

State of the Internet 2010: A Report on the Ever-Changing Threat Landscape

CA Technologies Internet Security Business Unit
Internet Security Intelligence Report

ABOUT THIS REPORT

Table of Contents

About This Report Authors & Contributors Foreword Executive Summary

Threat Landscape

- Top New Discovered Threats ...8
- Category and File Format Distribution ...10
- Exploits In The Wild ...11
- Prevalent Threats ...14
- Threat Distribution Vector ...17

Threat Intelligence

- Rogue Security Software ...18
- Blackhat SEO Attack ...21
- Crimeware ...23
- Email Spam Trend ...38
- Spamming via Instant Messaging ...40
- Ransomware ...44
- Notable Backdoor ...45
- Notable File Infection ...47
- Mac OS X Threat ...50

Safe Computing Advice

References

“State of the Internet 2010: A Report on the Ever-Changing Threat Landscape” (CA Technologies Internet Security Business Unit [ISBU], Internet Security Intelligence Report) is a compilation of findings offering an overall perspective of the status of the threat landscape in the first half of 2010 (H1 2010). The report is written by CA Technologies’ ISBU global team of security researchers and threat experts. It delivers insights and analysis based on data gathered from notable threats, trends and statistics from January to June 2010. This report also includes tips and reminders on routine PC security and safe online behavior.

For regular updates about Internet threats and timely research news, visit the CA Technologies Global Security Advisor Web page:

<http://www.ca.com/securityadvisor>

Driven by Research.

Contributing Authors

Akhil Menon
Senior Research Engineer, ISBU India

Mary Grace Gabriel
Research Engineer, ISBU Australia

Kenneth Yu
Research Engineer, ISBU Australia

Ricardo Robielos
Research Engineer, ISBU Australia

Kiran Bandla
Research Engineer, ISBU USA

Rossano Ferraris
Research Engineer, ISBU EMEA

Don DeBolt
Director of Threat Research, ISBU USA

Zarestel Ferrer
Senior Research Engineer, ISBU Australia

Methusela Cebrian Ferrer
Senior Research Engineer, ISBU Australia

System and Research Automation

Michael Grucz
Technical Lead, ISBU USA

Stefan Geisenheiner
Senior Software Engineer, ISBU GMBH

Suresh Kumar Kanniappan
Technical Lead, ISBU India

Simy Chacko
Technical Manager, ISBU India

Ramprasad Selvaraj
Senior Technical Lead, ISBU India

External Contributor

Nick Hurle
Technical Editor, ISBU Melbourne, Australia

Melissa Goldman
Communications, ISBU USA

FOREWORD

Today approximately 1.8 billion people use the Internet to do everything from conduct business, communicate with friends and family, keep up with current events or simply entertain themselves playing games or watching videos. Each individual and each Internet-connected device presents a certain footprint that is exposed and often manipulated for criminal or political gain. Malware, or malicious software, is often the catalyst for this manipulation, while targets span the gamut from corporate and national secrets to personal information that can be used to directly steal money or perpetuate another crime. Technology and the Internet provide the means and opportunity, while global socio-economic trends provide the motive to perpetuate these crimes.

Supporting this criminal activity and adding to the challenges of protection and law enforcement is the growth of a criminal ecosystem. This network of criminals and services introduces multiple layers of anonymity while providing modular functionality for perpetuating cybercrime. In this paper we have defined this ecosystem as “Crimeware-as-a-Service,” and we share examples of how this ecosystem is exploiting the latest technology trends of cloud computing and social media. The ability to perpetuate these crimes across the Internet without swift and severe repercussions further fuels this Crimeware, challenging security professionals and governments alike to find new ways to protect valuable information.

It is the role of the security professional to limit the exposure to malware and the associated criminal element. Yet through the use of classic security controls such as firewalls, anti-malware products, and intrusion detection systems we have had only limited success. The growth of Internet-born threats means tighter controls must be placed at the endpoint itself, and yet we can't afford to impact performance of the end device. This dichotomy presents significant security challenges, and we must find ways to use the latest prevention technologies to better balance protection and performance.

Please keep the criminal element and prevention controls in mind as you review the details of the malware seen to date in 2010.

Don DeBolt

Director of Threat Research

CA Technologies - Global ISBU

Key Findings

Top New Discovered Threats (p. 8 - 9)

- ◆ CA Technologies' ISBU researchers identified more than 400 new families of threats. Rogue security software, downloaders, and backdoors are the top ranking types of newly discovered threats, accounting for 18%, 17% and 14% respectively.
- ◆ Offensive effort focuses on online banking, accounting for 29% of the new infostealer Trojans.

Overall Distribution of Threats (p. 10)

- ◆ Trojans are the most prevalent category of threat, accounting for 73% of the total threat infections reported to CA Technologies' ISBU around the world.

Malicious File Format Distribution (p. 10)

- ◆ The number of Windows i386 (32-bit) portable executables dropped 5% from 92% in 2009 H1 to 87% in 2010 H1. The threat landscape is displaying a notable movement from the Windows executable platforms to an immense opportunity in the Web as an executable platform.

Exploit In The Wild (p. 11 - 13)

- ◆ Affected versions of Internet Explorer, Java, and Adobe PDF and Flash Player vulnerabilities are the biggest zero-day exploit attack vector in H1 2010.
- ◆ 84% of the total active exploited vulnerabilities are found in browser-based attacks.
- ◆ 71% of the total browser-based vulnerabilities target Internet Explorer.

Classification of Prevalent Threats (p. 14 - 16)

- ◆ The most prevalent Trojan families are information stealers, accounting for 47% of the total Trojan families processed in H1 2010.
- ◆ The top three most prevalent worms propagate through removable drives, *autorun.inf*, network shares and social networking sites.

Threat Distribution Vector (p. 17)

- ◆ The Internet is the primary threat distribution vector and source of infection. This equates to 86% of the total threat landscape, a growth of 8% compared to 78% last year.

Rogue Security Software (p. 18 - 22)

- ◆ Rogue security software remains the most prevalent Internet threat.
- ◆ Economies of scale identified through rogue security software using custom clones features and multiple language support.
- ◆ Multiple language support enables an international cybercriminal operation and distribution to more geo-specific targets.
- ◆ Rogue security software distribution through Blackhat SEO, advanced social engineering, and drive-by download attacks.
- ◆ Expanding cybercriminal partner networks are enabling other prevalent threats such as Win32/Zlob, Win32/Bredolab, and PDF/Pidief to distribute rogue infection.

Crimeware (p. 23 - 37)

- ◆ 96% of Trojans are components of a larger underground market-based mechanism we call *Crimeware-as-a-Service*.
- ◆ Crimeware refers to modular threats designed to perform specific tasks; these threats work together to form the *crimeware ecosystem*.
- ◆ Crimeware's main distribution mode is through *social engineering* and *drive-by download* attack.
- ◆ Social engineering attack manipulates human behavior using a technique that responds to authority pressure and favor on compliance.
- ◆ The increasing events of Facebook's viral and abusive applications is the most noteworthy in H1 2010.
- ◆ Crimeware highlights cloud computing as new delivery model.
- ◆ Social media is identified as the latest crimeware market.
- ◆ Crimeware's latest offensive capabilities highlight Zeus and Spyeeye.

Spam (p. 38 - 43)

- ◆ EU regions ranked as the number-one source of email spam, recording 31%, followed by 28% Asia Pacific and Japan (APJ), 21% India (IN), and 18% United States (US).
- ◆ Active proliferation of unsolicited chat messages on Skype promotes online fraud, cheap software, penny stocks and diploma mills.

Ransomware (p. 44)

- ◆ Ransomware promotes rogue security software features.
- ◆ Win32/DotTorrent.A is the latest and noteworthy ransomware discovery in H1 2010. It uses FakeAV's scare tactics by displaying fake warnings and deceiving popups to persuade users to pay.

Notable Backdoor (p. 45 - 46)

- ◆ Win32/Hydraq highlights the features of an advanced persistent threat (APT).
- ◆ Win32/Hydraq, Win32/Wisp, and Win32/Arugizer highlights features and distribution of a notable backdoor attack.

Notable File Infector (p. 47 - 49)

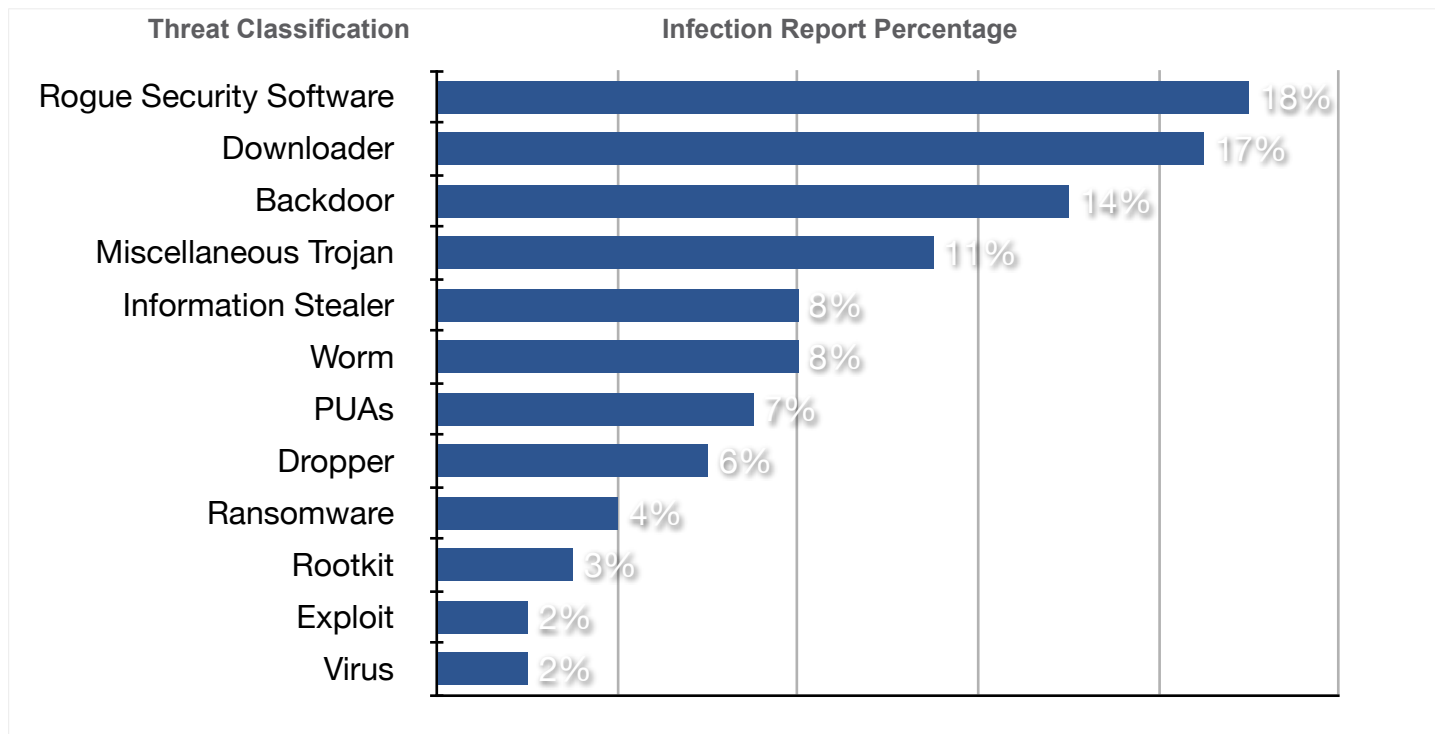
- ◆ Alureon and Pushdo/Cutwail's latest offensive feature is the ability to infect system drivers.
- ◆ Win32/Imm322Patched, Win32/Patchload and Win32/SillyDI.SBW are detection for a patched DLL file modified to load malicious DLL file components such as a variant of Win32/Zbot.
- ◆ Win32/Sfcpatched infection continues to proliferate. This is a detection for a patched sfcfiles.dll file modified to unprotect system files by disabling a feature called Windows File Protection (WFP), a part of the System File Checker.

Mac OS X Threats (p. 50 - 51)

- ◆ The proof-of-concept Blocker ransomware emerged after a traffic redirection attack in January.
- ◆ Hellraiser 4.2 server component spotted in the wild.
- ◆ PremierOpinion, a known spyware in Windows since 2008, crossed over to Mac OS X this year.

Threat Landscape

Top New Discovered Threats



CA Technologies' ISBU receives and processes reported infections from customers and partners around the world. In the first half of 2010, ISBU researchers identified more than 400 new families of threats. Rogue security software, downloaders and backdoors are the top-ranking types of new threats, accounting for 18%, 17% and 14% respectively.

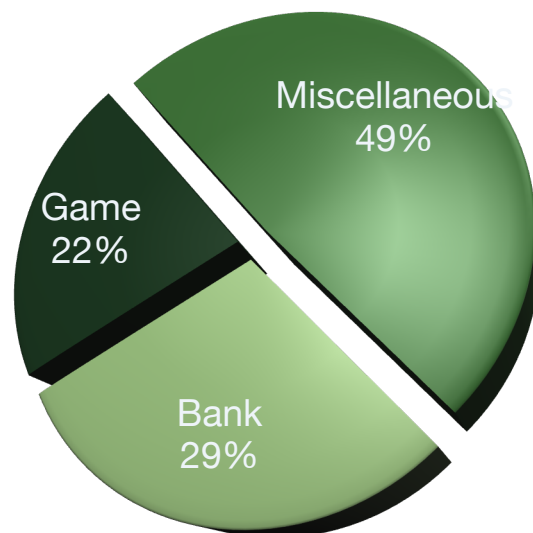
Miscellaneous Trojans are types of threats that assist attackers in performing malicious activity, including obfuscation, redirection, clickers, browser helpers and programs to avoid discovery (e.g., disabling firewall, anti-virus, online security Web sites and forensic tools).

The development of backdoor-type threats has been more active compared to Trojan stealers and worms in H1 2010. More than ever, attackers are interested in using remote control features, giving them more freedom to take full control and manipulate a target on demand.

Threat Landscape

Top New Discovered Threats: Information Stealers

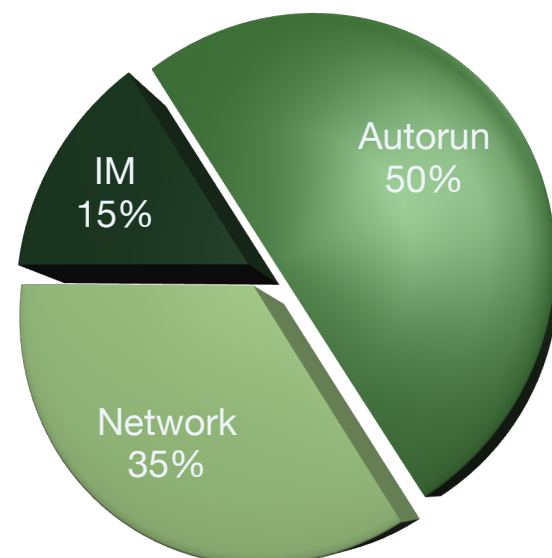
Newly discovered information stealer families show that the Miscellaneous category accounts for 37% of the total types of info stealer. Miscellaneous refers to information specific to the target system (e.g., OS version, installed application), online services (e.g., FTP, Dynamic DNS, social networks), and instant messaging application (e.g. Yahoo, Skype, MSN). These artifacts of stolen information create an opportunity for organized cybercriminals to distribute various forms of attack over the Internet.



A second identified offensive effort focuses on online banking, accounting for 29% of the new infostealer Trojans. These types of threats specifically target a list of banking and online shopping transactions. Information stealers targeting online games account for 22% of the overall newly discovered infostealers in H1 2010.

Top New Discovered Threats: Worms

The top three categories for newly discovered worms in H1 2010 propagate through removable drives, *autorun.inf*, network shares and instant messaging applications (IM).

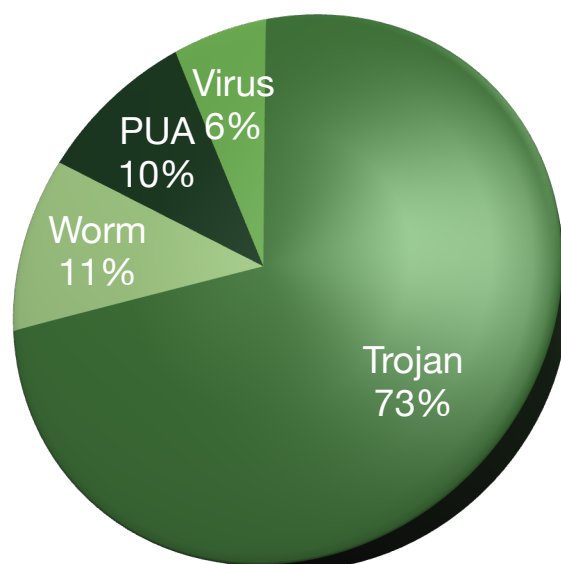


Only a very small number of newly discovered threats are using peer-to-peer and email as means of propagation.

Threat Landscape

Overall Distribution of Threats

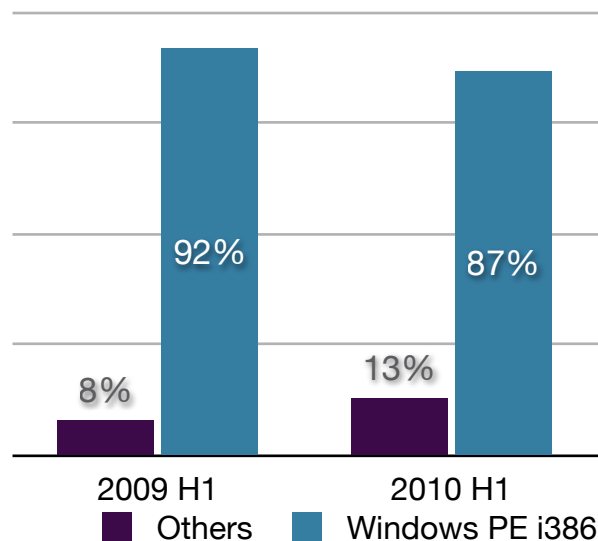
Trojans are the most prevalent category of threat, accounting for 73% of the total threat infections reported to CA Technologies' ISBU around the world. Trojans are not self-replicating pieces of code but pose a serious threat when installed on a users' system. Worms, potentially unwanted applications (PUAs) and viruses share a very small percentage of the overall threat landscape.



Malicious File Format Distribution

Tracking attackers' use of various file formats aids our understanding of infection and propagation. The amount of Windows i386 (32-bit) portable executables dropped 5% from 92% in 2009 H1 to 87% in 2010 H1. Non-Windows i386 (32-bit) format noted as Others grew 5%. This landscape includes Text (e.g. PHP, HTML, Java Scripts), Adobe Rich Content (e.g. PDF, SWF), and Archive/Compressed (e.g. RAR, ZIP and CAB) file formats accounting for 7%, 3%, and 2% respectively.

The threat landscape is displaying a notable movement from the Windows executable platform to an immense opportunity on the Web as an executable platform.



Threat Landscape

Zero-Day Exploits in the Wild

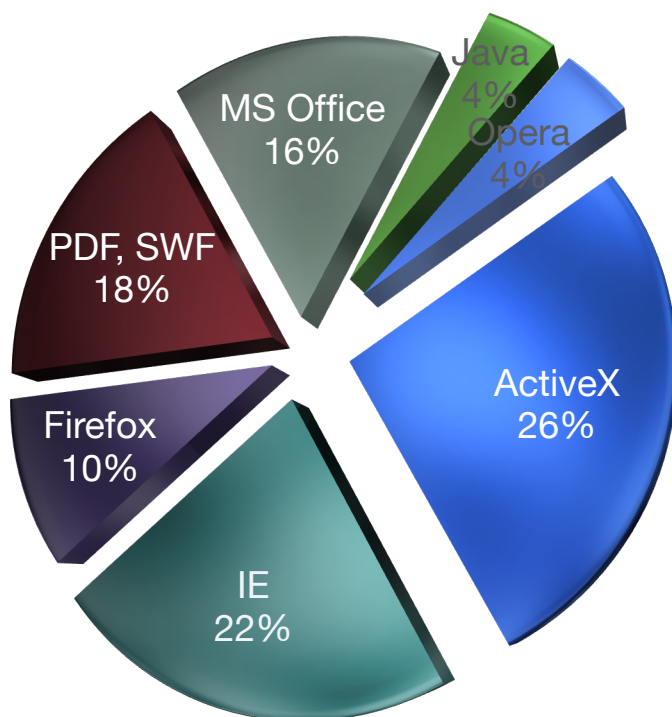
CVE Reference	Affected	Detection
CVE-2010-0188	Adobe Acrobat and Reader 9.3 and earlier versions.	PDF/CVE-2010-0188!exploit
CVE-2010-0249	Internet Explorer 6,7 and 8	JS/CVE-2010-0249!exploit
CVE-2010-0483	Internet Explorer 6,7 and 8	VBS/CVE-2010-0483!exploit
CVE-2010-0806	Internet Explorer 6,7 and 8	JS/CVE-2010-0806!exploit, aka "Aurora Exploit"
CVE-2010-0886	JDK and JRE 6 (desktop java)	JS/CVE-2010-0886.A!exploit
CVE-2010-1297	Adobe Flash Player 10.0.45.2 and earlier versions; Adobe AIR 1.5.3.9130 and earlier versions	SWF/CVE-2010-1297!exploit
CVE-2010-1885	Windows XP/2003; Internet Explorer	HTML/CVE-2010-1885!exploit; (Attack vector: hcp:// URL Cross-site scripting)

Affected versions of Internet Explorer, Java, and Adobe PDF and Flash Player vulnerabilities are the biggest threat vector in H1 2010. Most of these exploit attacks take place through the browser and are notably used for zero-day attacks.

Prevalence of Exploited Vulnerabilities

Organized cybercriminals constantly integrate latest known remote execution exploit codes to increase their chances of compromise. These threats are widely distributed through drive-by download and targeted attacks.

Browser-based exploits accounted for 84% of the total actively exploited known vulnerabilities in the wild. Exploited vulnerabilities in Internet Explorer, ActiveX control, Java, and Adobe PDF and SWF have all been proven to work successfully in Internet Explorer. Thus, Internet Explorer is the most targeted browser, accounting for 70% of exploits. Microsoft Office exploits remain prevalent and widely used in targeted attacks.



Threat Landscape

Adobe PDF and Flash Player

Exploit	Affected	Detection / CVE Reference
Collab.collectedEmailInfo()	Adobe Acrobat and Reader 8.1.1 and earlier	PDF/Pidief, CVE-2007-5659
util.printf()	Adobe Acrobat and Reader 8.1.2 and earlier	PDF/Pidief , PDF/CVE-2008-2992!exploit
Collab.getIcon()	Adobe Acrobat and Reader 8.1.2 and earlier	PDF/Pidief, CVE-2009-0927
getAnnots()	Adobe Acrobat and Reader 8.1.4 and earlier	PDF/Pidief , CVE-2009-1492
jbig2decode	Adobe Acrobat and Reader 9 and earlier	PDF/CVE-2009-0658!exploit , CVE-2009-0658
media.newPlayer()	Adobe Acrobat and Reader 9.2 and earlier	PDF/Pidief , CVE-2009-4324
Libtiff	Adobe Acrobat and Reader 9.3 and earlier versions.	PDF/CVE-2010-0188!exploit, CVE-2010-0188
integer overflow	Adobe Flash Player 9.0.115.0 and earlier, 8.0.39.0 and earlier	CVE-2007-0071, SWF/CVE-2007-0071!exploit
intf_count' Integer Overflow	Adobe Flash Player 10.x and earlier and Adobe AIR 1.5.2 earlier	CVE-2009-1869, ActnS/Swif

Microsoft Office

CVE Reference	Bulletin Reference / Affected	Detection
CVE-2006-0009	MS06-012, Microsoft Powerpoint .PPT	PP97M/MS06-012!exploit
CVE-2006-2492	MS06-027, Microsoft Word .DOC	W97M/SmartTags!exploit
CVE-2006-2389	MS06-038, Microsoft Word .DOC	W97M/SmartTags!exploit
CVE-2006-6456	MS07-014, Microsoft Word .DOC	W97M/SmartTags!exploit
CVE-2008-4841	MS09-010, Microsoft Word .DOC	W97M/ CVE-2008-4841!exploit
CVE-2009-0556	MS09-017, Microsoft Powerpoint .PPT	PPT97/PPDropper
CVE-2009-1129	MS09-017, Microsoft Powerpoint .PPT	PPT97/PPDropper
CVE-2009-3129	MS09-067, Microsoft Excel .XLS	X97M/EXEDropper!exploit

Firefox

CVE Reference	Affected	Description
CVE-2006-0005	Firefox .9 and later,	Microsoft Windows Media Player Plugin EMBED element buffer overflow
CVE-2005-2265	Firefox before 1.0.5, Mozilla before 1.7.9, and Netscape 8.0.2 and 7.2	InstallVersion.compareTo Code Execution
CVE-2006-3677	Firefox 1.5.04 and later	JavaScript Navigator Object Vulnerability
CVE-2009-1136	Firefox 3.0.6 and later	Local file stealing with SessionStore
CVE-2009-2477	Firefox 3.5 and later	Font Tags Remote Buffer Overflow Vulnerability

Internet Explorer

CVE Reference	Microsoft Bulletin	Microsoft Bulletin
CVE-2006-0003	MS06-014	Microsoft Data Access Components (MDAC) Remote Code Execution
CVE-2006-4868	MS06-055	Windows Vector Markup Language Vulnerability
CVE-2006-5559	MS07-009	Microsoft Data Access Components (MDAC) Remote Code Execution
CVE-2006-3643	MS06-044	MMC Redirect Cross-Site Scripting Vulnerability
CVE-2006-1359	MS06-013	Microsoft Internet Explorer createTextRange()
CVE-2006-3730	MS06-057	Internet Explorer WebViewFolderIcon setslice exploit
CVE-2007-0024	MS07-004	VML Buffer Overrun Vulnerability
CVE-2008-4844	MS08-078	XML Handling Remote Code Execution
CVE-2009-0075	MS09-002	CFunctionPointer Memory Corruption
CVE-2009-0076	MS09-002	Malformed CSS Memory Corruption
CVE-2010-0806	MS10-018	IEPeers Remote Code Execution
CVE-2010-0267	MS10-018	Uninitialized Memory Corruption

ActiveX control

CVE Reference	Description
CVE-2006-4777	Microsoft DirectAnimation ActiveX Controls Memory Corruption Vulnerability (MS06-067)
CVE-2006-6884	WinZip FileView ActiveX Control Multiple Vulnerabilities
CVE-2007-3147	Yahoo! Webcam Uploader ActiveX control
CVE-2007-3148	Yahoo! Webcam Viewer ActiveX control
CVE-2007-4336	DirectX - DirectTransform FlashPix ActiveX
CVE-2007-4034	Yahoo! Widgets Buffer Overflow
CVE-2008-2463	Microsoft Office Snapshot Viewer(MS08-041)
CVE-2008-1309	RealAudioObjects.RealAudio ActiveX control
CVE-2009-1136	Microsoft Office Web Components Spreadsheet ActiveX control
CVE-2009-1538	Microsoft DirectShow(MS09-028)
CVE-2006-5820	AOL SuperBuddy ActiveX Control LinkSBIcons() Vulnerability
CVE-2007-6250	AOL AmpX (AOLMediaPlaybackControl) ActiveX control vulnerability
CVE-2007-5755	AOL AmpX Multiple Buffer Overflow

Java

Exploited Function	Affected	Detection / CVE Reference
getSoundbank()	JDK and JRE 6 (desktop java)	Java/CVE-2008-5353 Java/Selace
openStream()	JDK and JRE 6 (desktop java)	CVE-2009-3867 ; Java/OpenStream

Opera

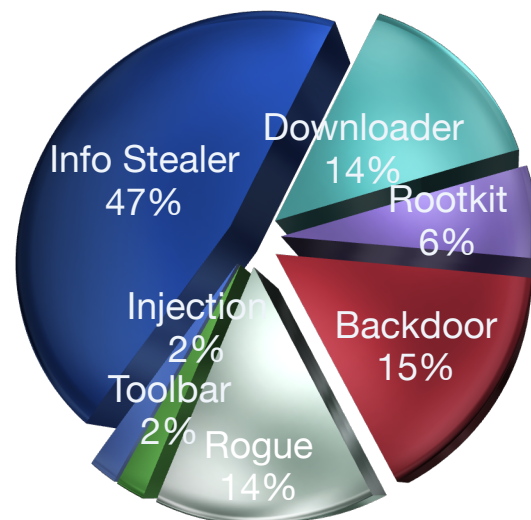
CVE Reference	Affected	Description
CVE-2006-0005	Opera 9.21 and earlier	Microsoft Windows Media Player Plugin EMBED element buffer overflow
CVE-2009-3269	Opera 9.52 and earlier	Opera TN3270

Threat Landscape

Classification of Prevalent Trojans

The most prevalent Trojan families are information stealers, accounting for 47% of the total processed in H1 2010. Threats perpetrated by organized cybercriminals show a widespread prevalence of Win32/Zbot, Win32/Spyeye, Win32/Gamepass, Win32/Bancos, and Win32/Banker—known families of threats that target users, banking information, online services transactions and information related to online games.

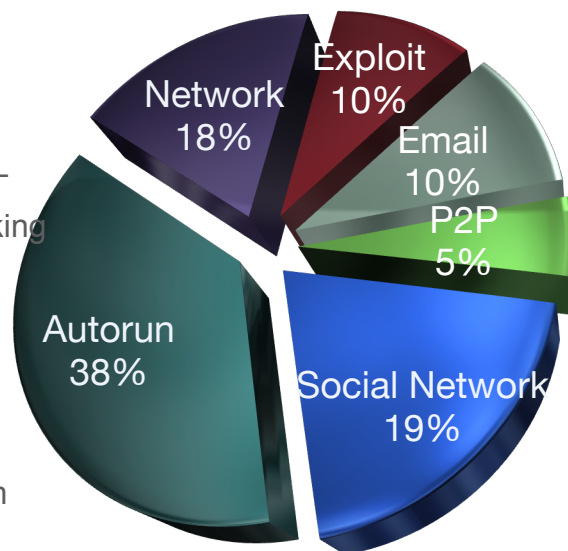
Malicious remote administration tools (RAT) and Backdoor Trojans account for 15% of the total distribution of classified Trojan threats.



Classification of Prevalent Worms

The three most prevalent worms propagate through removable drives, *autorun.inf*, network shares and social networking sites.

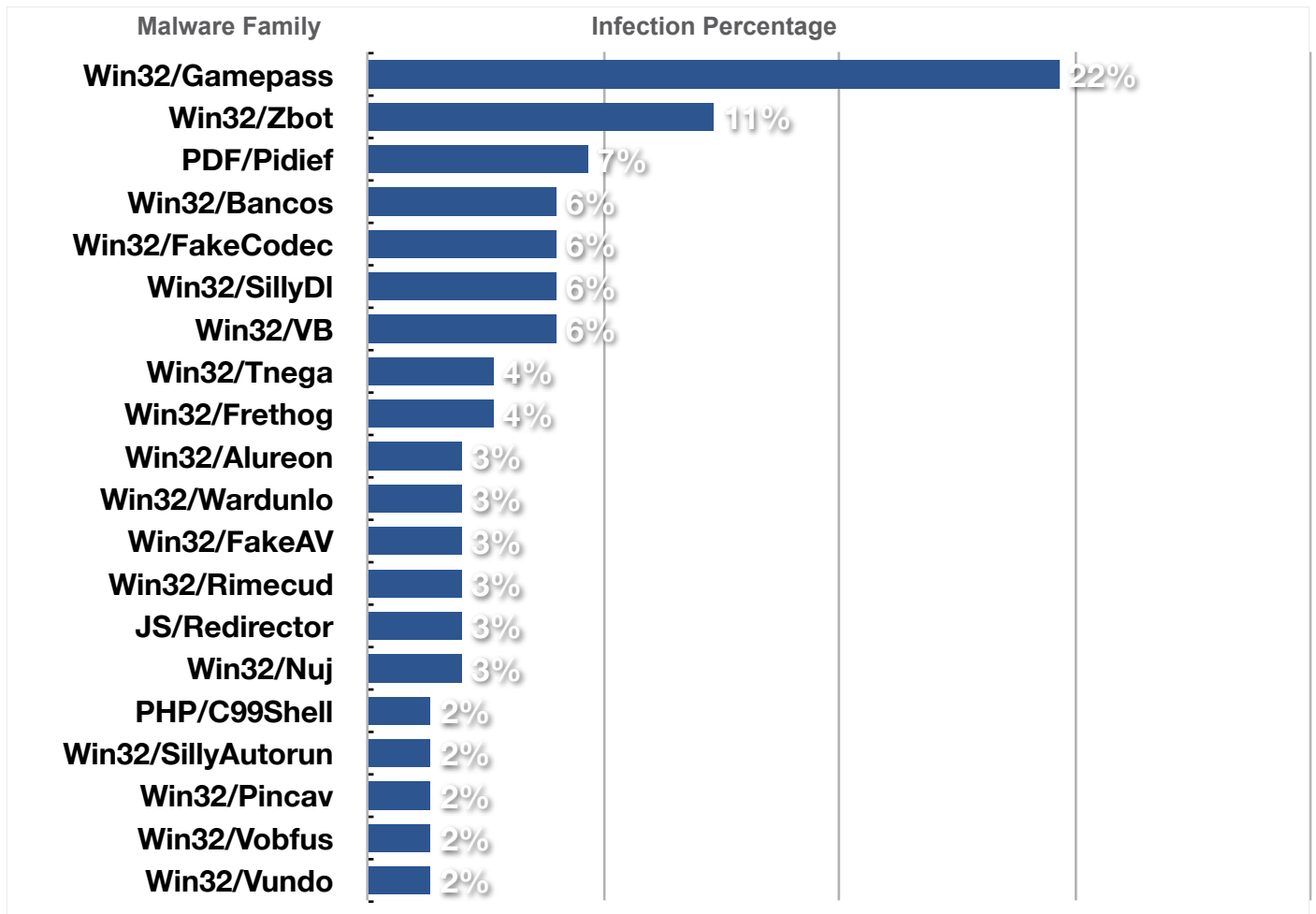
Win32/Rimecud, Win32/Frethog, Win32/Nuj, and Win32/Vobfus are known prevalent autorun families in H1 2010. Win32/Malar and Win32/Conficker are also prevalent worm families capable of propagating through autorun, network shares and exploits (MS08-067, MS06-040, MS05-039, MS04-011, MS03-026 and MS04-007). While, the prevalence remains active for Win32/Fruspam, spreading via email message attachment, removable drive, and P2P file sharing networks.



The social networking worm Win32/Koobface is increasingly active, with more components and variants each day.

Threat Landscape

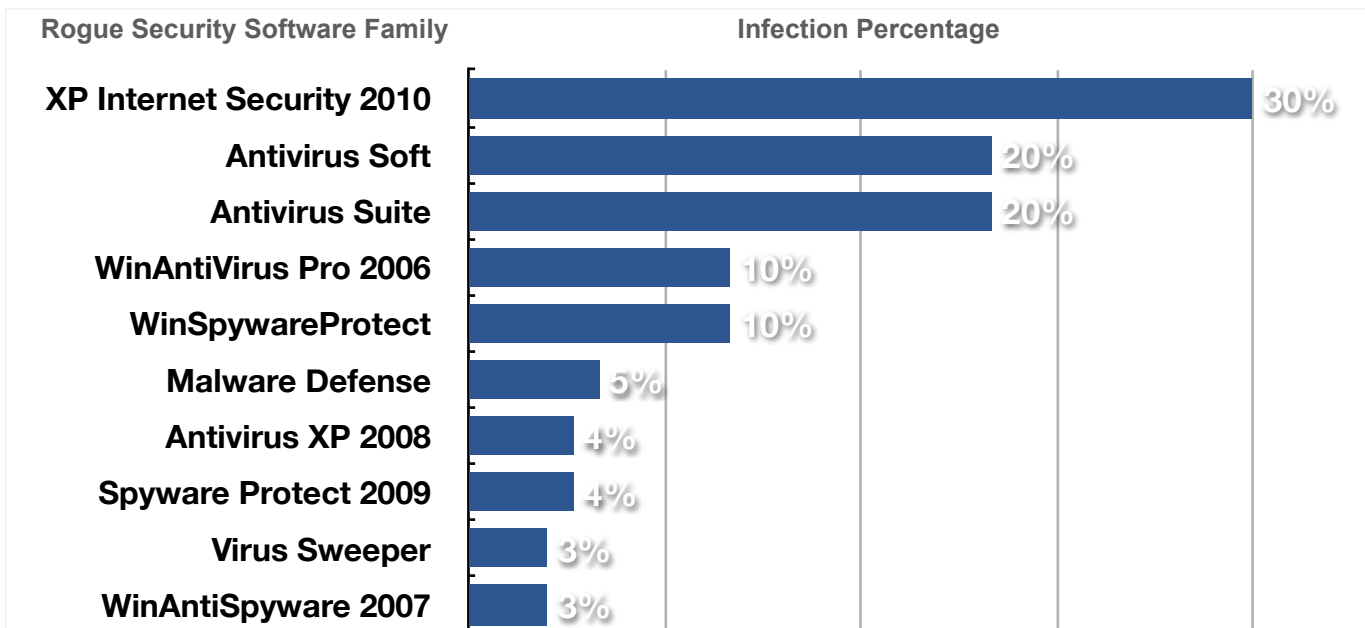
Top 20 Most Detected Malware Families



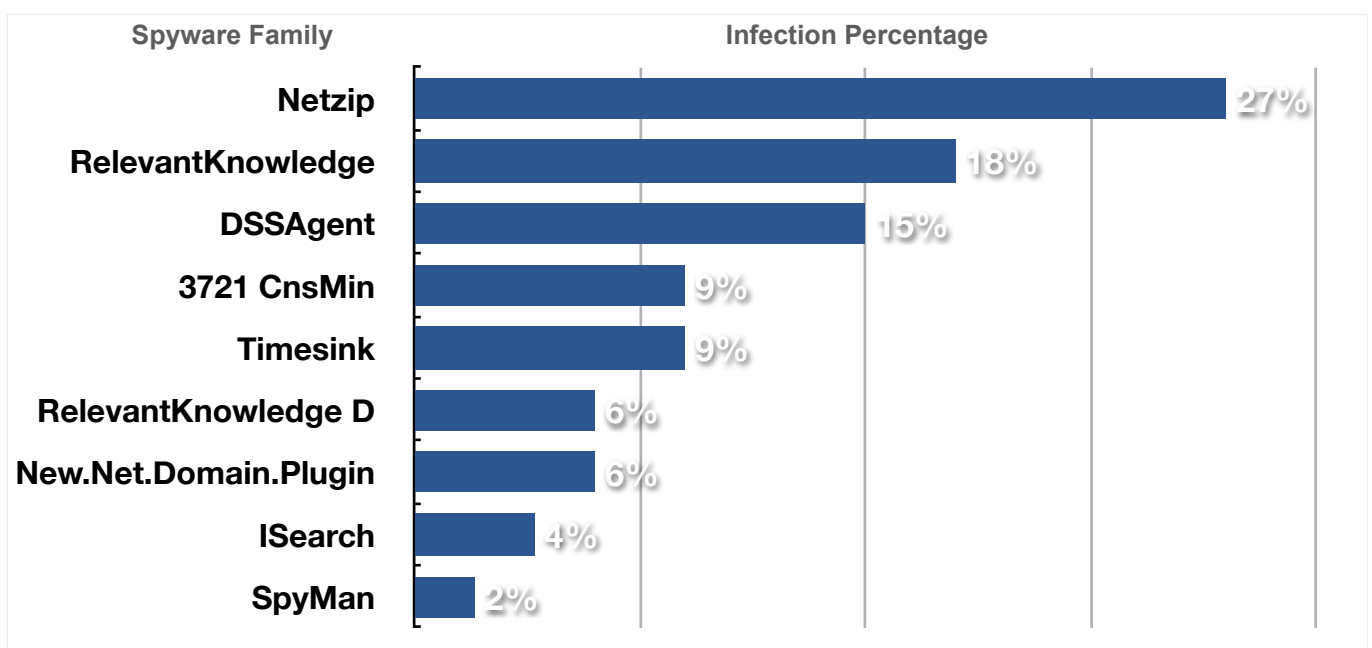
Based on customer-escalated infection, Win32/Gamepass, a family of game info stealer, is the most prevalent malware family base, followed by banking and infostealer Win32/Zbot.

Threat Landscape

Ten Most Prevalent Rogue Security Software

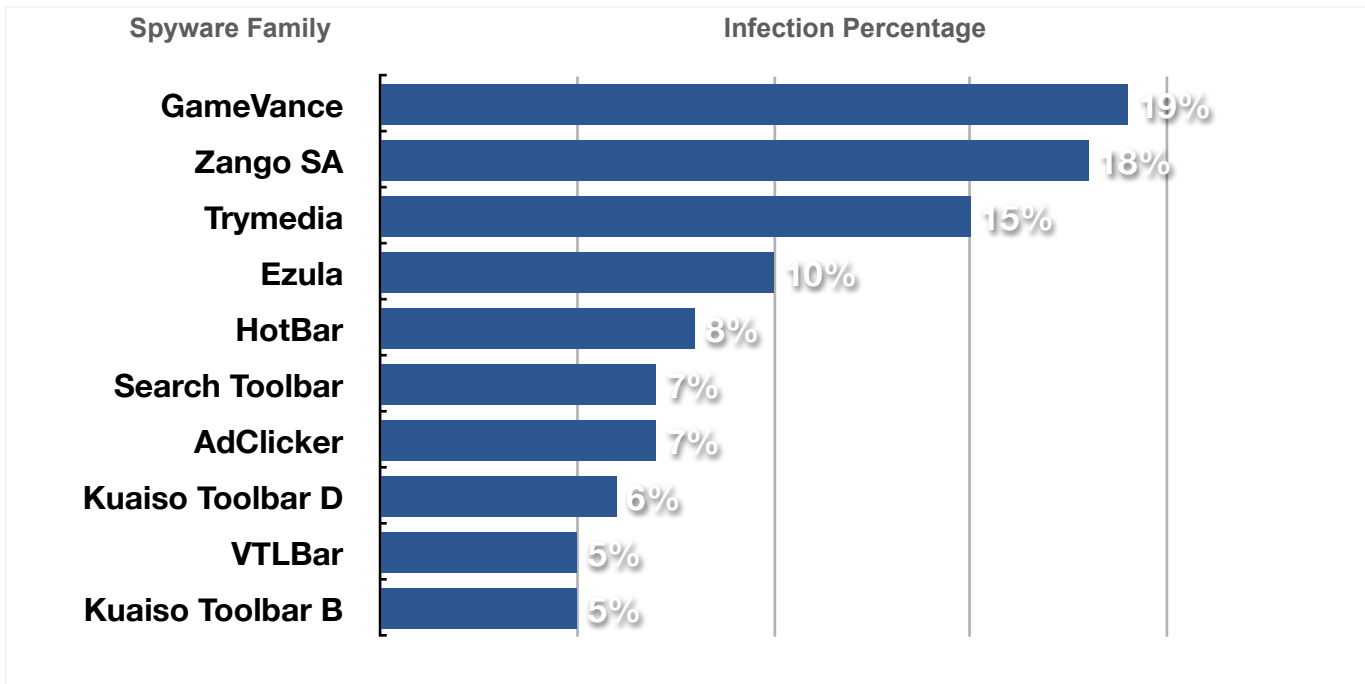


Top 10 Most Prevalent Spyware Infection



Threat Landscape

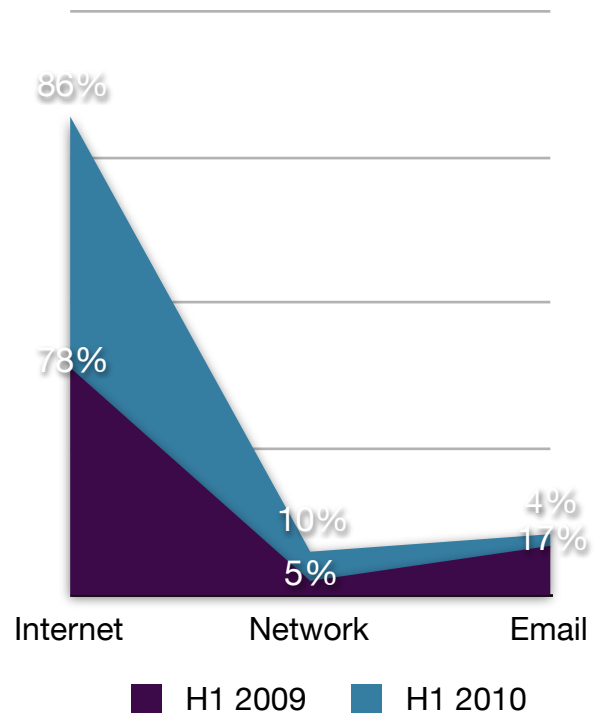
Top 10 Most Prevalent Adware Infection



Threat Distribution Vector

The Internet is the primary threat distribution vector and source of infection. This equates to 86% of the total threat landscape, a growth of 8% over last year. Notably, the email vector dropped significantly from 17% to 4%, while network (e.g., removable and shared network drives) increased by 5% in H1 2010.

The 5% drop in Windows i386 (32bit) portable executable infection as discussed in Malicious File Format Distribution confirm this trend, and further demonstrates Web-based executables are notably increasing this year.



Threat Intelligence






Rogue Security Software

The U.S. Federal Bureau of Investigation (FBI) warned Internet consumers about the threat of pop-up security messages in a press release published December 11, 2009. It was further noted that scareware, also known as rogue security software or Fake AV, has already cost victims more than \$150 million [1].

Leading off from a steady surge in popularity of rogue security software from previous years, H1 2010 also saw this category of malware continue its dominance. Google, the most popular Internet search engine, became an alluring target for organized criminals to distribute rogue security software. Research presented this year at the 3rd Usenix Workshop on Large-Scale Exploits and Emergent Threats in San Jose, Calif. highlighted that the distribution of Fake AV accounts for 15% of threats detected by Google on the Web [2]. Google researchers analyzed 240 million Web pages over a 13-month period and discovered 11,000 domains involved in rogue security software distribution. The research also emphasized its finding of the steady rise of rogue security software domains from 93 unique rogue security software domains in January 2009 to 587 as observed in the last week of January 2010.

Typically, rogue security software is fake protection software that will display bogus alerts post-installation on the infected machine and then coerce the user to pay up for its fake service to clean up the system. User systems that fall prey to rogue security software then become a platform for annoying warnings, forceful payment pop-ups and other malware that gets pulled down from the Internet. In the following sections we will see a few interesting trends relating to rogue software observed in H1 2010.

Report Highlights

-  Rogue security software remains the most prevalent Internet threat.
-  Economies of scale identified using custom clones feature of existing rogue security software and the multiple language support.
-  Multiple language support enables international cybercriminal operation and distribution to more geo-specific targets.
-  Rogue security software distribution through Blackhat SEO, advance social engineering and drive-by download attacks.
-  Expanding cybercriminal partner networks are enabling other prevalent threats such as Win32/Zlob, Win32/Bredolab and PDF/Pidief distribute Rogue infection.

Threat Intelligence

Custom Clones

An interesting trend saw an influx in clones of existing rogue security software. The huge number of such clones clearly shows how lucrative this has become for malware authors. The most deceiving clones are those impersonating legitimate anti-malware products and Web sites hosted through a typo-squatted domain. Certain rogue security software added a new feature that enables auto-custom clones on every installation.

One such highly popularized example of rogue software with multiple clones is Antispyware XP. [Figure 1]

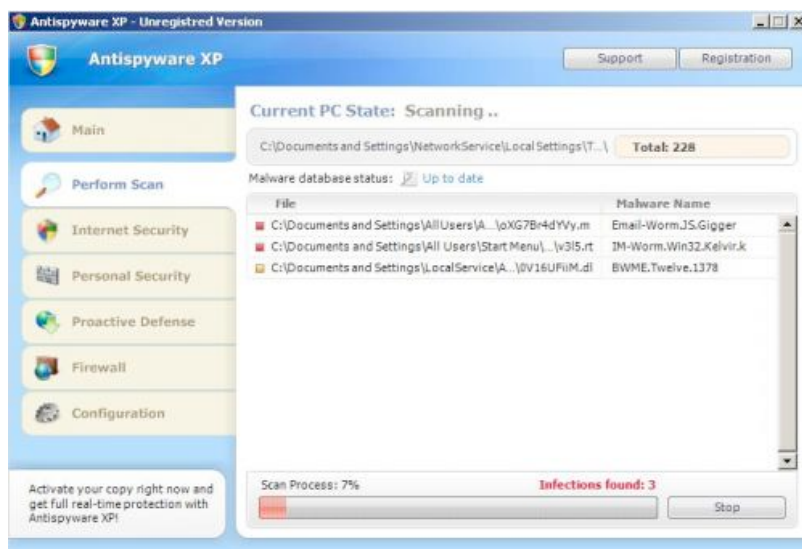


Figure 1 - Rogue Antispyware XP

The same rogue security software also came in various cloned copies using different names. Interestingly, the associated source malware setup file drops a custom clone copy of itself on every installation. It uses a template to construct its product name based on the infected system's Windows operating system version [3] as shown below:

Windows XP	Windows Vista	Windows 7
xpsmartsecurity2010	antispywarevista	antispywarewin7
xpsmartsecurity	vistasmartsecurity	win7smartsecurity2010
xpsecuritytool2010	vistasmartsecurity2010	win7smartsecurity
xpsecuritytool	vistaantimalware	win7antimalware2010
xpsecurity	vistaantimalware2010	win7antimalware
xpdefenderpro	vistasecuritytool	win7securitytool2010
xpdefender	vistasecuritytool2010	win7securitytool
xpantimalware2010	totalvistasecurity	totalwin7security
xpantimalware	antivirusvista	antiviruswin7
totalxpsecurity	vistasecurity	win7security
antivirusxp	vistadefenderpro	win7defenderpro
antispywarexp	vistadefender	win7defender

Threat Intelligence

Multi-Language Support

Aside from Windows OS version auto-customized clones, organized cybercriminals also introduced multiple language support in H1 2010.

The rogue security software business became a global cybercriminal operation, enabling distributions to more geo-specific targets [Table 1].

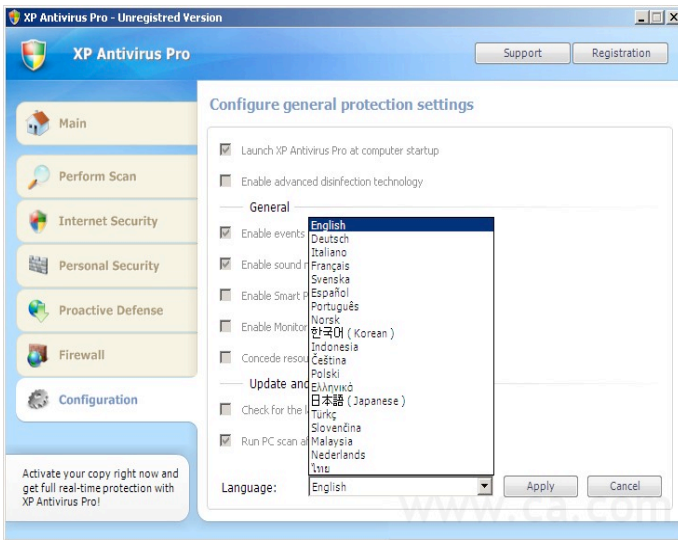


Figure 2 - Multiple Language Support

Language	Major Countries
English	
German	
Italian	
French	
Swedish	
Spanish	
Portuguese	
Norwegian	
Korean	
Indonesian	
Czech	
Polish	
Greek	
Japanese	
Turkish	
Slovak	
Malaysian	
Dutch	
Thai	

Table 01 - Major Supported Countries

Distribution Points

Rogue security software distribution points include email, instant messaging and the Internet. Specifically, the most popular targets are Google, Twitter, Facebook and YouTube. Rogue security software employs an advanced social engineering attack to increase the chances of installation [Figure 3] [4].

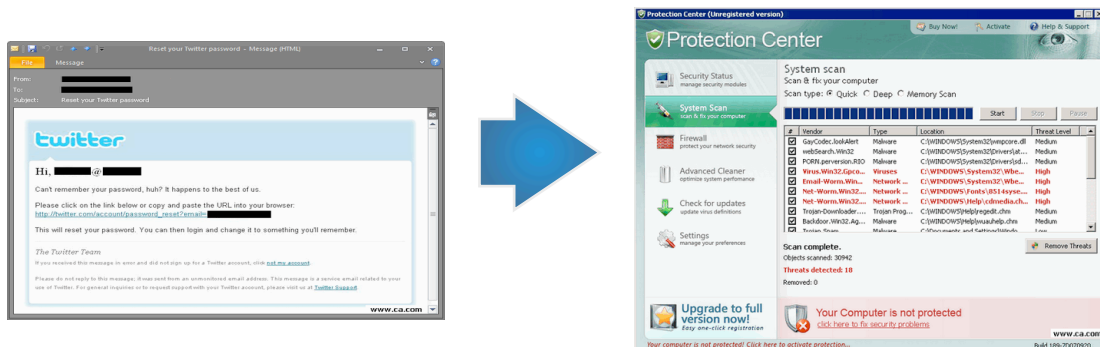


Figure 3 - Spam Masquerading as Twitter Password Reset Notification

Threat Intelligence

Blackhat SEO Attack

The most prevalent distribution of rogue security software is through Blackhat SEO (search engine optimization). Most rogue security software online distributions are encountered on domains that contain trending keywords. These domains are often compromised Web sites controlled by automated Blackhat SEO bots. Using a cloaking technique, the attacker manipulates and deceives the search engine in two ways: 1) Keyword stuffing, which is inserting scraped contents from legitimate sources or 2) Link farming, or hyperlinking to other Web sites to boost search engine rank.

Once the attacker successfully spams the index of the Google search engine, it will start to influence the ranking of the attacker's controlled pages in Google's search engine result page or *SERP*. This technique is called *Google bombing*, manipulating SERP to increase the likelihood of people finding it.

In this first half, we observed the Blackhat SEO serving rogue security software and drive-by download attacks.

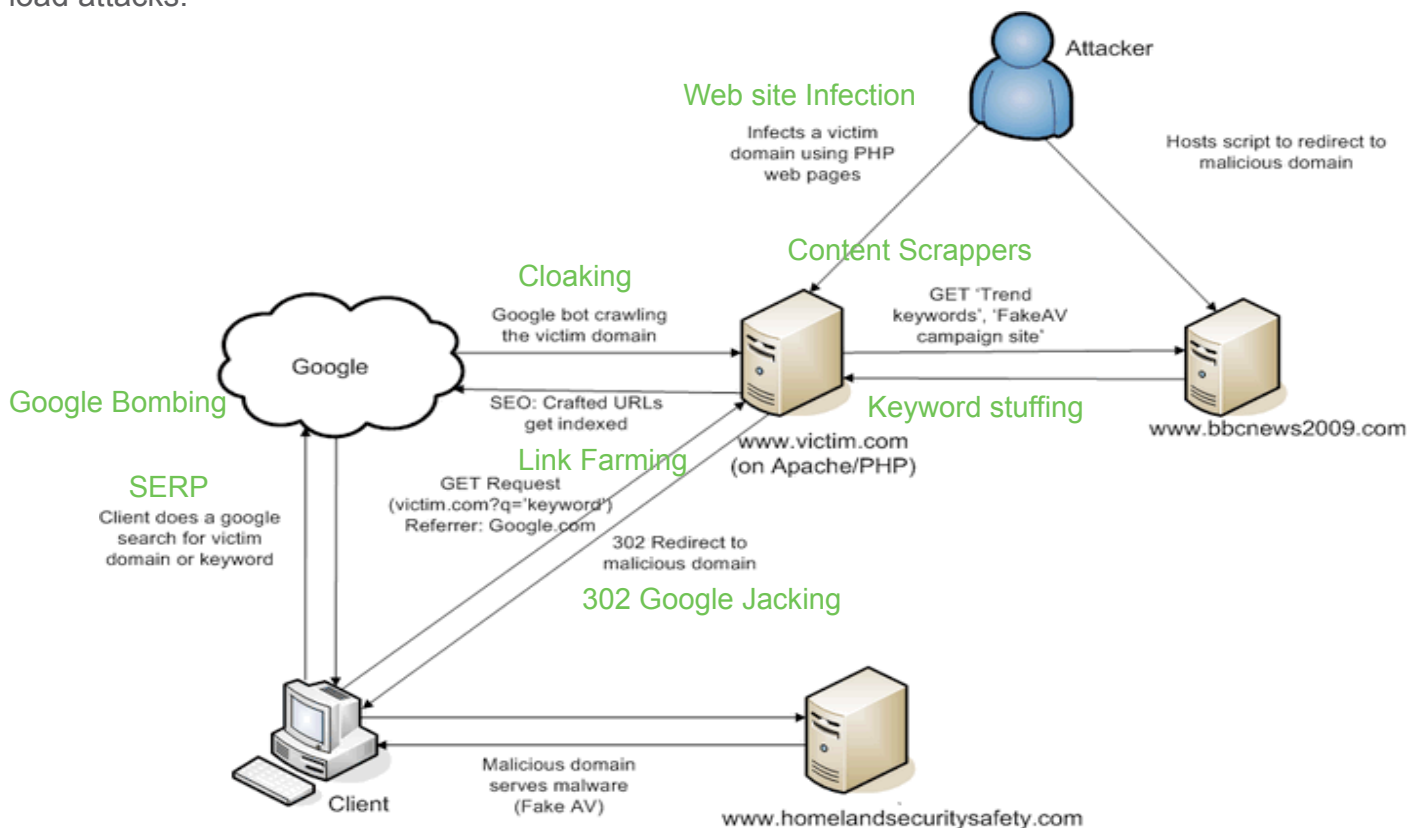


Figure 4 - Google Blackhat SEO Attack from January 2010 [5]

Threat Intelligence

Related Detection

Malware Family	Description
Win32/FakeAV Win32/FakeAVDI Win32/FakeAlert	Detection generally associated with rogue security software installer, downloader and components that display alert messages.
Win32/Multidropper Win32/Bugnraw Win32/Oneraw Win32/Refpron Win32/Donloz Win32/Droplet Win32/Renos	Family of Trojans leading to rogue security software infection.
Win32/Zlob Win32/Bredolab PDF/Pidief Win32/Ertfor	Prevalent threats that participate and deploy rogue security software.

Threat Intelligence

Crimeware

Threats are classified by categories and types. For example, 73% of malware processed in H1 2010 would be categorized as Trojans. However, Trojan detection is a classification and identification for a specific piece of code. We have classified the most detected Trojans in H1 2010, finding that 96% function as a component of a larger underground market-based mechanism we call *Crimeware-as-a-Service*.

Crimeware is class of threat designed to automate cybercrime. It collects and harvests valuable information through a large-scale malware infection. It is primarily designed to perpetrate data and identity theft to access user's online banking services, shopping transactions, and other Internet services.

The U.S. Federal Trade Commission (FTC) Consumer Sentinel Network Data Book recorded over 1.3 million consumer complaints for calendar year 2009 [6]. Fraud-related complaints account for 54%, with subsequent consumer losses amounting to over \$1.7 billion; 40% are fraud-related complaints using credit cards as payment. Identity theft ranked number one, accounting for 21% of overall recorded consumer complaints. Furthermore, the report explains that fraud commonly takes place through Internet and email, accounting for 48%, and 12% respectively.

The technological aspects of real-world criminal activity demonstrate a much broader and complex issue with today's technology. Organized criminals are just like any regular organization, finding market opportunities and expanding visibility using technological presence (e.g., Web site, Facebook, online advertisement) to increase financial gain.

Organized cybercriminals understand Internet business models and know how to operate to avoid legal prosecution.

Report Highlights

- 96% of Trojans are components of a larger underground market-based mechanism we call *Crimeware-as-a-Service*.
- Crimeware is primarily designed to perpetrate data and identity theft.
- The economics of crimeware is "Delivering threats over the Internet."
- Crimeware is an on-demand and Internet-enabled service.
- Crimeware's main distribution mode is through *social engineering* and *drive-by download* attack.
- Crimeware highlights cloud computing as a new delivery model.
- Social media are the latest crimeware market.
- Crimeware's latest offensive capabilities highlights Zeus and Spyeye.

Threat Intelligence

Business Model

A business model describes the rationale of how an organization creates, delivers and captures value to generate revenue. The economics of crimeware is “*Delivering threats over the Internet.*” It is an on-demand and Internet-enabled service.

Internet-enabled Service

Affiliate ➤ Revenue Sharing

Advertising ➤ Referral fees and commissions

Consumption ➤ Installation fee

Transaction ➤ Transaction fee

Cloud-enabled ➤ value-added revenue opportunity

On-Demand

Network, Internet-based delivery ➤ remote and bot controlled

Economies of scale ➤ mass distribution (e.g., encrypt, pack)

Commoditized ➤ accessible, easy adoption, ready-made

Interoperability ➤ browser-based language (e.g. JavaScript, Web application)

Usage-based revenue ➤ pay-per scheme, referrals, affiliate, transaction

Organized cybercriminals capture value from the time a user visits a compromised Web site (downloading and installing a piece of malware and executing its infection payload) to the time when the attacker finally relinquishes control (when the malware is identified and removed). Each action represents an opportunity to generate revenue, making Crimeware a form of modular malicious code.

The modularization strategy creates advantages in terms of scalability, performance and flexibility to respond in a changing environment. Each module is designed to perform specific task. Working together, they become a symbiotic *crimeware ecosystem*.



Figure 5 - Crimeware Business Model

Threat Intelligence

Crimeware Ecosystem

Zbot, Bredolab, and Cutwail are known prevalent modular threats that play an important role in spam campaigns observed during H1 2010.

Win32/Cutwail, also known as “Pandex,” is a threat-family responsible for sending spam emails that contain contents like Canadian pharmacies, diploma mills, and Rolex replicas.

Win32/Bredolab is a threat family responsible for downloading and executing other malicious malware into the user's system. Bredolab is also notable for downloading FakeAV variants such as Win32/ProtectCenter.

Win32/Zbot is a threat family that plays the most important role for the crimeware botnet. It is responsible for stealing personal information like bank account numbers and online banking credentials, credit card information and personal account details.

These three distinct classes of malware represent the anatomy of crimeware. Email spam botnets such as Cutwail, Waledac and Storm are modular threats that serve as a means to *distribute* threats. Once the attack or threat arrives at a targeted platform, the *installation* module penetrates and installs the *payload*. The payload is a part of crimeware that generates revenue for the organized cybercriminal. The payload may install and execute other threat components or modules such as root-kits, click fraud, sniffers, hack tools, and keyloggers to assist cybercriminal. These components act as a *service* module that may extend the crimeware payload further.

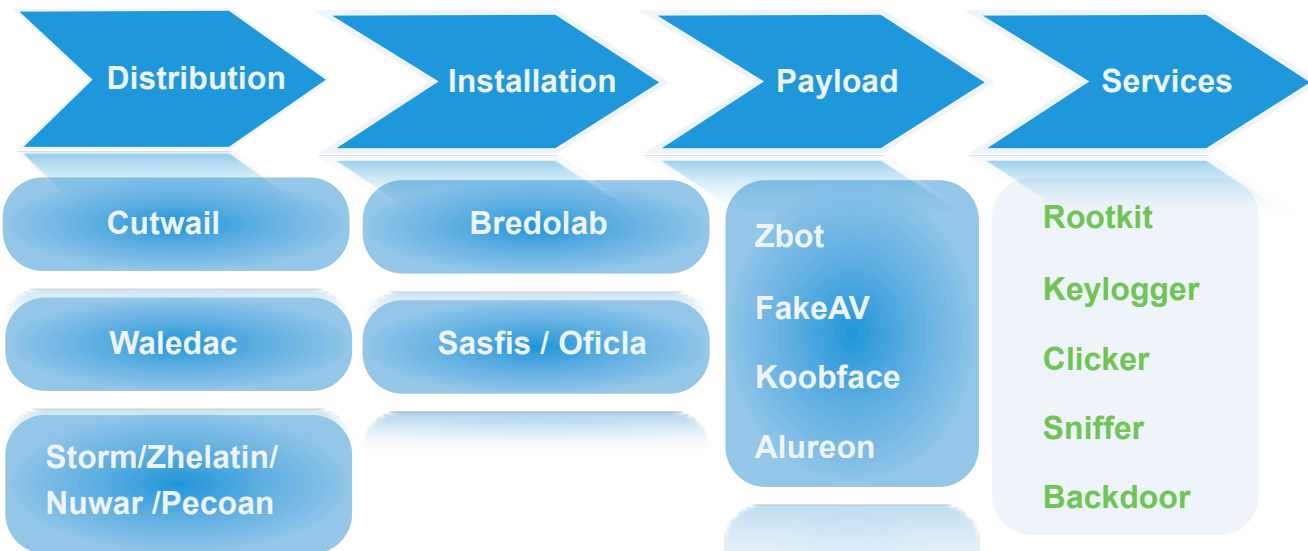


Figure 6 - Anatomy of a Crimeware Ecosystem

Threat Intelligence

Crimeware Distribution

Crimeware is distributed mainly through *social engineering* and *drive-by download* attacks. A combination of *technology* and *psychology* enables attackers to effectively use social engineering techniques to manipulate unsuspecting users into voluntarily divulging sensitive information, or fool them into performing harmful and destructive actions.

Psychological Effect of Authority Pressure and Favor on Compliance

The first option is to send an authoritative email asking the target user to open or click a link. The link will lead to a legitimate-looking Web site where the user will be asked to comply by downloading and executing different kinds of reports, tools, and statements for example the IRS Fraud Application, fake Microsoft Outlook Update [Figure 7], ICS Monitoring, FDIC Deposit Insurance Coverage, Social Security Statement, Macromedia Flash Player Update, and Marcus Law Center and Crosby & Higgins Copyright Infringement Lawsuit.

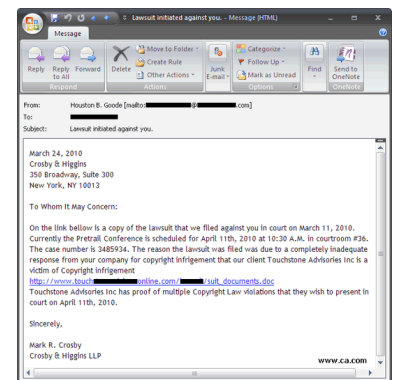


Figure 7 - Lawsuit Against You

The second option is to send an authoritative email asking the target to open an attached archive file pretending to be a legitimate tool from a popular brand examples include the Myspace Password Reset Confirmation [Figure 8] and the Vodafone Balance Checker Tool.

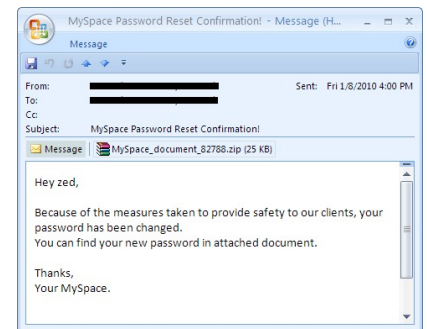


Figure 8 - MySpace Password Reset

The third option is the “phishing with a twist” technique [Figure 9], often targeting Facebook and Myspace users, who are lured to click a link from an email. The link is connected to a legitimate-looking Facebook or Myspace site, where the user is asked to type in credentials to log in. After logging in, the user is asked to download and execute an “update tool.”

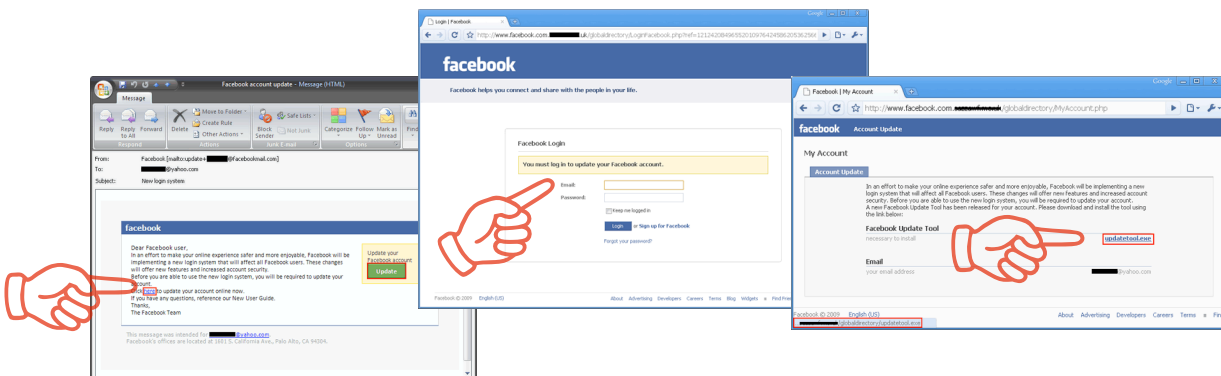


Figure 9 - The value of “Pay-per-Action”

Threat Intelligence

The fourth option is the *social engineering* and *drive-by download* combined technique. Unsuspecting users receive an authoritative email requesting the user to comply for a returned favor. The link is redirected to a malicious server hosting browser-based exploits (exploits in the wild are discussed on pages 11-13).

Figure 10 displays an email from the IRS requesting the user to click the “Tax Refund Request Form” to receive a returned favor of \$760.22.

The fifth option is called the *infection combo* technique, a combination of social engineering tricks exposing vulnerable users to phishing and drive-by download attacks.

As shown in figure 11, a targeted user receives an email notification from his/her bank. When the user clicks the link, it leads to a legitimate-looking Web site crafted to perform phishing attacks to gain user’s credentials. Simultaneously in the background, it loads a piece of malicious code that exploits a list of browser-based vulnerabilities resulting in a drive-by download attack. Once the phishing attack is complete, it loads another page asking the user to download and install a tool.

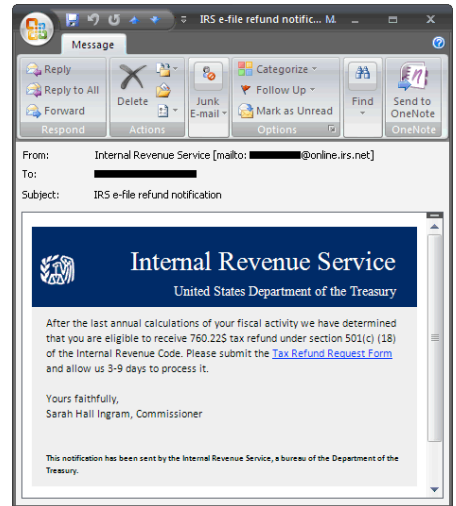
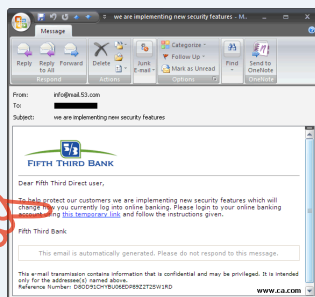
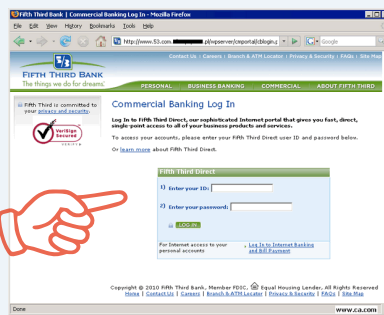


Figure 10 - Tax Refund Request Form

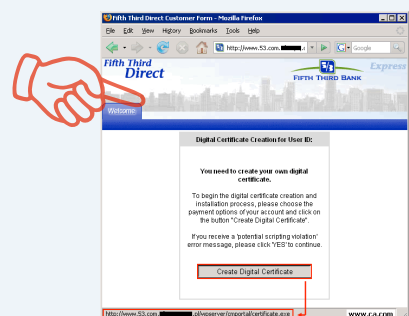
1. Click a Link



2.1 Phishing Attack



3. Click to Download



2.2 Drive-by Download Attack



Figure 11 - Infection Combo Technique

Threat Intelligence

Cloud Computing as a Crimeware Delivery Model

Crimeware is a cloud-enabled threat. Gartner defines cloud computing as “a style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to customers using Internet technologies.” The National Institute of Standards and Technology (NIST) definition of cloud computing describes three service models: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS); and four deployment models: Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud [7].

In general terms, cloud computing includes Web services and applications that perform specific functions traditionally carried out with software installed on a desktop computer. Specifically, these are Web and Internet applications (e.g., Google Apps), social media platforms (e.g., Facebook, YouTube, Flickr, Wordpress), online productivity suites (e.g., Apple iWorks, Google Docs, Microsoft Office Live), and real-time mobile Web services (e.g., Twitter, Google Maps, RSS Readers). The ongoing paradigm shift from desktop to cloud computing also shows the emergent transition of the threat landscape to the cloud as a means of distribution and infection.

The most popular cloud services today are Google and social media-related websites. Facebook, with an estimated 500 million users spending at least six hours per month, equates to 54% of the world’s most popular Internet brands, according to a Nielsen blog posted on June 15, 2010 [8]. It is evident that organized cybercriminals perpetrating crimeware pay attention to these business opportunities, taking advantage of the Internet’s most popular brands to victimize and distribute crimeware.

Notable Abuse of Cloud Services

Google Group

In May 2010, CA Technologies’ ISBU received a malicious spam campaign using Google Groups (a service that supports discussion groups, including many Usenet newsgroups) to host a malicious email attachment detected as Win32/FakeAV variants [9] [Figure 12].

In September 2009, a Trojan detected as Win32/Grubpot.A was spotted using Google Groups to distribute command and control functionalities [10].

Amazon EC2

In December 2009, a spam campaign spreading a notable variant of Zeus bot was discovered taking advantage of Amazon EC2 cloud-services for the command and control functionalities [11] [Figure 13].

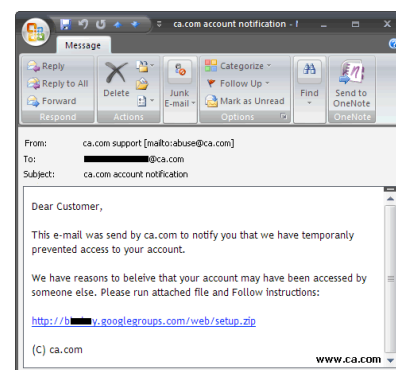


Figure 12 - Google Group

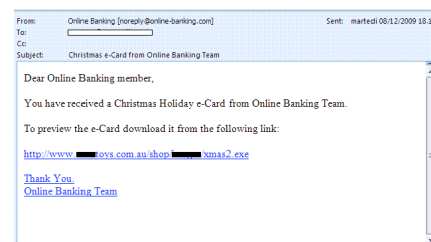


Figure 13 - Amazon EC2

Threat Intelligence

Social Media: Twitter Spam (“Twam”)

A recent malicious spam campaign poses as an email notification targeting unsuspecting Twitter and YouTube users. The email contains pornographic images to effectively lure the target to follow a compromised Web site hosting a drive-by download attack [12] [Figure 14]; consequently causing Win32/Bredolab and Win32/FakeAV variant infections. This is a campaign with an infrastructure and known established capability of an email spam botnet.

However, an emerging spam trend targets social media tools such as Twitter and Facebook. Twitter Spam (also known as “Twam”) is an increasing trend that varies from annoyance to scams, phishing attacks and those serving malware. Spammers use legitimate link-shortening services to deliberately obscure the malicious links. A year ago, we witnessed an infestation of malicious links enticing users to *juste.ru* to watch a “Best Video” posing as embedded content from YouTube. However, in the background, the Web site loads an iframe that performs PDF exploits and then installs the rogue security software “System Security.”

The trend of malicious Twitter spams are more frequent and use more social engineering tricks to effectively persuade target users to malicious links.

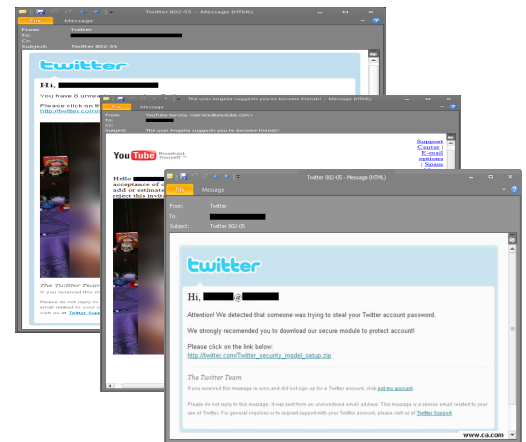


Figure 14 - Twitter Spam Campaign



Figure 15 - Twitter Follower Spam [13]



Figure 16 - Twitter Trending Topic Attack

H1 2010 Twitter Trends

January: Twitter “Follower Spam” Continues

Twitter sends an email notification whenever someone signs up to “follow” you [Figure 15].


February: Compromised Twitter Accounts

Twitter pushed out a password reset to accounts that were believed compromised using “dictionary attack” - a targeted technique using a pre-arranged list of user names and passwords harvested from torrent and download sites [14].

March: Direct Message “Phishing Attacks”

In late February, the “Lol Bzpharma” phishing attack was making its rounds. This was immediately followed by scams involving diet/weight loss plans, themed.

April: Impersonating Twitter Support.

A spam run disguised as a “Twitter Support” email notification requests users to follow a link leading to a fake online Canadian Pharmacy. 

May: Twitter Account “Confirmation Change”

Another round of phishing attacks disguised as Twitter notifications asking users to follow a link to confirm the change.

June: Twitter Trending Topic Attack

Compromised and generated accounts use targeted keywords [Figure 16], phrases and trending topics to serve backdoor Win32/Bifrose variants. We also observed a “Twitter account password” spam campaign serving Win32/Alureon and Win32/FakeAV variants [15].

Threat Intelligence

Social Media: Facebook Viral and Abusive Apps

The Facebook ecosystem is a very attractive platform for malicious users to deploy different types of abusive activity. Threats may include cyberbullying, stalking, identity theft, phishing, scams, hoaxes and annoying marketing spams.

The infamous Koobface botnet has successfully established an offensive capability to perform viral and abusive attacks against social media platforms such as Facebook, Twitter, MySpace, Hi5, Friendster, Bebo, Tagged, MyYearBook, Netlog and Fubar. In the latest attack, we have observed Koobface propagation vectors as direct messages and instant messaging.

Email spam botnets also lure users through social network themes, for example Win32/Bredolab "Facebook Password Reset Confirmation" [16], and Win32/Fruspam "You have got a new message on Facebook!" [17].

The increasing events of Facebook viral and abusive applications are the most noteworthy in H1 2010.

Name: "Stalker Application"

Description: Facebook application that entices users to see who's checking, stalking, or spying their profile. Facebook users receive notification via the Facebook wall and post a photo montage of all infected friends [18]. It is also known using the following tag lines:

Who is stalking you?

Who is checking my profile?

Who is your top follower?

Type: Rogue Application

Security Risk: Account access and control, privacy violation and viral activity.



Name: "Quiz Scam"

Description: Facebook application that bombards users with requests to take quizzes like the "IQ Test."

Type: Rogue Application

Security Risk: Steals mobile numbers and sends premium text messages, resulting in unwanted charges to user's regular mobile phone bill.



Name: "Naughty Camera Prank! [HQ]"

Description: Facebook application that entices users to check an illicit video entitled "this is without doubt the sexiest video ever! :P :P :P."

Type: Rogue Application, Spammer

Security Risk: Account access and control, clickjacking, viral activity and exposure to FLV Player Adware installer.

**Name: "Friends Revealed"**

Description: An application that usually appears on the Facebook wall and claims that a friend (who's infected) answered several questions about the target (you). Once installed, it spams the same application to all the target's Facebook friends.

Type: Rogue Application, Spammer

Security Risk: Account access and control, privacy violation and viral activity.

**Name: "Distracting Beach Babes [HQ]"**

Description: Facebook application that entices users to check an illicit video entitled "this is hilarious! lol :P :P :P."

Type: Rogue Application, Spammer

Security Risk: Account access and control, clickjacking, viral activity, and exposure to FLV Player Adware installer.

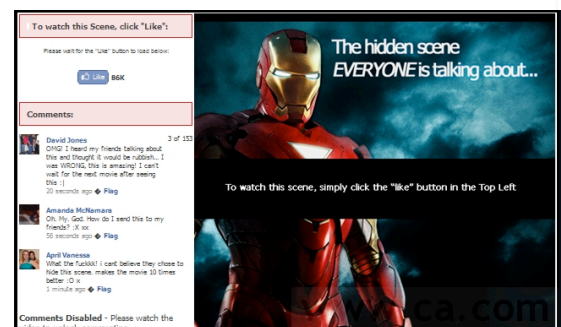
Note: Rerun version of "Naughty Camera Prank! [HQ]"

**Name: "Like"**

Description: Facebook application that entices users to click a "Like" button using a catchy subject line, for example "OMG! OMG! OMG! I Can't Believe this HIDDEN IRON MAN 2 SCENE! Check this out!" [19].

Type: Rogue Application, Spammer

Security Risk: Account access and control, "like-jacking" viral activity and exposure to phishing attack.

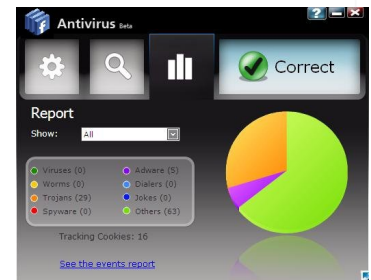


Name: "Facebook Antivirus Beta"

Description: A deceptive application that entices users to install a Facebook Antivirus beta version. Once installed, the malicious application will start tagging friends in a photo and post a message on the wall saying "Try it, really works!" [20].

Type: Rogue Application, Spammer

Security Risk: Account access and control, privacy violation and "photo tagging" viral activity.

**Name:** "Teacher Beats Up"

Description: A deceptive application that entices users to check a shocking video often with this message "I am shocked!!! The teacher nearly killed this boy:
<http://bit.ly/aWeBM1> - Worldwide scandal!"

Type: Rogue Application, Spammer

Security Risk: Account access and control, privacy violation and viral activity.



In the most recent Facebook viral attack, the rogue application "Teacher Beats Up" seems to purposely use Bit.ly - url-shortening services, to market the attack capability with the recorded traffic statistics.

The viral shelf-life was six days (June 9-14, 2010). The overall clicks within this timeframe were 190,743 and are mostly referred from Facebook.com, email clients, IM, air apps, mobile, and touch Facebook [Figure 17]. This is a sign of showing off, a rich opportunity to monetize this vector in the underground market.

This security risk concerning the world's most populated Internet community reflects how organized and sophisticated cybercriminals can perpetrate and harvest users' identities and profiles, using them to launch dictionary hack-attacks in various levels of infrastructure (public, private and government).

Top Referrers ?

Referring Site	Click(s)
www.facebook.com +	129,452
Email Clients, IM, AIR Apps, and Direct +	35,238
Direct Traffic includes people clicking a bit.ly link from: - Desktop email clients like Microsoft Outlook or Apple Mail - AIR applications like Twhirl - Mobile apps like Twitterific or BlackBerry Mail - Chat apps like AIM - SMS/MMS messages It also includes people who typed a bit.ly link directly into their browser	
m.facebook.com +	23,897
touch.facebook.com +	1,833

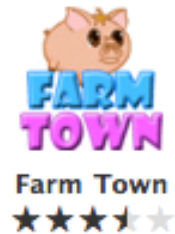
Figure 17 - "Teacher Beats Up" Top Referrers

Furthermore, legitimate Facebook applications cannot escape the prying eyes of cybercrooks, especially those with millions of active online users. In H1 2010, there are two known incidents of malvertisement on Facebook.

Application Name: "Farm Town"

Incident Description: Users reported that the GreetingCards flash advertisement on Farm Town (a gaming application) displays fake alert messages and causes redirection to rogue security software Web sites.

Malvertisement:



Application Name: "Family Link"

Incident Description: Users reported that the GreetingCards flash advertisement on Family Link (a family tree application) displays fake alert messages and causes redirection to rogue security software Web sites.

Malvertisement:



Threat Intelligence

Social Media as the Latest Crimeware Market

The recently observed viral activities and abusive applications in popular social media services like Twitter and Facebook are the result of a strong underground marketing campaign [21].

In a recent research investigation, we observed that a black market is evolving to develop and sell interesting tools such as social networking bots. As shown in Figure 18, underground marketers promote new social networking services that include account checkers, wall posters, wall likers, wall commenters, fan inviters and friend adders. These new crimeware-as-a-service capabilities became evident with the latest Facebook viral attacks and abusive applications.

Facebook.com		<u>SOFTW</u> at allB
Jumbo Bot (All in one) (Friends Acceptor + Friend Adder + Status Updater + Friends Accepted Wall Notification Deleter + Posted Links Deleter + Link Poster + Friends' Comment Deleter + Wall Posts Deleter + Wall Poster + Photo Uploader)	N/A	<input type="button" value="Buy Now"/> \$900.00 \$700.00
Accounts Checker	N/A	<input type="button" value="Buy Now"/> \$120.95 \$95.00
Wall Poster	N/A	<input type="button" value="Buy Now"/> \$320.95 \$250.00
Wall Liker with Commenter (Like and comment on the walls that matches given keywords)	N/A	<input type="button" value="Buy Now"/> \$320.95 \$250.00
Events Wall Poster (Attend Event then send Wall Post)	N/A	<input type="button" value="Buy Now"/> \$320.95 \$250.00
Groups Wall Poster (Join Group then send Wall Post)	N/A	<input type="button" value="Buy Now"/> \$320.95 \$225.00
Verifier and Getting Started (Steps Skipper) NEW	N/A	<input type="button" value="Buy Now"/> \$320.95 \$160.00
Wall Commenter (It post comments on Wall Posts on list of your profiles) NEW	N/A	<input type="button" value="Buy Now"/> \$320.95 \$180.00
Fan Inviter NEW	N/A	<input type="button" value="Buy Now"/> \$320.95 \$180.00
Application Inviter NEW	N/A	<input type="button" value="Buy Now"/> \$320.95 \$250.00
FanPage Wall Poster NEW	N/A	<input type="button" value="Buy Now"/> \$320.95 \$225.00
Classmates Grabber NEW	N/A	<input type="button" value="Buy Now"/> \$320.95 \$225.00
Friend Adder	<input type="button" value="Buy Now"/> \$120.95 \$99.95	<input type="button" value="Buy Now"/> \$275.95 \$225.00
Twitter.com		
Tweets Updater (It allows you to load the list of accounts and it update Tweets on all of them automatically)	N/A	<input type="button" value="Buy Now"/> \$340.95 \$250.00
IDs Grabber (It automatically searches for profiles from the list of search, followers and being-followed from any profile. For e.g. you can grab people, who are following Anderson Cooper and also, who are being followed by her)	N/A	<input type="button" value="Buy Now"/> \$340.95 \$295.00
Follower (It automatically searches for profiles based on your keywords and starts following them)	N/A	<input type="button" value="Buy Now"/> \$340.95 \$160.00
Un-Follower (It automatically checks and un-follow those, who are not following you on list of accounts)	N/A	<input type="button" value="Buy Now"/> \$340.95 \$160.00

Figure 18 - Facebook Crimeware as a Service

Threat Intelligence

Crimeware Data and Identity Theft

Information-stealing Trojans have been the major vehicle for financially motivated attacks. In the first half of 2010, malware families whose main behavior is to steal log-in credentials and valuable information dominated the CA Technologies' ISBU day-to-day anti-malware operation, accounting for 47% of overall Trojan families processed. Threats perpetrated by organized cybercriminals illustrated the prevalence of Win32/Zbot, Win32/Gamepass, Win32/Bancos, Win32/Banker, and Win32/Spyeye. These are known malware families that target a user's banking information, online service transactions, and information related to online games. Win32/Spyeye is the latest offensive development and known infostealer bot in the underground market. The information gathered by these malware families creates finances for exchange of goods in both the virtual and real worlds.

Win32/Zbot "Zeus bot" Targets

Zeus bots are components of the crimeware toolkits available for cybercrime operations. They are primarily designed to steal a user's information and banking credentials as defined by their server-side configuration file. This file contains a list of targeted financial institutions and online services. CA Technologies' ISBU tracked and ranked the percentage of financial institutions targeted by Zeus bot, classifying them to present the distribution of targeted countries during H1 2010 [Figure 19] [22].

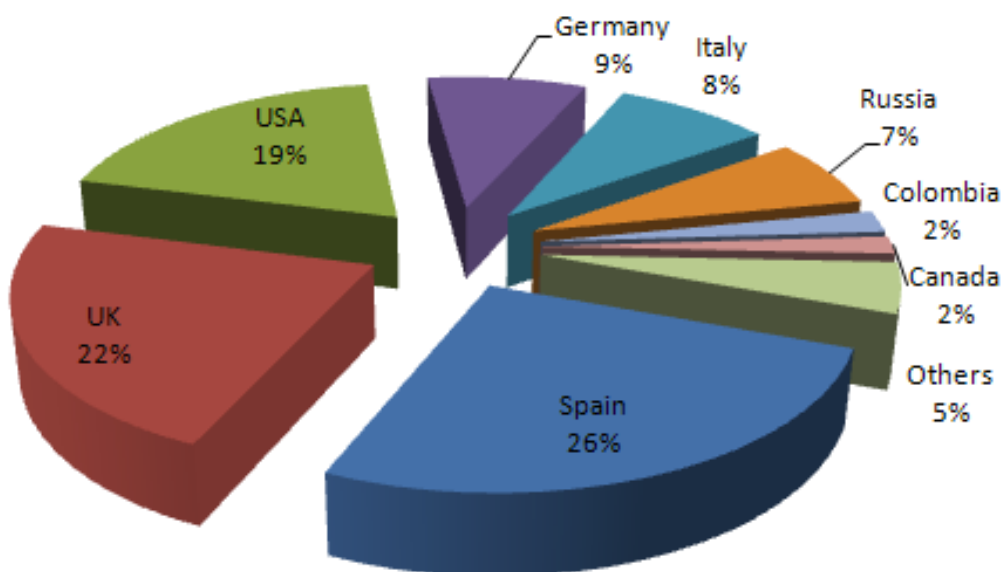


Figure 19 - H12010 Zeus Bot Distribution of Targeted Countries

Threat Intelligence

Spain, the United Kingdom (UK), the United States (USA) and Germany are the top countries targeted by the Zeus bot, making their financial institutions the most vulnerable. However, Zeus bot also explores opportunities in other countries such as Ireland, Australia, Taiwan, France, Pakistan, Portugal, United Arab Emirates, Bulgaria, Turkey, Poland, Netherlands and Belgium.

The latest Zeus bot configuration (referred to as version 3) contains a list of targeted financial institutions from Spain, Germany, the UK and the USA. Previous versions contain a list of financial institutions from different countries around the world, while the new version only contains four targeted countries in two pairs: Spain-Germany and UK-USA.

As observed, the new version of Zeus bots command-and-control (“C&C”) are mostly hosted in Russia.

It is also worth noting that Zeus bot is stealing credentials from known popular online brands as defined by its configuration file:

- amazon.com
- blogger.com
- facebook.com
- flickr.com
- livejournal.com
- microsoft.com
- myfarmvillage.com
- mspace.com
- youtube.com
- odnoklassniki.ru
- vkontakte.ru

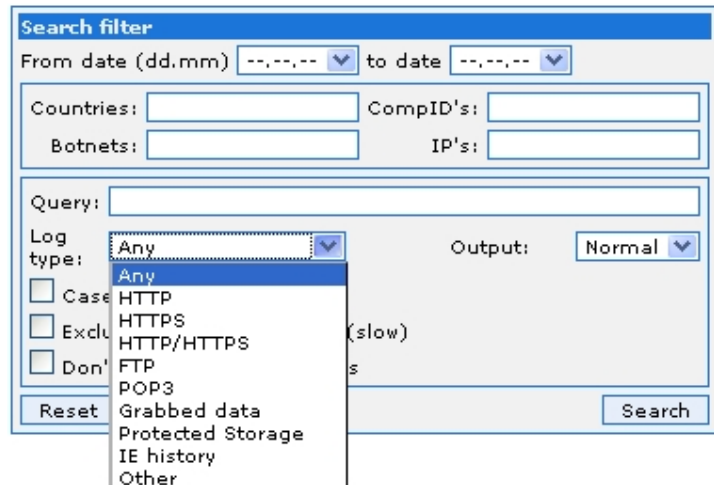


Figure 20 - Zeus Log Types

Amazon, the largest online retailer and known provider of cloud services, is a target in the latest Zeus bot version. This became more evident when we discovered the Zeus command and control distribution hosted in Amazon’s EC2 services in December 2009[11] [23]. Zeus crimeware is not only interested in banking information but also in online services that fuel the crimeware distribution space.

Threat Intelligence

Win32/Spyeye

Win32/Spyeye is one of the latest offensive developments released in the underground market. Similar to Zeus bot, Spyeye is part of a crimeware toolkit with the primary goal of collecting system information and users' banking log-in credentials. It creates inline hooks on APIs used to access the Internet and employs a user mode rootkit to hide its presence in the system. Spyeye shares many similar features and functionalities with Zeus bot, creating an impression that Spyeye is the likely successor of Zeus.

Spyeye adopted ' business model, offering a competitive capability for a much lower price. Old Zeus kits are still averaging around US \$4000, while Spyeye builds are available for \$US500 (although with new plugins, costs may increase to US \$2000). In addition, Spyeye includes a code module that terminates and hijacks Zeus bot when found in the target system.

Zeus bot's latest release includes additional hooked APIs as part of its stealing behavior. Spyeye, on the other hand, added a few. A complement to Spyeye's information-stealing behavior is a feature that disables the cross-site scripting protection on Internet Explorer 8 and its capability to modify other security settings.



Figure 21 - Spyeye Business Campaign

Crimeware marketers post screenshot images of Spyeye panels to display how operators control all the bots and harvest information [Figure 21]. Similar to Zeus, Spyeye has capabilities to automate the process of stealing bank and credit card information. Among the major features are:

- Form grabber—an advanced keylogging method for capturing Web form data supporting Firefox, Internet Explorer, Maxthon and Netscape
- A credit card auto-fill module
- FTP and Pop3 grabber
- Screen capture
- Zeus spy and kill feature

Furthermore, the presence of early Spyeye versions in the system is determined by a mutex name “__CLEANSWEEP__” while “__SPYNET__” for the latest ones.

Threat Intelligence

Email Spam Trend

CA Technologies' ISBU recorded global spam bot activity from May 8, 2010 to June 20, 2010, capturing 42 days to provide a snapshot of the present situation. The database contains about one million records, including duplicates. Duplicate records are a necessary feature in the database to understand the persistence of hits of the same bot's IP address against the spam traps. The most targeted IP addresses observed actively sending spam are from the National Internet Backbone, Bharti Broadband and Tele Norte Leste Participacoes S.A.

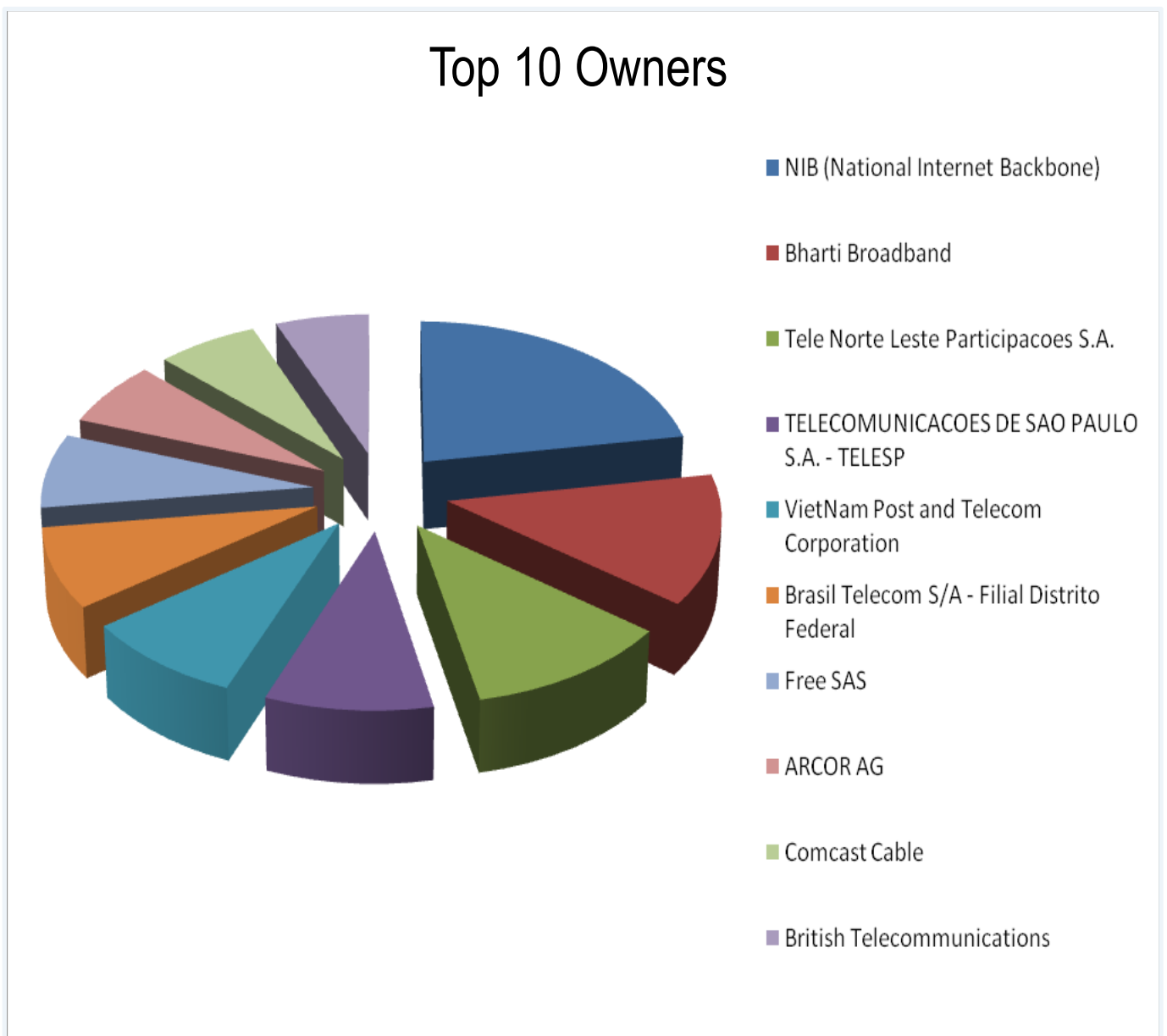


Figure 22 - Top Owners of Spam Bots' IP

Threat Intelligence

The percentage of unique IP address recorded in the period of observation determines the source of regions where the spam bot is most prevalent. The EU regions ranked as the number one source of spam, recording 31%, followed by 28% in Asia Pacific and Japan (APJ), 22% in India (IN), and 19% in the United States (US). The participation of these regions as a source of unsolicited email contributes to the growing ecosystem of the threat landscape.

Most Prevalent Regions

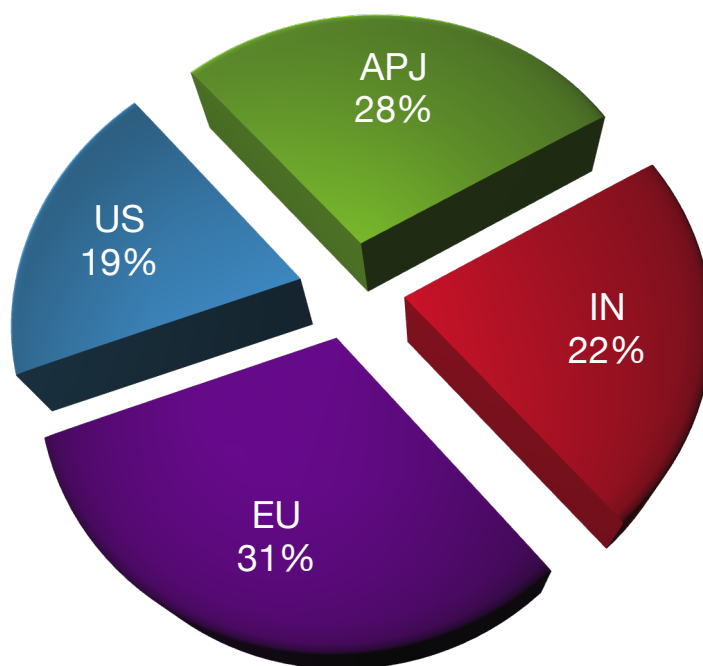


Figure 23 - Source of spam by region

Threat Intelligence

SPIM - Spamming via Instant Messaging

Spim is a form of spam that arrives through instant messaging applications such as MSN Messenger, Yahoo Messenger and Skype. This form of unsolicited messaging is very similar to email spam. Marketers employ persuasive social engineering tricks to lead users to fraudulent and malicious Web sites.

CA Technologies' ISBU observed an active proliferation of unsolicited chat messages on Skype in H1 2010. Skype users may have observed the following social engineering schemes:

Cheap Software

A marketing scheme offering cheap software. Offers may include popular retail and OEM Software [24] [25].

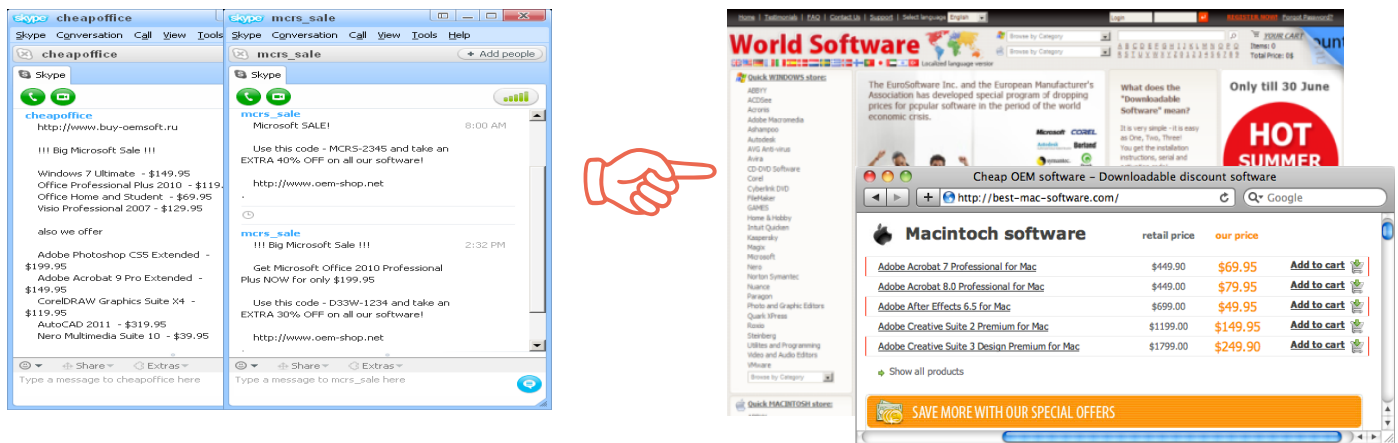


Figure 24 - Marketing Cheap Software

Impotency/Weight-Loss Pills

A marketing scheme offering male enhancement pills such as Viagra or Acai Berry that apparently allow miraculous weight loss. The promotional pitch also includes cheap or hard-to-get pills or treatments [26].

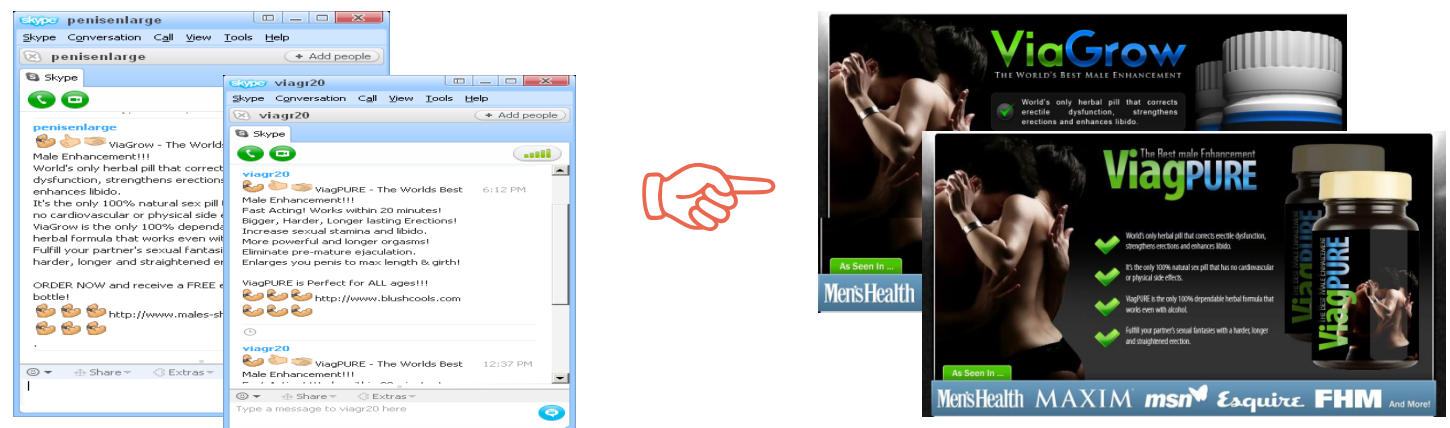


Figure 25 - Marketing Impotency Pills

Threat Intelligence

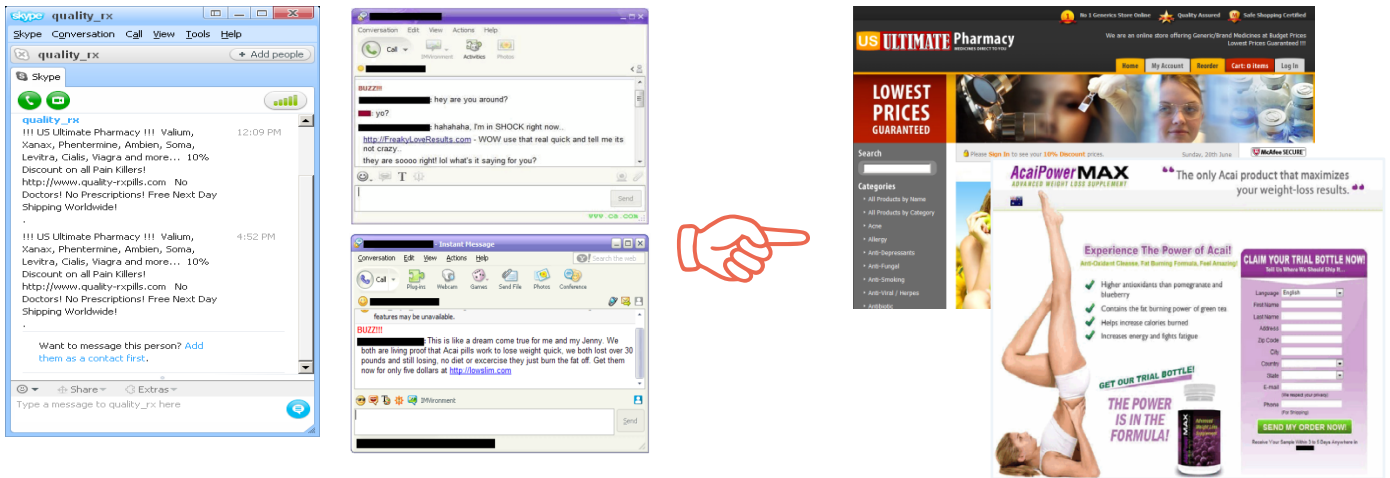


Figure 26 - Marketing Online Pharmacy

Adult Dating

A marketing scheme offering a free registration for an adult dating Web site. Notable subject lines are “date the wives,” “my cheating wife finder,” “dream lady,” “free russian lady,” “mature dating,” “discreet dating,” and “married community dating”.

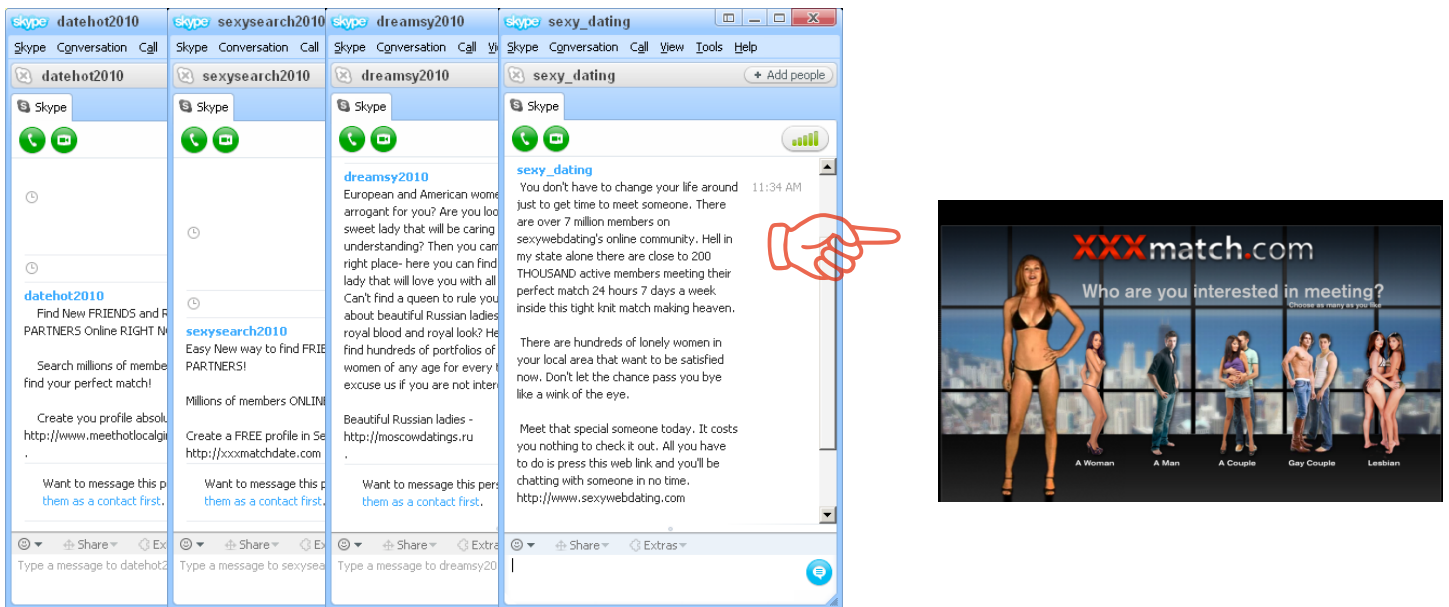


Figure 27 - Marketing Adult Dating Web Sites

Threat Intelligence

Penny stocks are stocks that usually sell for less than \$1 per share. In a pump-and-dump scheme, the promoter gains control of a large number of shares in a penny stock market. The promoters “pump” the stock by crafting exciting news, for example touting the company’s performance and new global ventures. It spreads this misleading information through various online distribution avenues (e.g., stock review Web sites, blogs and forums). A successful online promotion and marketing campaign will attract investors, creating a high demand for shares. The promoters “dump” their large number of shares and gain a large profit, leaving investors with a negative return.

We found promoters of pump-and-dump schemes to be very active through Skype instant messaging in H1 2010.

This marketing scheme offers the fastest way to get a college degree or diploma. This “Diploma Mill” is an organization that awards academic degrees and diplomas with substandard or non-academic study, and without recognition by official educational accrediting bodies.



The figure shows two screenshots of stock alert notifications. The first screenshot, from 'stockalert' dated 20/03/10 5:36 PM, features a 'Stock Alert!' with two yellow stars. It lists the symbol 'WTKN.ob', current price '.10', short term '.32+', long term '75+', and a 'Very Strong' rating. Below this, it says 'Take a close look at WTKN (OTCBB) it is a great small cap play trading at .15 cents.' and 'Dont wait to do your research on WTKN. When this stock takes off its moves can be explosive. WTKN is poised to make some savvy traders and investors very happy starting Monday of this week. Learn more at: <http://thebulletintrackers.com>'. The second screenshot, from 'imai_2010' dated 9/05/10 4:01 PM, shows a news item from <http://bulletin-trackers.com> with a title 'IMAI is the next Smoking Gun' and a 'Very Strong' rating. It lists the market symbol 'IMAI', current price '.09', short term '.30+', long term '.92+', and a 'Very Strong' rating. The text below reads: 'The current leader of the pack, International Merchant Advisors, Inc. (PINK SHEETS: IMAI), through the company's wholly owned subsidiary, Organic Science, Inc. project revenues over the next twenty four months to exceed \$10,000,000.00 from facilities IMAI either already manages today or the company has active plans in place for opening and operation.'

Figure 28 - Marketing Penny Stocks

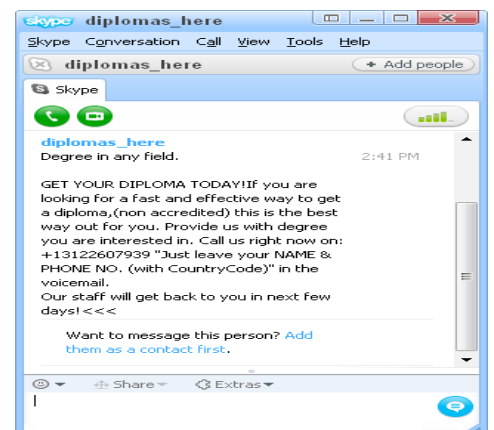


Figure 29 - Marketing Diploma Mill

Threat Intelligence

Work Opportunity

This marketing scheme offers ways to increase income and generate a lot of money quickly.

sarah_wil01 19/03/10 10:32 PM

I quit my day job last month and started working from for Google. I made \$3,872 this month so far and I have never been so happy. Im recommending this to all my friends and family.
<http://usnews3.com/homefinance> - Thats the link to the Google Jobs Blog. Its so easy, check it out and thank me later!

homebus10 9/05/10 8:17 AM

Secret to Wealth Success!
The World #1 Home-Based Business: 50% monthly, 300% in a half year + Guaranteed Affiliate Earnings!
Earn a Substantial Income While Asleep!

<http://financialindependencetoday.com/>

Figure 30 - Marketing Work Opportunity

More concerning than the annoyance factor is that spim often leads to phishing sites that steal users' sensitive information and credit card details.

Most spims are generated by bots using fake IM accounts, although compromised IM accounts may be used as IM spam bots. We have also observed that some families of threats are sending out unsolicited chat messages as payloads.

Win32/Skipe is a known Trojan capable of sending out unsolicited chat messages to all online Skype contacts. New variants of this threat were also actively observed this H1 2010.

Threat Intelligence

Ransomware

At the start of the year, CA Technologies' ISBU observed a recycled version of a ransomware discovered last year called Win32/FileFixPro2009. The repackaged version was spotted in the wild and is detected as Win32/DataDoctor2010 [27]. The names have changed, but the GUI template used was the same, and the encryption logic was slightly modified.

However, the most prevalent ransomware families observed in H1 2010 are Win32/RansomPinkBlocker [28] and Win32/RansomStv, whose main feature is to block Web browsing and display pornographic content. Once installed, this threat lures the user by playing a pornographic video for a limited time before locking down the Web browser or the system.

Win32/Hexzone is another ransomware family discovered since 2008 but still in the wild. This threat installs a BHO and injects script pages that display ransomware messages [Figure 32] on every Web site visited by the user.

Win32/DotTorrent.A is the latest ransomware discovery in H1 2010, and it is noteworthy. It uses FakeAV's scare tactics by displaying fake warnings and deceiving popups to persuade users to pay. Upon a system restart, this ransomware takes full control by completely blocking the desktop. Furthermore, Win32/DotTorrent.A includes language support for ten languages [29].



Figure 31 - Win32/DataDoctor2010

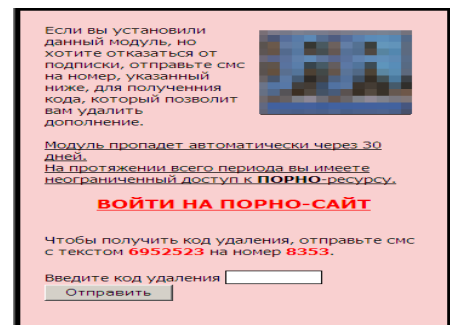


Figure 32 - Win32/Hexzone



Figure 33 - Win32/DotTorrent

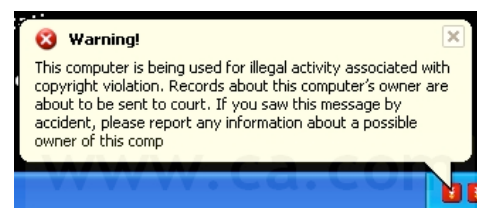


Figure 34 - Win32/DotTorrent Scare Warning

Threat Intelligence

Notable Backdoors

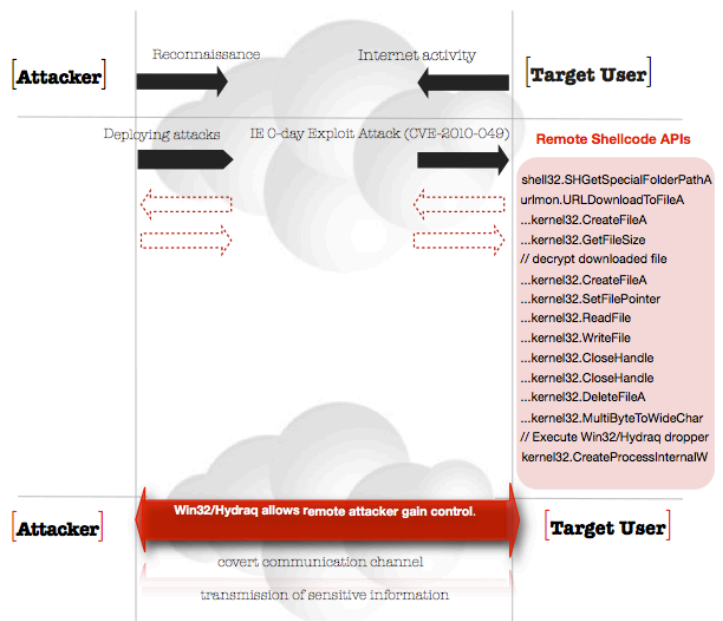
In the first half of 2010, backdoors ranked second next to Infostealer Trojans, capturing 15% of the overall Trojan threat landscape. A backdoor is a piece of malicious code that enables remote attackers to gain unauthorized access and full control of the affected system. The relationship of the victim (hosting the server component) and the remote attacker (hosting the client component) is more specific and targeted compared with botnet command and control attacks. Backdoors are often installed as payloads after a successful exploit attack. The availability of exploit kits in the underground market increases the demand of remote administration tools (RAT) and other modular developments, such as encryption and packaging. Thus, backdoors are prevalent and considered common threats similar to infostealers and downloaders. The latest notable high profile backdoor developments that employ techniques designed to spy and obtain secret information for military, political, economic and business advantage are an emerging trend.

Win32/Hydraq

Description: Hydraq is a family of threats involved in a targeted attack against large and high-profile corporate networks. It is referred to as Operation Aurora, Google Hack Attack and Microsoft Internet Explorer 0day (CVE-2010-0249 and MS10-002) [30].

Hydraq's advanced persistent threat features include:

- Probing
- Exfiltration of sensitive information
- Surveillance
- Covert communication
- Covering tracks
- Add on or expandable features



Vector: Internet Explorer 6, 7 and 8

Discovery: January 14, 2010 | Microsoft Patch Release: January 21, 2010

Zero-day Attack Exposure: 7 days

Threat Intelligence

Win32/Wisp

Description: Backdoor Wisp is another threat that was distributed in websites exploiting the 0day vulnerability in Internet Explorer, referred to as Microsoft Security Advisory 98137 (MS10-018). This threat is capable of sending information and receiving commands to and from its command and control [31].

Vector: Internet Explorer version 6 and 7 0day

Discovery: March 09, 2010 | Microsoft Patch Release: March 30, 2010

Zero-day Attack Exposure: 21 days



Win32/Arugizer

Description: This backdoor was brought to our attention by the United States Computer Emergency Readiness Team (US-CERT). The Energizer DUO USB battery charger installer creates Arucer.dll in the %system% folder and executes it on system start. This dll file contains the malicious code that is capable of receiving and executing commands from a remote connection. After the reported incident, the Energizer website published a press release that the sale of this product had been discontinued, and the download Web site of the compromised installer had been taken offline [32].

The backdoor is capable of executing the following commands:

- Retrieve and send information about the logical drives
- Retrieve and send filename and file contents of specified directory
- Set the value of the registry entry

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\svchost

- Delete a specified file
- Download and execute a file in the infected system

Threat Intelligence

Notable File Infection

Alureon and Pushdo/Cutwail Infecting System Drivers

Win32/Alureon aka *Tidserv/TDSS/DNSChanger* is a family of multiple component Trojans that functions and provides services within the crimeware ecosystem. The opportunity to distribute this threat and capture value through pay-per schemes fuels its continuous offensive developments. One of its main functionalities is to download and execute arbitrary files. The payload may include hijacking the Web browser to display fake Web pages, capture user's search engine queries, hijack user's search engine results, steal data and confidential information (including banking details), perpetrate click frauds, modify DNS settings to continuously monitor and redirect Internet traffic, and install rogue security software often associated with Win32/FakeAV variants. However, the most exceptional feature of Win32/Alureon is its advanced rootkit/stealth technique, which enables it to evade detection and remove threats from affected systems.

Win32/Alureon's latest offensive feature, as observed in H1 2010, is the ability to infect known system drivers such as:

- %system%\driver\atapi.sys
- %system%\driver\iastor.sys
- %system%\driver\iastorv.sys
- %system%\driver\idechndr.sys
- %system%\driver\ndis.sys
- %system%\driver\nvata.sys
- %system%\driver\nvatabus.sys
- %system%\driver\nvgts.sys
- %system%\driver\nvstor.sys
- %system%\driver\nvstor32.sys
- %system%\driver\sisraid.sys
- %system%\driver\vm SCSI.sys

Once the infected system driver is loaded, Win32/Alureon installs other components like the rootkit to hide files and disk sectors to evade detection and removal. This allows it to perform malicious routines continuously. Some variants of Win32/Alureon infection cause corruption on certain system driver files, making the system crash or become unusable.

Earlier this year, Win32/Alureon gained media attention with the Blue Screen of Death (BSOD) error after users applied the Microsoft patches MS10-015 and MS10-012 on infected systems.

Threat Intelligence

The **Pushdo/Cutwail** is also one of the more notable threats this year. Win32/Cutwail is a spambot component installed by the *Pushdo* botnet. Win32/Pushdo is the bot loader responsible for multiple installations of threats, including includes spambots and rootkits. Similar to latest offensive feature of Win32/Alureon, Cutwail variants were also observed infecting system drivers primarily to load the rootkit component, designed to evade detection and prolong the monetization of infection.

Examples of targeted system drivers include the following:

- %system%\driver\ndis.sys
- %system%\driver\cdrom.sys
- %system%\driver\atapi.sys
- %system%\driver\agp440.sys

Malware keeps patching up!

CA Technologies' ISBU observed prevalent malware families, specifically game password stealing Trojans such as Win32/Frethog, Win32/Wowpa, Win32/Zuten, and Win32/Gamepass added new offensive features.

This family of Trojans steals login credentials and in-game information related to various Massively Multi-player Online Role Playing Games (MMORPG) by logging keystrokes, monitoring window names and online game Web sites.

Aside from their regular malicious routine, new features have been added to these variants to execute or load malicious component files, generally a specific DLL file on the infected system. To do this, the malware patches or inserts a tiny piece of malicious code to the target file.

Some of these detected patched files include the following:

Win32/Imm32Patched

These are patched DLL files "*imm32.dll*" or "*comres.dll*" located in the Windows System folder. A patched DLL has a newly created section named ".ss32". Once a patched DLL loads, it installs the file that is listed in a configuration file "*wsconfig.db*," which is the malicious DLL component file of the main malware.

Example contents of *wsconfig.db*:

```
[0]
o=C:\WINDOWS\system32\kb141012387.dll
```


Threat Intelligence

Win32/Patchload, Win32/Sound

These are detection for patched DLL files that load a malicious DLL component of a main executable malware. The DLL file that it loads may have a *.TMP*, *.IME*, *.DRV* or *.LOG* file extension. Some of the specific DLL files targeted by the malware include the following, which are usually located in the Windows System folder:

- ddraw.dll
- dsound.dll
- d3d8.dll
- d3d9.dll
- olepro32.dll
- dbghelp.dll
- asycfilt.dll
- perfctrs.dll
- msimg32.dll

These malware patchers patch specific DLL files because most of these DLLs are related or dependent on applications such as games that attackers are monitoring. The infection also serves as their auto execution of malicious code.

Win32/Sfcpatched

This is a detection for Windows system file “sfcfiles.dll” commonly patched by *Win32/FakeAlert*, *Win32/Hodprot* or *Win32/VilseI* variants. The DLL file ‘sfcfiles.dll’ is part of the *System File Checker* (SFC) application used to verify and restore damaged/missing/corrupted system files.

Thus, once the “sfcfiles.dll” file is patched, the system can no longer protect system files, or the Windows File Protection will be disabled. As a result, the malware may perform its malicious routine successfully.

Win32/SillyDI.SBW

These are EXE files that have been modified or patched by inserting a piece of malicious code in the available or free space found in the first section of the executable. Once a patched executable is executed, it downloads and executes a popular variant of Win32/Zbot malware.

Threat Intelligence

MAC OS X Threats

Unwanted email and chat messages, phishing URLs, online fraud, cyberbullies, browser hijacking, and viral attacks in popular social media platforms are the types of threats that are not necessarily platform-specific. In the first half of 2010, the following notable Mac security threats were discussed:

January: Traffic Redirection Attack

In January 2010, Mac users observed unusual redirection on links shared through social networking sites, search engine results [33], and compromised legitimate Web sites. The redirection attacks do not serve malicious code; instead, the traffic is redirected to promote fraudulent Web products and services (e.g., pirated software, cheap movie downloads and dating sites), which may lead users to online identity theft and unwanted credit card charges.

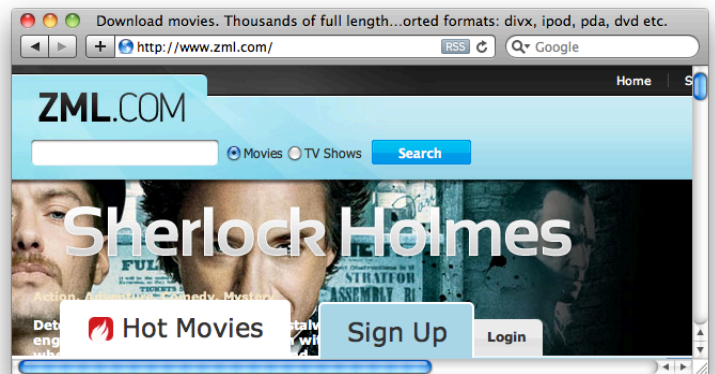


Figure 35 - Traffic Redirection Attack

February: Mac OS X Ransomware 'Blocker'

The traffic redirection attack raised suspicion and questioned the real intentions behind a fraudulent message. An active online discussion immediately emerged and soon disclosed further details. Mac users' traffic will be redirected to a new malware that is designed to lock the desktop screen, and the victim will be instructed to send money for disinfection. The described zero-day malware in Macintosh is a ransomware and the distributed proof-of-concept version is called "Blocker" [34].



Figure 36 - Mac OS X Ransomware 'Blocker'

March: CVE-2010-1120

An unchecked index issue exists in Apple Type Services' handling of embedded fonts. Viewing or downloading a document containing a maliciously crafted embedded font may lead to arbitrary code execution [35].

Charlie Miller demonstrated a Safari drive-by-download attack using this vulnerability during this year's CanSecWest Pwn2own contest.



Threat Intelligence

April: HellRaiser 4.2

DCHKG, an Underground Mac Programming Team, released “HellRaiser 4.2” in October 2009. Although client-server programs are known useful tools for managing remote administrator tasks, this type of program is also classified as a security threat since it can be used for malicious purposes.

The HellRaiser 4.2 server component was discovered in the wild disguised as an iPhoto installer. The server may include auto-duplication features to enable persistent installation and auto launch entry.

It is important to note that the server applications do not require root privileges to install. Just a decent trick for a simple click, then it is ready to receive remote commands [36].

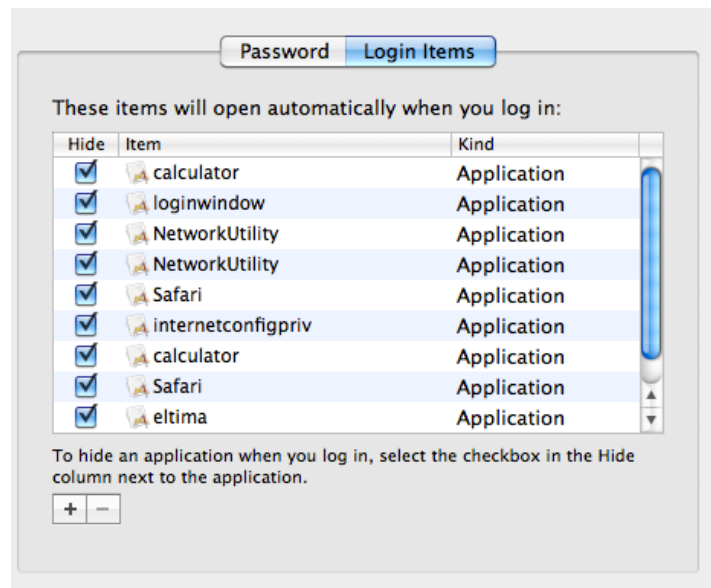


Figure 37 - HellRaiser 4.2 Server Auto-Duplication Feature

May: Safari Carpet Bomb Vulnerability

Apple Safari carpet-bombing is a vulnerability that allows a remote attacker to silently download arbitrary files in a users' default download directory (~/.Download) [37] via a malicious Web site. The author recently revisited the vulnerability and confirmed that Safari Browser on OSX remains unpatched.

June: “PremierOpinion” Mac OS X Spyware

PremierOpinion spyware is a known pest on the Windows platform since 2008. Although the software may perform all sorts of malicious behavior in the background, this pest is widely classified as spyware because of the informed consent.

PremierOpinion spyware was initially discovered bundled in several application and screen saver installer packages from MacUpdate, Version-Tracker and Softpedia [38].

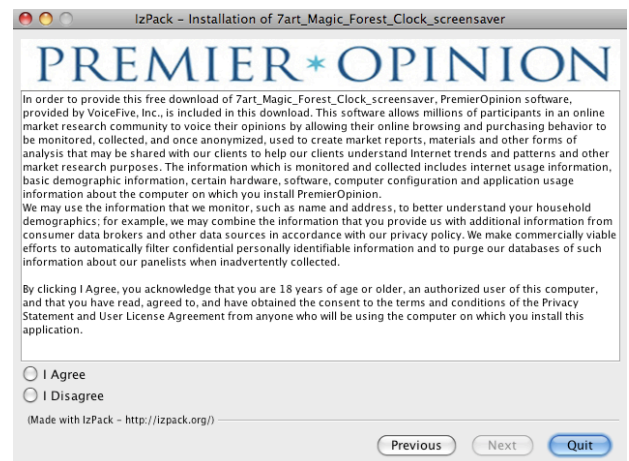


Figure 38 - PremierOpinion Mac OS X Spyware

CA Technologies identifies this threat as OSX/OpinionSpy.

Safe Computing Advise

With the proliferation of Web-based attacks and the increasing methods used to deploy social engineering tricks, it is more important than ever to be cautious to ensure safety online. Security is a process. To be sure, you must be aware, apply the right technology, understand your daily computing activity and identify the amount of information or data you want to secure.

Let the Technology Work for You

Here are some easy steps to ensure that your CA Technologies security product provides optimal protection for you:

1. **Your security scanner must always be turned on and up-to-date with the latest signatures.** Real-time scanning protects you from possible information you may get from compromised Web sites, network shares, email and flash drives.
2. Turn on your firewall. Your firewall provides a different layer of security that guards you from network attacks and blocks unauthorized access to your machine. A firewall with real-time malware behavior intrusion detection could prevent or lessen the impact of malware infection.
3. Increase your browser security settings. You can refer to the CERT Web browser security tips at http://cert.org/tech_tips/securing_browser/.

Be Security-Aware

1. Do NOT open email from people you don't know. Think twice and verify before clicking a URL or opening an attachment. Don't be click happy! All it takes is a moment of inattention.
2. Implement a strong password that you can remember. Refer to these Microsoft tips for creating a strong password: <http://microsoft.com/protect/yourself/password/create.msp>.
3. When conducting online banking or financial transactions, make sure your browser connection is secure.
4. Encrypt online communication and confidential data.
5. Back up your important data. Keep a copy of all your files and store them separately.
6. Be cautious about instant messaging. Avoid chatting with people you don't know, especially if they ask for personal information such as photos or want you to do something for them.

7. Protect your identity while enjoying online social networking activities. Be wary of clicking links or suspicious profiles. Double-check the integrity of the connection or friends' request before adding anyone to your network. Be aware when installing extras such as third party applications; they may lead to malware infection, or attackers could use them to steal your identity.
8. Avoid piracy by downloading from secure sources.
9. Avoid threats that use social engineering techniques by checking user feedback about a Web site before visiting it. Read feedback about an application before installing it.
10. If you are using Adobe PDF Reader, prevent your default browser from automatically opening PDF documents. Refer to our CA Technologies' Security Advisor Research blog entry at <http://community.ca.com/blogs/securityadvisor/archive/2009/02/24/attackers-love-zero-day.aspx>.
11. Check for and install security updates regularly.
12. Be careful with search engine results. Read them carefully and check to ensure that the content relates to your subject before clicking the Web site link.

Make Internet computing safe —
report suspicious files and Web sites to virus@ca.com.

References

[1] Pop-Up Security Warnings Pose Threats

<http://www.fbi.gov/pressrel/pressrel09/popup121109.htm>

[2] The Nocebo* Effect on the Web: An Analysis of Fake Anti-Virus Distribution

http://www.usenix.org/event/leet10/tech/full_papers/Rajab.pdf

[3] More on Rogue Security Software's Multi-Language Support

<http://community.ca.com/blogs/securityadvisor/archive/2010/02/09/more-on-rogue-security-software-s-multi-language-support.aspx>

[4] GreenAV: rogue security software and social engineering walk together

<http://community.ca.com/blogs/securityadvisor/archive/2009/09/03/greenav-rogue-security-software-and-social-engineering-walk-together.aspx>

[5] Black Hat SEO Demystified: Abusing Google Trends to Serve Malware

<http://community.ca.com/blogs/securityadvisor/archive/2010/01/18/black-hat-seo-campaign-using-latest-trend-keywords-demystified.aspx>

[6] Consumer Sentinel Network Data Book for January - December 2009

<http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf>

[7] NIST Definition of Cloud Computing

<http://csrc.nist.gov/groups/SNS/cloud-computing/>

[8] Social Networks/Blogs Now Account for One in Every Four and a Half Minutes Online

http://blog.nielsen.com/nielsenwire/online_mobile/social-media-accounts-for-22-percent-of-time-online/

[9] Misuse of Google Groups for Malicious Spam Campaign

<http://community.ca.com/blogs/securityadvisor/archive/2009/09/17/bot-using-and-abusing-google-groups.aspx>

[10] Bot Using and Abusing Google Groups

<http://community.ca.com/blogs/securityadvisor/archive/2010/05/10/misuse-of-google-groups-for-malicious-spam-campaign.aspx>

[11] Zeus "in-the-cloud"

<http://community.ca.com/blogs/securityadvisor/archive/2009/12/09/zeus-in-the-cloud.aspx>

[12] Twitter and YouTube Spam Campaign in Disguise

<http://community.ca.com/blogs/securityadvisor/archive/2010/06/10/twitter-and-youtube-spam-campaign-in-disguise.aspx>

[13] Stay safe with your Twitter account!

<http://community.ca.com/blogs/securityadvisor/archive/2010/04/30/stay-safe-with-your-twitter-account.aspx>

[14] Reason #4132 for Changing Your Password 5

<http://status.twitter.com/post/367671822/reason-4132-for-changing-your-password>

[15] Twitter Password Spam Campaign

<http://community.ca.com/blogs/securityadvisor/archive/2010/06/08/twitter-password-spam-campaign.aspx>

[16] Bredolab, Cutwail and Zbot Christmas Function

<http://community.ca.com/blogs/securityadvisor/archive/2009/12/16/bredolab-cutwail-and-zbot-christmas-function.aspx>

[17] Frusspam - Personal Message On Facebook

<http://community.ca.com/blogs/securityadvisor/archive/2010/05/11/frusspam-personal-message-from-facebook.aspx>

[18] Facebook: "Who is checking my profile" application deceitful and privacy invasion

<http://community.ca.com/blogs/securityadvisor/archive/2010/03/15/facebook-quot-who-is-checking-my-profile-quot-application-deceitful-and-privacy-invasion.aspx>

[19] Facebook Scam and the Hidden Iron Man 2 Scene!

<http://community.ca.com/blogs/securityadvisor/archive/2010/06/07/facebook-scam-and-the-hidden-iron-man-2-scene.aspx>

[20] Warning: Facebook Antivirus Will Virally Spam Your Friends

<http://thefacebookinsider.com/2010/03/warning-facebook-antivirus-will-virally-spam-%20your-friends/>

[21] Bots for Sale!

<http://community.ca.com/blogs/securityadvisor/archive/2010/06/07/bots-for-sale.aspx>

[22] Zeus Version 3 – Target Spain, Germany, UK, and USA Banks

<http://community.ca.com/blogs/securityadvisor/archive/2010/07/12/zeus-version-3-target-spain-germany-uk-and-usa-banks.aspx>

[23] Zeus Crimeware using Amazon EC2 as command and control server

<http://www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110>

[24] Buy our software and ... join the illegal market!

<http://community.ca.com/blogs/securityadvisor/archive/2010/02/15/buy-our-software-and-join-the-illegal-market.aspx>

[25] Best-mac-software.com

<http://ithreats.net/2010/01/13/best-mac-software-com/>

[26] More Spim About Acai Pills

<http://community.ca.com/blogs/securityadvisor/archive/2010/01/22/more-spim-about-acai-pills.aspx>

[27] Ransomware Taking Legal Action on Copyright Violation

<http://community.ca.com/blogs/securityadvisor/archive/2010/04/13/ransomware-taking-legal-action-on-copyright-violation.aspx>

[28] Ransomware: The Pink Porno Browser Blocker

<http://community.ca.com/blogs/securityadvisor/archive/2010/03/22/ransomware-the-pink-porno-browser-blocker.aspx>

[29] Ransomware Taking Legal Action on Copyright Violation

<http://community.ca.com/blogs/securityadvisor/archive/2010/04/13/ransomware-taking-legal-action-on-copyright-violation.aspx>

[30] In-depth Analysis of Hydraq

http://www.ca.com/files/securityadvisornews/in-depth_analysis_of_hydraq_final_231538.pdf

[31] Command and Conquer with Backdoor Wisp

<http://community.ca.com/blogs/securityadvisor/archive/2010/03/12/command-and-conquer-with-backdoor-wisp.aspx>

[32] Win32/Arugizer - Backdoor in Energizer DUO Battery Charger Software

<http://community.ca.com/blogs/securityadvisor/archive/2010/03/09/win32-arugizer-backdoor-in-energizer-duo-battery-charger-software.aspx>

[33] Taking advantage of Apple iPad “Hot” Trending Topics

<http://community.ca.com/blogs/securityadvisor/archive/2010/01/28/taking-advantage-of-apple-ipad-hot-trending-topics.aspx>

[34] Mac OS X Ransomware

<http://ithreats.net/2010/03/16/mac-os-x-ransomware/>

[35] Security Update 2010-003

<http://support.apple.com/kb/HT4131>

[36] Rat for Mac

<http://ithreats.net/2010/04/20/rat-for-mac/>

[37] Safari users still vulnerable to “carpet-bombing” attack

<http://ithreats.net/2010/05/26/safari-users-still-vulnerable-to-carpet-bombing-attack/>

[38] “PremierOpinion” Spyware Now in Mac OS X

<http://ithreats.net/2010/06/02/premieropinion-spyware-now-in-mac-os-x/>