk e-threats.

**Win32.Worm.Palevo.DS** followed shortly after and took by assault users of both Yahoo!® Messenger and Windows Live® Messenger (formerly MSN® Messenger). This particular descendant of the Palevo

[6] The so-called background noise is encoded using the base64 algorithm to conceal the commands issued by the bot-herder. However, since base64 comments look suspicious enough and are extremely easy to decode, the approach does not seem to be efficient for a large-scale botnet based on Youtube.

family has a special feature allowing it to kill the Windows Firewall, a critical step in the malware offensive which will be triggered by Palevo's spam component after infection completes.

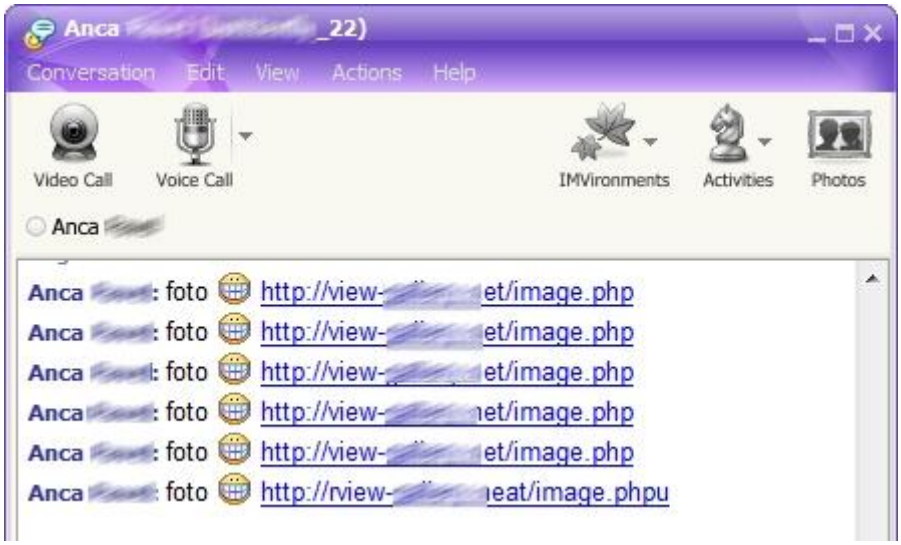



**Figure 8: Messages sent by Win32.Worm.Palevo.DS to entice users into downloading a copy of itself.**

Mid-May brought **Backdoor.Tofsee** back into the spotlight. This incredibly powerful backdoor was particularly targeted at Skype™ and Yahoo!® Messenger users, and only systems running either of the applications could be infected. Should the backdoor not find either of these IM clients, it would exit silently and remove itself from the system.

**Backdoor.Tofsee** is shielded by a rootkit driver and features multiple layers of protection in order to make analysis and removal extremely difficult. Apart from its worm-like spreading, mechanism, **Backdoor.Tofsee** also features a backdoor component that allows a remote attacker to take **complete control** over the infected machine.

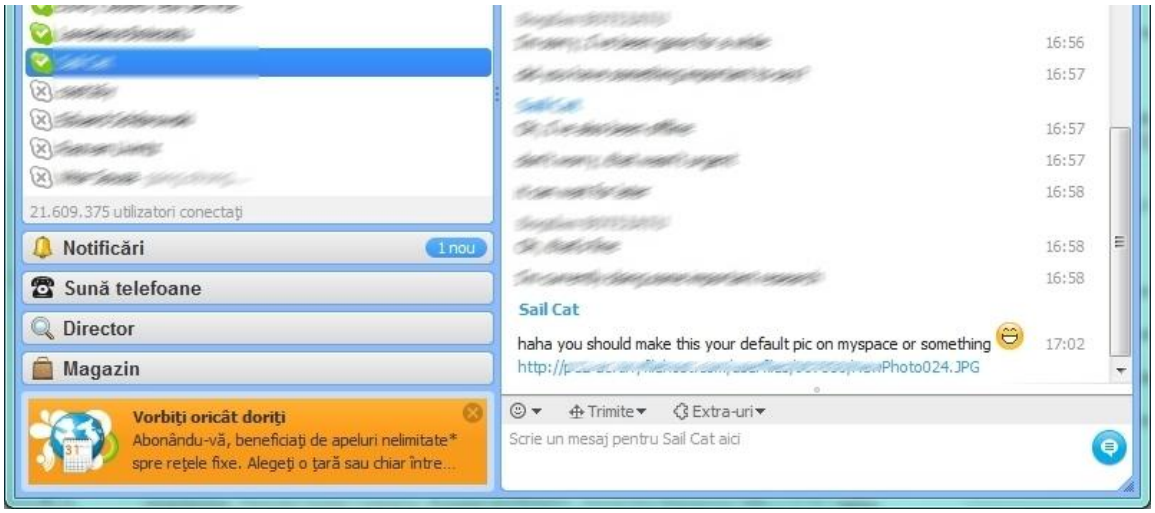



**Figure 9: The worm only sends messages during already initiated conversations in order not to raise suspicion.**

## Peer-to-Peer Malware

April saw the emergence of a new and innovative type of malware set to extort money from faint-hearted users that were into Peer-to-Peer downloads. This new e-threat, detected by BitDefender as **Trojan.Maer.A**, hit the web on April 11 and it mainly targets computer users who download files via sharing services based on the BitTorrent® protocol. Shortly put the ransomware Trojan claims that it had found pirated content installed onto the system (even on clean, 100% genuine Windows® installs) and "offers" to settle things for as much as $399.85.

In order to gain credibility, the Trojan displays a couple of organization logos including RIAA® and MPAA®. The piece of malware is packed full with links to an organization called ICCP Foundation, which poses as "a law firm assisting intellectual property holders exploit and enforce their rights globally[7]". It also displays a list of "pieces of evidence", made up by all the **.torrent** files the user may have downloaded to the %AppData% folder.


**Figure 10: Warning message displayed by the ransomware Trojan.**

[7] As advertised on the (now suspended) webpage of the fake foundation.

After successfully infecting the system, the Trojan would behave like an average rogue AV by displaying numerous popups reading “Copyright infringement”, and by performing various browser redirects to the ICCP Foundation home page.

Fake codec scams have been around for quite a while now, and they always end badly for the end-user. Some of the most common approaches of squeezing extra money from unwary users have one single root: **Trojan.Wimad**. This specific Trojan relies on a feature included in the ASF file format[8] specifications in order to direct the user to a web location that can provide the proper codec, in case such codec is not be installed on the system.

**Trojan.Wimad** is mostly pushed on Peer-to-Peer websites under the guise of block-buster movies that sometimes haven’t even been premiered yet. As soon as the user launches the pirated movie using Windows® Media Player, they will be redirected to a website selling a video player application that will allegedly allow them to watch the movie.

Needless to say that the movie will not play even after the brand new player has been paid for and installed. Please note that the player is advertised as $0.95, but this price only covers the first three days of trial. If subscription is not cancelled within three days, the user will be charged $29.95 per month.

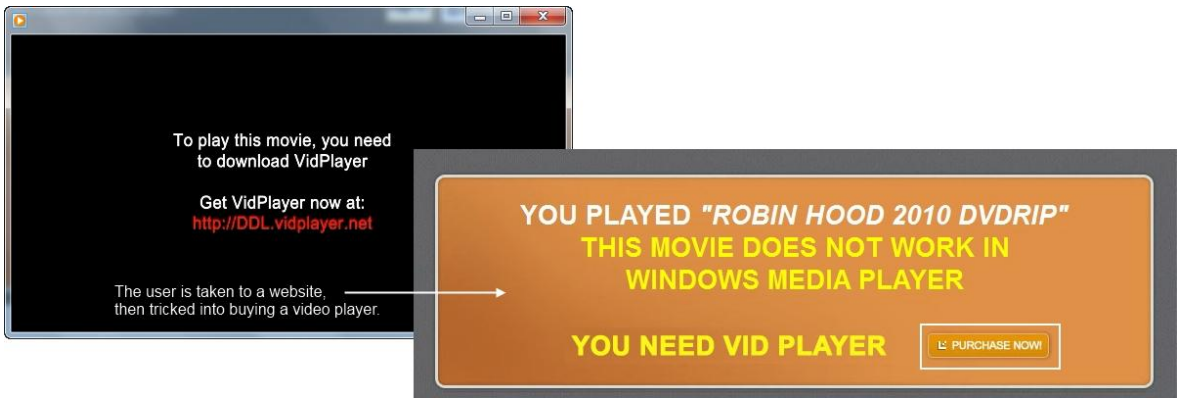



**Figure 11: Fake AVI file redirecting users to buy various video players**

The second approach also relies on an URL redirection that takes the user to a webpage offering a free - yet missing – codec. As soon as the unwary users install the codec (which is in fact one of the many flavors of Rogue AV), they will be constantly pushed into buying the “full version” of the product.

[8] For a complete description on how the Trojan.Wimad family works, please visit http://www.bitdefender.com/VIRUS-1000455-en--Trojan.Wimad.Gen.1.html

## Malware targeting Facebook® Users

As one of the largest social networks in the world, Facebook® is constantly under the scope of cyber-criminals, who are trying to either harvest most of the personal details available in users' profiles, or to determine account holders to take part in various illicit schemes.

During the first half of 2010, most of the security incidents targeting Facebook® users were related to the proliferation of the Koobface worm, the increase of clickjacking practices, as well as to the deployment of adware via third-party rogue applications for Facebook®.

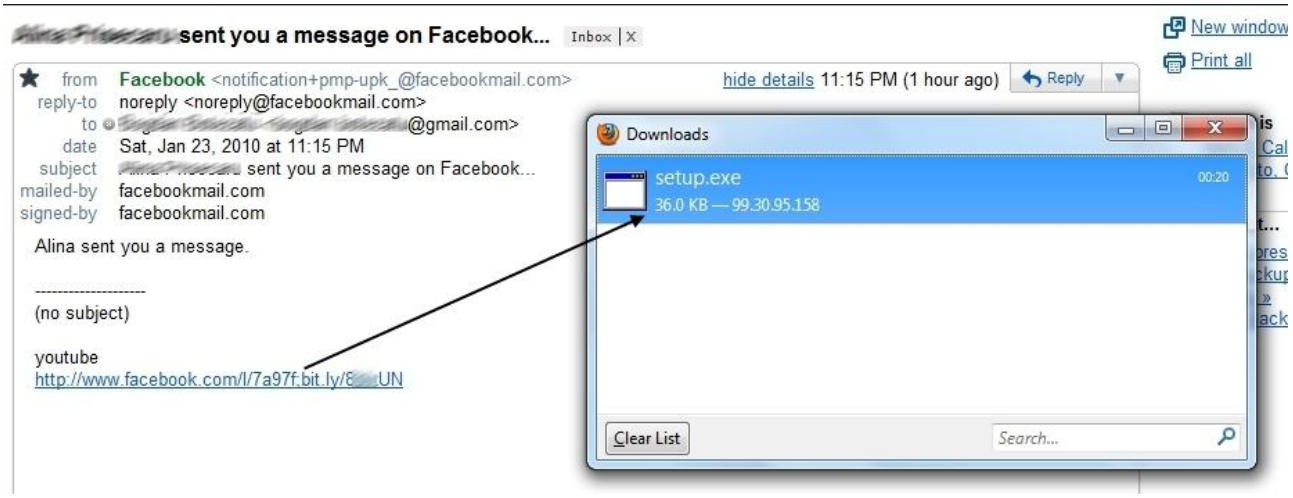



**Figure 12: The Koobface worm starts sending messages to all the Facebook® friends of the infected users. The message contains what appears to be a URL to a video page, but it actually leads to a Koobface-infected executable file.**

After a rudimentary A variant released in early August 2008 and only affecting myspace.com users[9], the worm morphed into a fully-fledged web-based application with an unimagined destructive potential.

The following variants of the worm were redesigned to divide each of its features into a distinct module, in a similar manner with commercially-available software. **Win32.Worm.Koobface** rapidly grew into a tool to attack most Web 2.0 social networks, including, but not limited to myspace.com, facebook.com, hi5.com, fubar.com, tagged.com, Friendster.com, and twitter.com.

It also made a shift in its behaviour: from a worm that only spread across the walls or profiles of infected users, it grew into an extremely dangerous tool able to steal data, intercept and hijack traffic or initiate ad campaigns inside the users' browsers. At the moment this report is written, **Win32.Worm.Koobface** is responsible for creating a massive botnet coordinated through an extremely resilient network of command & control centers that perform various tasks for its masters, including e-banking espionage and forcing rogue antivirus utilities on the already infected systems.

[9] The Koobface.A technical description from BitDefender: http://www.bitdefender.com/VIRUS-1000362-en--Win32.Worm.KoobFace.A.html

**Clickjacking** has also played an important role in disseminating malware among Facebook® users. This technique is exploiting a documented feature in Facebook®, which allows an application developer to register an anonymous "like" button without adding extra security checks. A hidden or transparent iframe is placed on top of a legitimate button which is most likely known by users.

As soon as they click what they know to be there - usually a message box - they are immediately redirected to a different page and asked to fill in forms, confirm their credentials, answer some questions or further click other links. Of course, this page looks legit and trustworthy so that the less tech-savvy user has no idea what happened.


**Figure 13: Clickjacking trick to force the posting of a link to a surveys website on the victim's wall.**

Cross-Site-Request Forgery attacks (also known as XSRF) have also contributed to the propagation of various messages and links from wall to wall. This type of attack is based on iFrames running third-party scripts in order to manipulate Facebook® and have the platform publish a wall post as if it were written by a friend. Unlike previously-identified XSRF attacks which posted links to phishing sites or malware on users' walls, this year's exploitations were mostly limited to posting commercial announcements.


**Figure 14: Work-from-home advertisement mass-spammed by the victim without his consent via a XSRF exploit.**

The first six months of 2010 have brought a certain number of new rogue applications designed by third-parties to integrate with Facebook®. These apps are neither hosted, nor sanctioned by Facebook®, so it is easy to imagine that some of them have a hidden agenda.

These rogue applications are usually populated with artificial content and friends to increase the victims' confidence that what they are about to visit is legit. The victim usually arrives on the application's page by following a link posted on their wall by one of their compromised friends.

As soon as the victim follows the link, the application asks for confirmation to pull out personal data, send message on users' behalf, as well as permission to always send these messages without any further confirmations. The example below presents the "Dance Class Video" application, which is described in detail in a Malware City article.

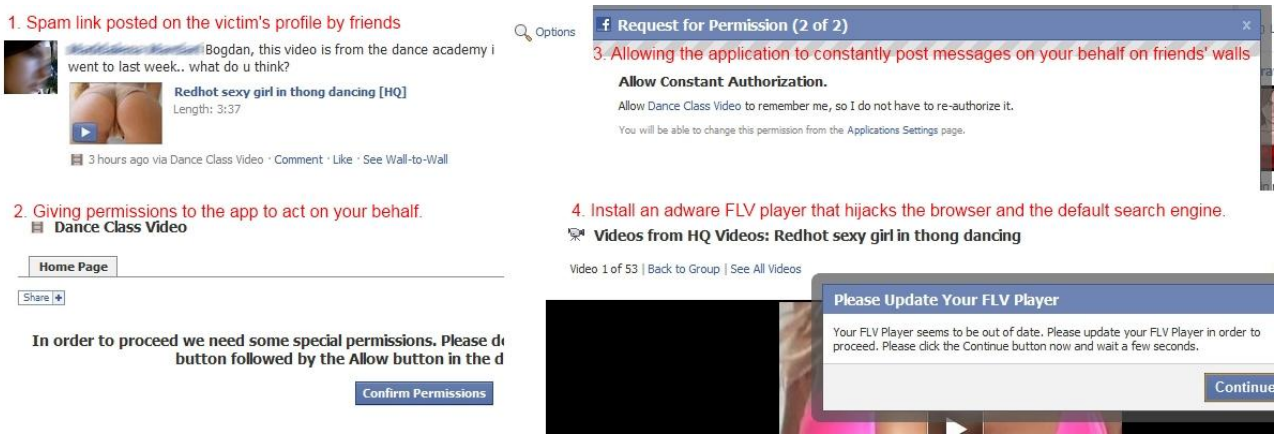



**Figure 15: Four-step tutorial to install an adware application starting from a link on your wall.**

# Spam and Phishing

Phishing is undoubtedly one of the most lucrative areas of spam, especially when it targets e-banking or online store users. However, as both webhosting companies and the anti-malware industry have allocated extensive resources to suspending or blocking phishing pages, cyber-criminals now focus on sending messages with the phishing form attached to the e-mail. Furthermore, since attachments are much easier to be analyzed, in a recent Visa® phishing wave forms were encrypted using the JavaScript **eval()** function.

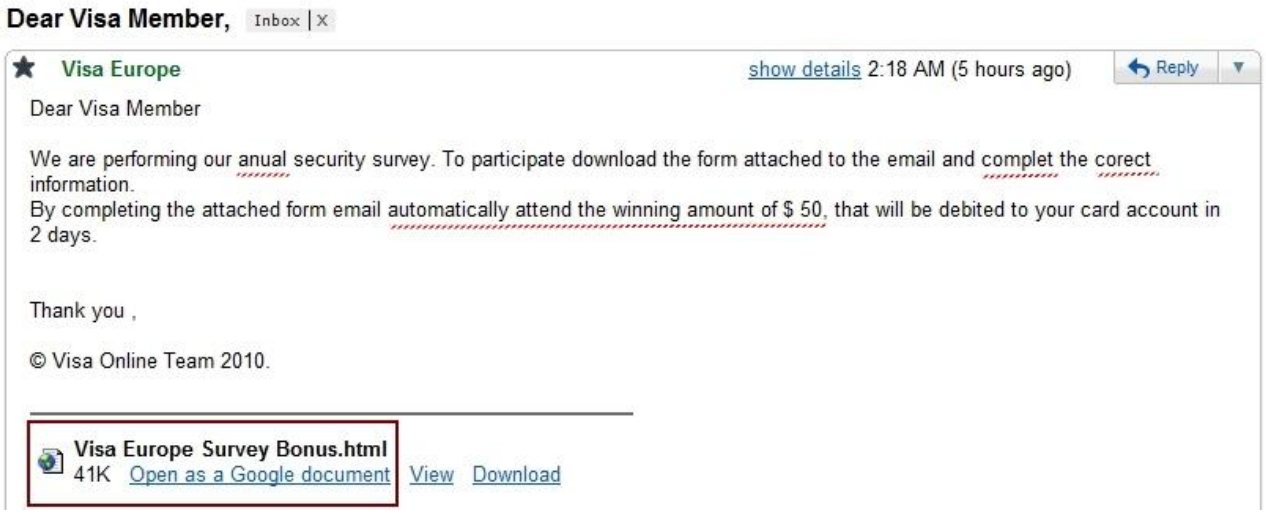



**Figure 16: Spamvertised Visa phishing with the phishing form attached to the message**

Most of these messages are written in poor English, which leads us to believe that the spam wave originated somewhere in Eastern Europe. Other traditional phishing attacks mostly relied on miscellaneous phishing packs available as exchange on various underground forums.

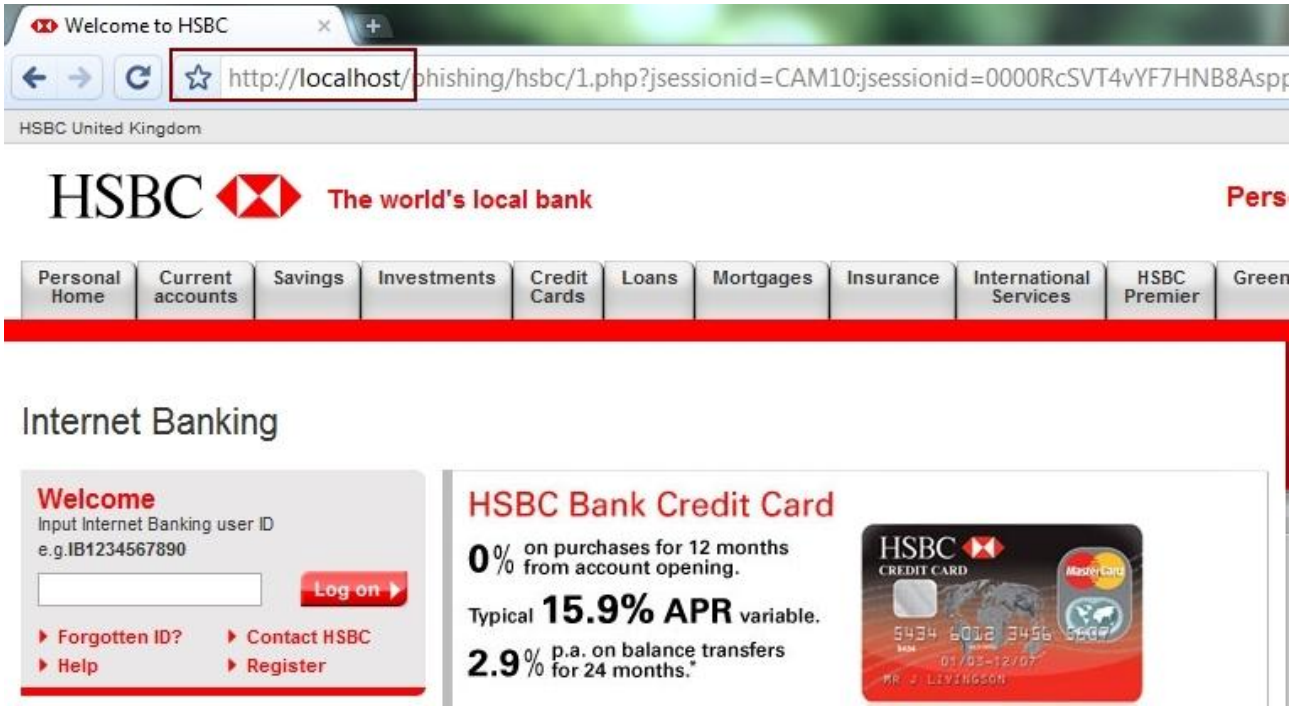



**Figure 17: HSBC phishing page set up using a phishing kit available on various forums.**

## Spam Threats in Review

Spam was one of the constant issues the computer user had to face in the first half of 2010. Most of the unsolicited messages sent worldwide were the notorious advertisements launched by Canadian Pharmacy, which also accounted for roughly 66 percent of the global spam.

## Spam Distribution by Territory

While Russia showed a slight regression during the second quarter of 2009 – mostly because of the sudden annihilation of the so-called "Bulletproof hosting providers[10]", - it quickly bounced back to being one of the top three global spammers.

**Spam distribution by point of origin**
**January – June 2010**

| | Current Values (H1 2010) |
|---|---|
| United States | 28.71% |
| China | 5.21% |
| Russia | 3.65% |
| Argentina | 2.14% |
| United Kingdom | 2.13% |
| Germany | 1.84% |
| Brazil | 1.65% |
| Canada | 1.60% |
| Romania | 1.58% |
| Japan | 1.50% |
| Others | 50.00% |

The United States of America and China are two of the most prolific countries, mostly because of the massive infestation with spam-sending malware, such as Rustock, Kobcka and various other spambots.

Canada, Romania and Japan rank last in the half-yearly spam top with average spam indexes of 1.5. Most of the spam originating in all these three countries is part of massive campaigns carried out by major spam groups rather than by local spammers promoting their own business.

[10] Bulletproof hosting is an umbrella term applied to all hosting companies that have a lax service policy regarding abuse. Most of the times, the term depicts web-hosting services that allow their customers to relay / send spam or to host phishing and malware pages on their servers.

.

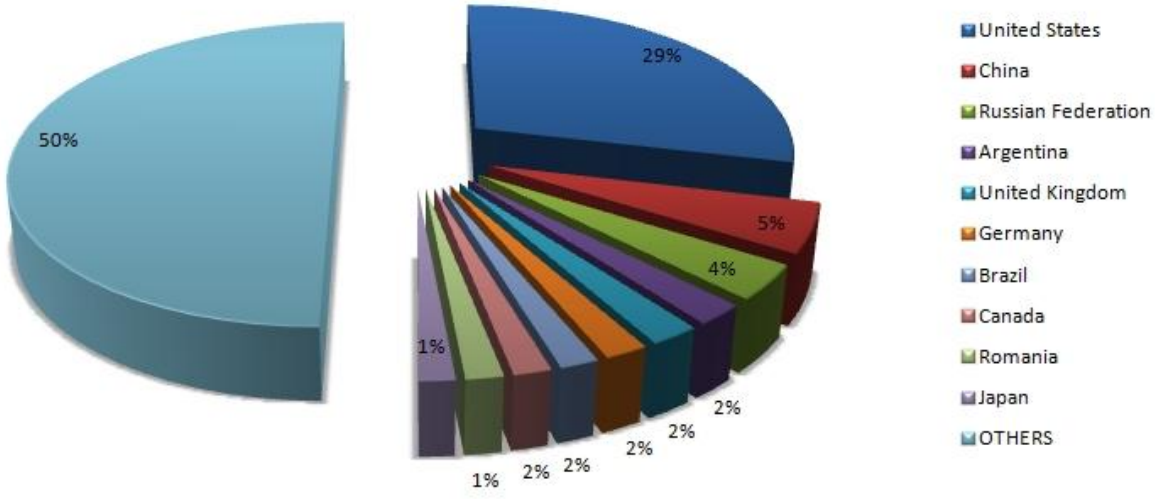
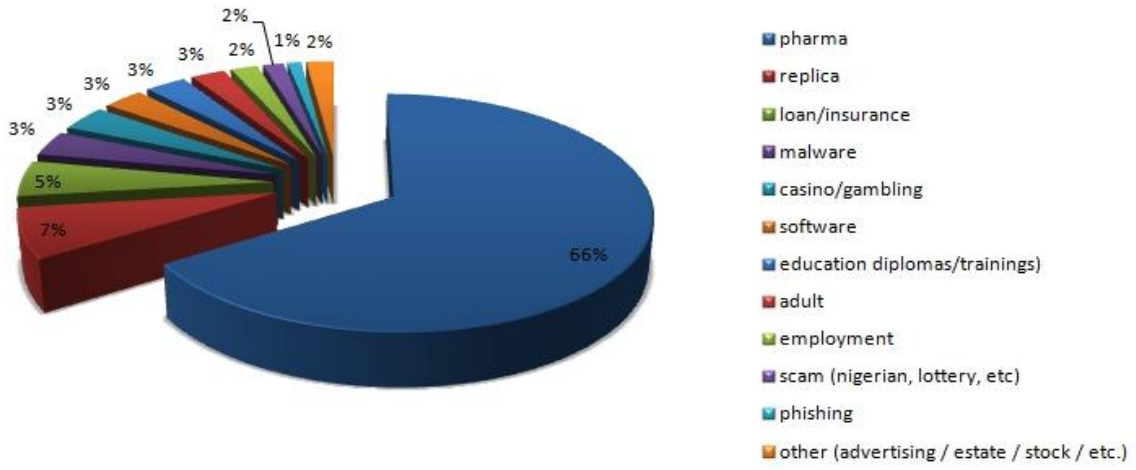



**Figure 18: Spam distribution by territory**

## Spam Breakdown by Type

During the first half of 2010, pharmacy spam accounted for the bulk of unsolicited messages sent worldwide. It also manifested an alarming increase, managing to spike from 50 to 66 percent in just six months. This long-time running operation appears to be originating from Russia, Ukraine and China. Most of these spam messages advertise Canadian Pharmacy, a one-stop pill shop that blends delivery of fake medicine with credit card fraud. The Canadian Pharmacy website has an incredibly large number of clones hosted either with bulletproof hosting companies in China, or directly on compromised computers that are part of fast-flux botnets.



Replica products rank second in the spam type top, with roughly 7 percent of the total amount of spam sent worldwide. These offerings include counterfeit copies of prestigious brands, especially watches and wearable accessories (shades, purses & bags and jewelry).


**Figure 19: Spamvertised replica website**

The precarious state of the global economy has also had a huge impact on the spam landscape almost 5 percent of which is consist of insurance and loan spam offers, making this the third ranking spam theme worldwide..

Malware-bundled spam has considerably declined from 6 percent in H2 2009 to only 3 percent in the first six months of 2010. However, the attached malicious files have become more and more aggressive: the Zeus bots, the Waledac greeting cards and the Mabezat.J worms are just some of the extremely destructive payloads that took users' inboxes by assault in 2010.

## Spam Trends

The first half of 2010 saw spam messages at 86.2 percent of the total number of electronic messages sent worldwide. Text-based spam is still the most popular form of unsolicited messages, although there have been some spikes in image-based spam all along the first quarter of the year. Most image messages are 6 to 12 KB Canadian Pharmacy ads. Average sizes for text-based messages fluctuate around 5.5 KB.


**Figure 20: Pill spam accounts for most of the unsolicited mail including images.**

International holidays such as Valentine's Day or large-scale events (the World Football Cup, for instance) have been well exploited in targeted messages carrying malware (especially Waledac bots disguised as greeting cards) or leading to phishing websites selling fake tickets for the World Cup.

Other spam messages carried DOC or PDF attachments impersonating tax forms, employment offerings or even banking transaction notifications which, once opened, took advantage of 0-day exploits identified in commercial software in order to run arbitrary code on users' computers.

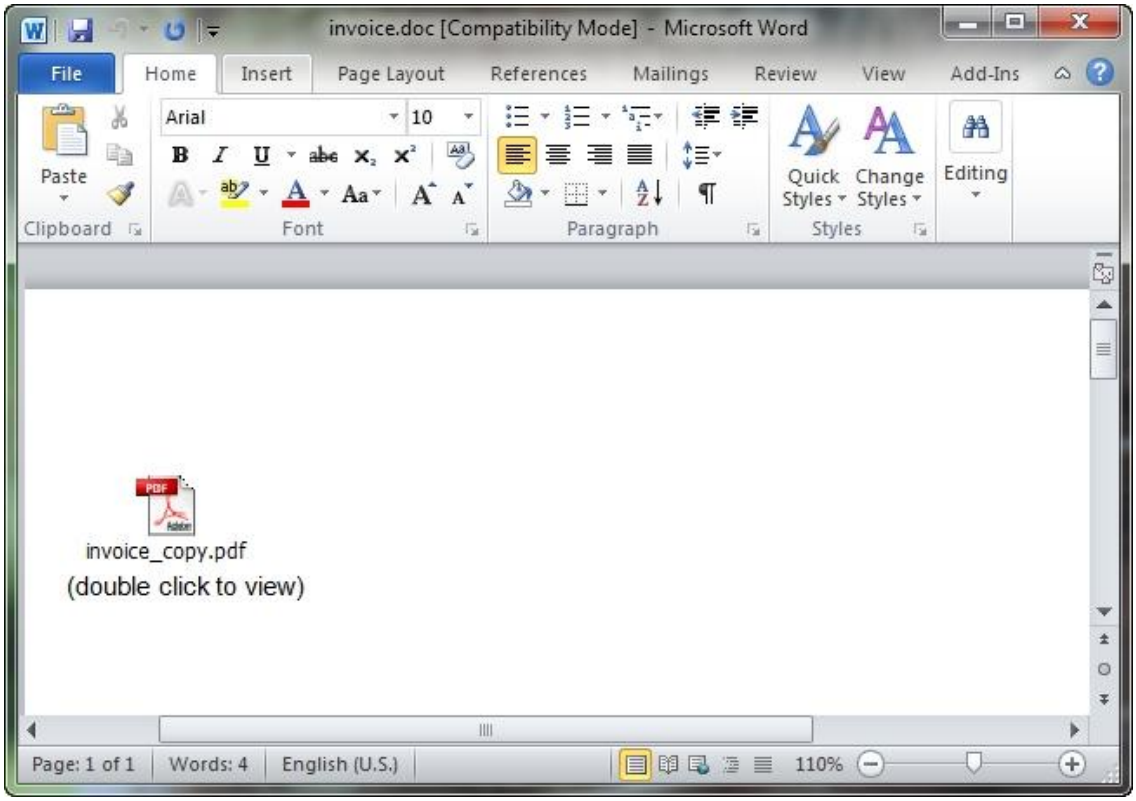



**Figure 21: Embedded executable file disguised as a harmless document detailing alleged bank transactions**

The natural disaster in Guatemala was yet another incentive for spammers and malware writers alike to capitalize on users' curiosity and to lure them into visiting malware-loaded webpages. black-SEO optimized pages related to the sinkholes in Guatemala were added to an impressive number of hacked websites.Visiting any of these pages redirected the victim to Rither rogue AV or to Adobe PDF 0-day exploits.

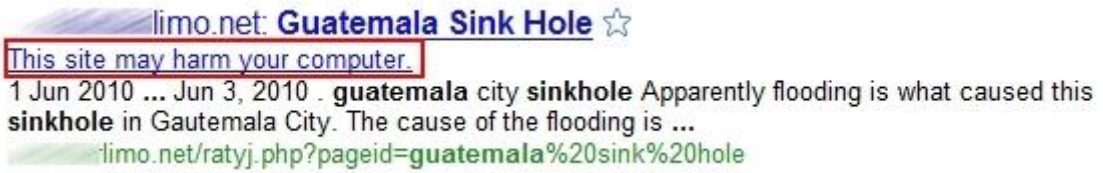



**Figure 22: Company page hacked and optimized to drive traffic related to the floods in Guatemala.**

# Phishing and Identity Theft

As one of the most damaging breeds of spam, phishing continued its evolution during the first months of 2010, despite the fact that most web-hosting providers and search engines have maximized their efforts in order to block dangerous pages.

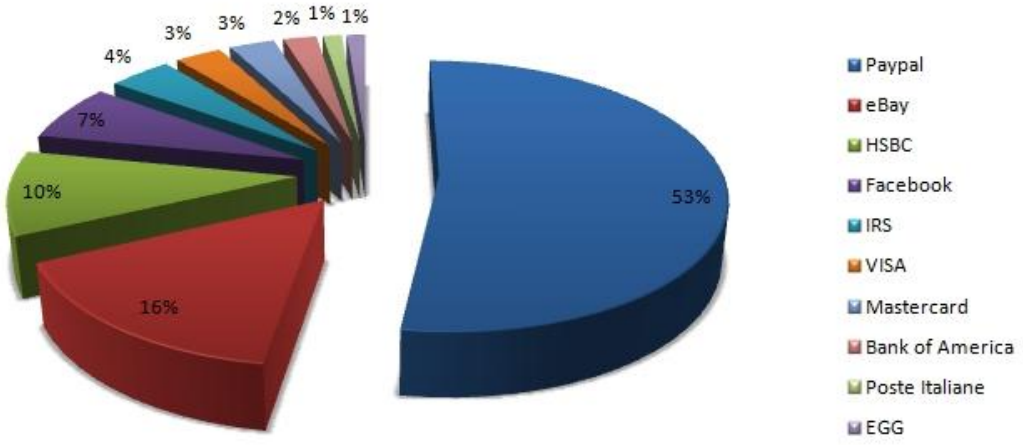



**Figure 23: Top phished institutions during H1 2010**

During the first half of the year, financial institutions were cyber-criminals' preferred targets, with more than 70 percent of the global phishing messages. Social networks have also been under heavy fire, since user profiles are an easy source of personal information and compromised accounts may effectively be used in spear phishing attacks.


**Figure 24: PayPal phishing page. In order to gain extra credibility, the attacker has created a folder called www.paypal.fr that actually contains the phishing form.**

Most of the phishing messages spammed out during the first half of 2010 were written in English (75 percent of all the spam messages processed by BitDefender), followed by French (13%) and Swedish (3%). Russian spam ranks fourth with roughly 2%, while the last place is taken by unsolicited messages written in Bulgarian with 0.42% percent of the global phishing messages.

The most phishing-friendly webhosting companies are located in Russia and the Czech Republic, which host almost 50 percent of the phishing pages. The so-called bulletproof hosting companies operating in Russia provide hosting and spam servers to international cyber-criminal organizations dealing with phishing, spam, Rogue AV as well as hosting command and control centers for massive botnets such as Zeus, Pushdo and Rustock.

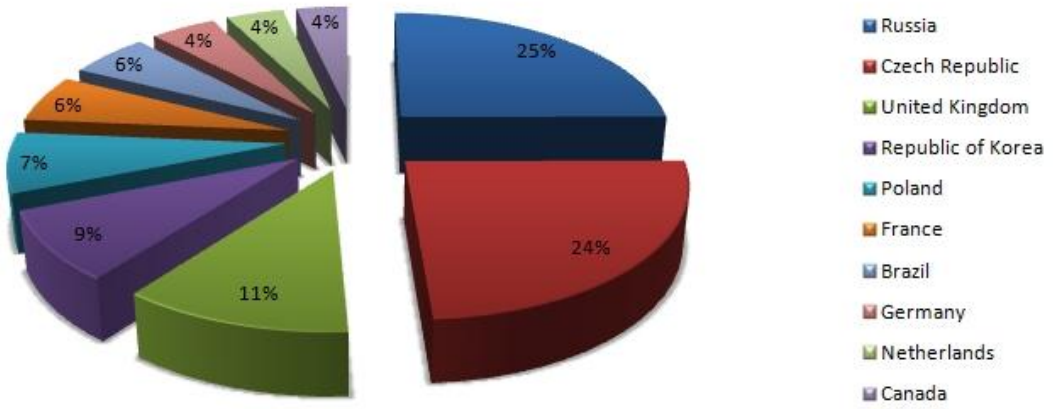



**Figure 25: Top global webhosting companies harbouring phishing pages.**

Although they cyber-attackers' most coveted victims, financial institutions are not the only ones affected by phishing. Online gaming communities such as Steam® and World of Warcraft® are also two other points of interest for phishers.

Once they have successfully carried out the attack and got the login credentials, attackers not only have access to the credit card information stored inside the account for billing purposes, but they can also sell, trade or otherwise transfer the victim's in-game items.

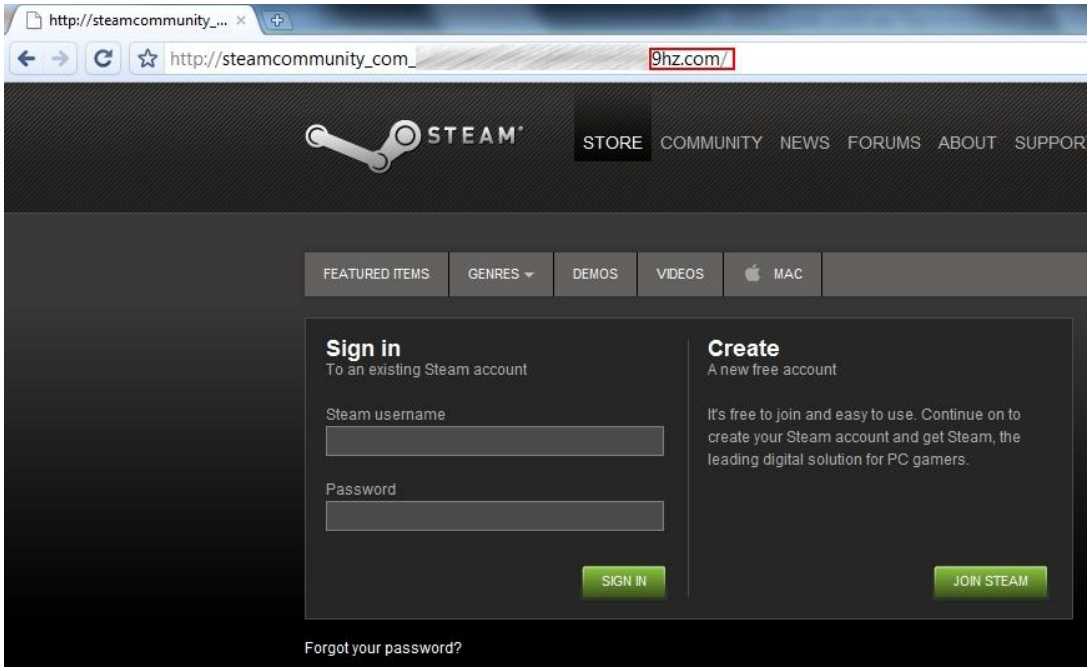



**Figure 26: Steam phishing page ready to lift credentials**

# Vulnerabilities, Exploits & Security Breaches

Compared to the last six months of 2009, the first half of 2010 was extremely rich in 0-day exploits, ranging from critical vulnerabilities in Microsoft® core components (Windows® Internet Explorer® versions 6 - 8) to bugs in third-party software such as Adobe® PDF and Adobe® Flash Player, among others.

## Overview of Exploits

January brought CVE-2010-0249, a Windows® Internet Explorer® 0-day exploit that takes advantage of a memory corruption vulnerability affecting all versions except for Internet Explorer 5.01 Service Pack 4 for Microsoft Windows 2000 Service Pack 4.

Intercepted by BitDefender as Exploit.Comele.A, the critical 0-day bug has been extensively used in the wild to trigger a large scale cyber-attack dubbed Operation Aurora. Among the affected institutions that officially acknowledged it are Google™[11], Adobe Systems Inc., Juniper Networks Inc. and Rackspace Ltd..

According to Google™, rather than just seeking access to personal information the exploit was part of a cyber-offensive with political and economic implications. Moreover, the exploit code went public

[11] The search engine giant confirmed and detailed the attack in an article called A New Approach to China and posted on the company's official blog.

before Microsoft® had any chance of issuing a patch, which led to other drive-by attacks initiated by various other attackers who had access to the exploit code.

January also brought a second critical vulnerability targeting Adobe® Reader®. Also known as CVE-2009-4324, this specific flaw affected Adobe® Reader® and Acrobat 9.2 and earlier versions and successful exploitation caused crashes, remote code execution as well as the capability to carry out cross-site scripting attacks.

CVE-2009-4324 exploits an error in the implementation of the "Doc.media.newPlayer()" JavaScript method, that is likely to corrupt memory when a specially crafted PDF file is run. The vendor issued a patch on January 12 in order to mitigate any further attacks based on this specific JavaScript method.

June came with multiple surprises in terms of security, with Adobe® products as main targets. Just as many other zero-day bugs aimed at the Adobe® Reader®, the attack vector for CVE-2010-1297 was represented by a malformed PDF file that contains both a specially crafted JavaScript code and an embedded .SWF file.

The exploit uses the embedded JavaScript to decrypt a shell-code script, which would subsequently decrypt and drop a binary file also located inside the malicious PDF file. In order for the attack to be successful, the presence of the exploitable file authplay.dll is mandatory on the target system.

## Other Security Risks

April ended with a major attack against a wide range of CMS software hosted with different providers. Thousands of website owners found their content management systems of choice compromised by base64-encoded functions injected in some PHP pages. In all cases, the base64 instructions performed redirects to websites hosting Rogue AV, but only when the unsuspecting visitor was referred by a search engine. This technique allowed the script to remain undetected to all visitors that accessed the website directly (including the administrators), while directing all the traffic originating from search engines to malware-loaded webpages.

Initial theories had it that the affected websites were running old and vulnerable versions of WordPress and were located on the servers of a specific webhosting company. However, a couple of days later, other PHP-based CMS platforms hosted with different providers fell victim to the same file hack. Further analysis revealed that improper server configurations paired with a wrong attribution of file privileges was the main factor that facilitated the attack.

# E-Threat Predictions

While the first six months of 2010 have been dominated by conventional e-threats such as Trojans and worms, various exploits pointing at third-party applications have rapidly gained ground, both in count and in terms of impact. As seen in the case of Exploit.Comele.A, zero-day vulnerabilities may be used for purposes that are beyond identity theft or compromising banking accounts: we are looking at fully-fledged weapons used in cyber-warfare and top-level industrial espionage.

## Botnet Activity

Since botnets are key mechanisms in any cyber-criminal infrastructure, their development and improvement will be the main concern for malware authors. However, as botnets are often in the crosshair of international authorities and responsible internet service providers (as the successful shutdown of the Mariposa (aka Rimecud aka Palevo) botnet proved), bot herders will be needed to experiment with alternative methods of coordination.

- The recent emergence of the do-it-yourself botnet creation tools controllable via Twitter may set the cornerstone for a new and extremely viable breed of zombified computers
- Fast-flux botnets will also gain extra ground as more and more web-hosting providers terminate accounts harbouring phishing pages, exploit packs or spam-sending applications. Fast-flux botnets not only solve the constant need for bulletproof hosting, but also make it difficult for authorities to trace the exact origin of an attacker.

## Malicious Applications

The first half of 2010 brought back to life older breeds of malware: ransomware and MBR-overwriting viruses. Trojan.Maer.A, Application.Scareware.Keytz and various flavours of Rogue AV are only some of the applications that forced users into paying for getting their computers up and running again. BitDefender estimates that ransomware-based rogue AVs will multiply during the second half of 2010 in order to trick victims into paying for their “full version”.

## Social Networking

With Facebook® surpassing 400 million users, most of the malware authors will focus on the social networking platform to deliver their newest payloads. Some of these attacks will focus on social engineering tricks (such as launching various attacks from compromised computers), while others will try to exploit different vulnerabilities or features already implemented across the platform.

Personal information leaks will also dramatically contribute to the success of various attacks, especially when data harvested from social networks is corroborated with personal blogs, career

history and other relevant data. Third-party applications are also expected to play an important role in social networking abuses.

## Other Threats

The introduction of HTML5, the upcoming major revision of the HTML standard, will add extra levels of interaction between the user and the webpage and will probably change the face of the Web as we know it. The new technology is highly likely to be exploited by malware authors to compromise the browser security.

Cracked and non-genuine software will also constitute a key element in the propagation of various malware. On the one hand, most of the mechanisms of circumventing commercial software protection available for download on “warez” portals are already rigged with various types of malware from keyloggers to backdoors. On the other hand, non-genuine copies of the Windows® operating system can’t receive the latest security updates, which will leave the machines running it unprotected against the upcoming 0-day exploits and vulnerabilities which are expected to be discovered in the next 6 months.

## Mobile Operating Systems

The second half of 2010 will still see mobile threats as a rarity, mostly because of the wide assortment of mobile phones and OSes. Google’s Maemo will continue to enjoy a safe road, both because it is built on a solid platform that derives from the popular Debian Linux and because it hasn’t managed to become one of the top three mobile operating systems available.

On the contrary, Nokia’s Symbian will likely have the most exposure to malware. According to research company Gartner, Symbian OS currently holds 44 percent of the mobile OS market for smartphones, which makes it enough of a viable target.

# Table of Figures

# 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.