

Phishing Activity Trends Report

1st Quarter
2010



Committed to Wiping Out
Internet Scams and Fraud

January – March 2010

Phishing Report Scope

The quarterly *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at <http://www.antiphishing.org> and by email submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation and propagation of crimeware drawing from the research of our member companies. In the last half of this report you will find tabulations of crimeware statistics and related analyses and results of a TLD phishing abuse survey.

Phishing Defined

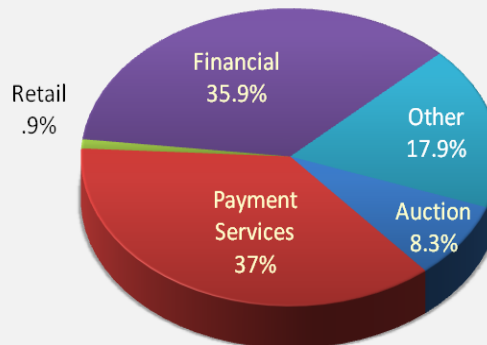
Phishing is a criminal mechanism employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords. Technical-subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords - and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

Table of Contents

Statistical Highlights for 1st Quarter, 2010	3
Phishing Email Reports and Phishing Site Trends	4
Brand-Domain Pairs Measurement	5
Most Used Ports Hosting Phishing Data	
Collection Servers in 1st Quarter 2010	6
Brands & Legitimate Entities Hijacked by	
Email Phishing Attacks	6
Most Targeted Industry Sectors	7
Countries Hosting Phishing Sites	7
Measurement of Detected Crimeware	8
Rogue Anti-Malware Programs	9
Phishing-based Trojans & Downloader's Host	
Countries (by IP address)	9
Desktop Crimeware Infections	10
Consumer Phishing Profile	10
Avalanche Attacks by Top-Level Domain 2H09	11
APWG Phishing Trends Report Contributors	12

eCrime Gangs Focus on Classifieds, Social Networking and Gaming Websites

Most Targeted Industry Sectors 1st Quarter '10



The proportion of the category "other" – social networking, online classifieds and online gaming – industries rose more than 37 percent from Q4, 2009 to Q1 2010. [See page 7]

1st Quarter '10 Phishing Activity Trends Summary

- The disappearance of a rogueware variant accounted for a 37 percent decrease in total samples detected in Q1 2010 compared to Q4 2009 [p. 9]
- Unique phishing reports reached a Q1 2010 high of 30,577 in March, down 25 percent from the record in August 2009 of 40,621 reports [p. 4]
- The number of total unique phishing websites detected at Q1's end, in March, was 29,879, off 47 percent from high of 56,362 in August 2009 [p. 4]
- The number of brand-domain pairs detected at end of Q1 was 10,752, down 56 percent from the record of 24,438 in August 2009 [p. 5]
- The number of phished brands reached a high of 298 in March, a decrease of 16 percent from the all-time high of 356 reached in October, 2009 [p.6]
- The United States continued its position as the top country hosting phishing sites during the first quarter of 2010 [p. 7]
- The proportion of infected computers increased from more than 47 percent in the fourth quarter of 2009 to more than 53 percent in Q1 2010 [p. 10]

Methodology and Instrumented Data Sets

APWG continues to refine and develop its tracking and reporting methodology and to incorporate new data sources into our reports. APWG has re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent out to multiple users, directing them to a specific phishing web site (multiple campaigns may point to the same web site). APWG counts unique phishing report emails as those in a given month with the same subject line in the email.

APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites. APWG additionally tracks crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample) as well as unique sites that are distributing crimeware (typically via browser drive-by exploits). The *APWG Phishing Activity Trends Report's* also includes statistics on rogue anti-virus software, desktop infection rates and relative rates of abuse in phishing attacks defined by the top-level domain used in phishing campaigns. With this edition, APWG includes statistics on phishing attacks' abuse of Top Level Domains.

Statistical Highlights for 1st Quarter, 2010

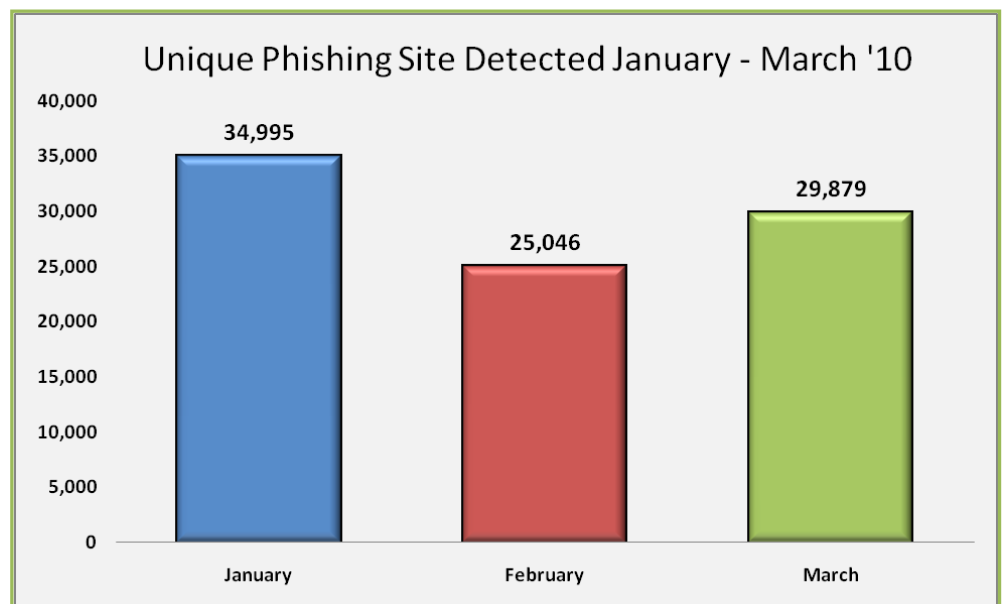
	January	February	March
Number of unique phishing email reports received by APWG from consumers	29,499	26,909	30,577
Number of unique phishing web sites detected	34,995	25,046	29,879
Number of brands hijacked by phishing campaigns	265	258	298
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	37.89%	52.70%	36.48%
No hostname; just IP address	2.85%	4.82%	3.46%
Percentage of sites not using port 80	0.14%	0.06%	0.18%

Phishing Email Reports and Phishing Site Trends – 1st Quarter 2010



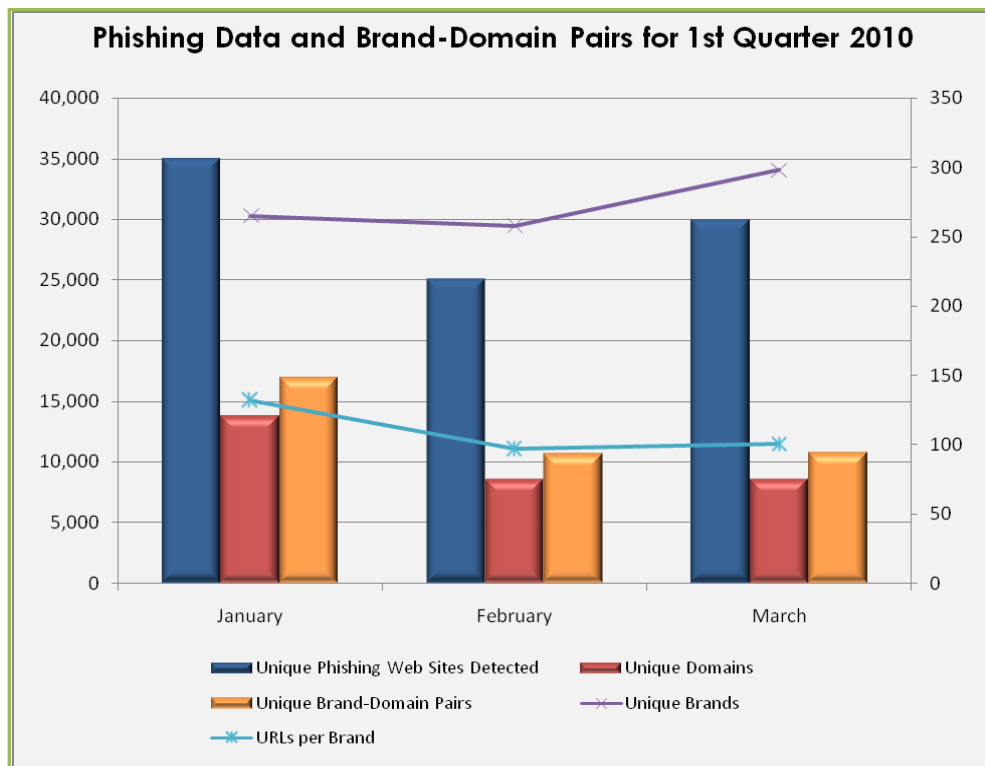
The number of unique phishing reports submitted to APWG in the first quarter 2010 reflected a gradual decrease that began after hitting an all-time high in Q3 2009. The Q1 2010 high of 30,577 in March was down nearly 25 percent from the all-time record in August 2009 of 40,621 reports.

The number of unique phishing websites detected by APWG during Q1 2010, fluctuated broadly from month to month within the quarter. The quarter ended with 29,879 reported in March, off by nearly 47 percent from the all-time high of 56,362 recorded in August 2009.



Brand-Domain Pairs Measurement – 1st Quarter 2010

The following chart combines statistics based on brands phished, unique domains, unique domain/brand pairs, and unique URLs. Brand/domain pairs count the unique instances of a domain being used to target a specific brand. *Example:* if several URLs are targeting a brand – but are hosted on the same domain – this brand/domain pair would be counted as one instead of several. The number of unique brand-domain pairs dropped during the Q1 2010. The 16,922 brand-domain pairs in January was followed by March with just 10,752, down some 56 percent from the record of 24,438 recorded in August, 2009.



“The total number of phishing URLs declined from the previous quarter due to a large drop in fast flux activity,” said Ihab Shraim, MarkMonitor’s chief security officer and vice president, network and system engineering, and *Trends Report* contributing analyst. “However, remaining ‘classic’ phish activity is even higher than levels seen before the advent of fast-flux attacks. This suggests that while fast-flux phishers made a large, temporary impact on phishing levels, traditional phishing techniques continued to evolve and grow.”

Forensic utility of this metric: If the number of unique URLs is greater than the number of brand/domain pairs, it indicates many URLs are being hosted on the same domain to target the same brand. Knowing how many URLs occur with each domain indicates the approximate number of attacking domains a brand-holding victim needs to locate and neutralize. Since Phishing-prevention technologies (like browser and email blocking) require the full URL, it is useful to understand the general number of unique URLs that occur per domain.

	January	February	March
Number of Unique Phishing Web Sites Detected	34,995	25,046	29,897
Unique Domains	13,762	8,509	8,525
Unique Brand-Domain Pairs	16,922	10,631	10,752
Unique Brands	265	258	298
URLs Per Brand	132.06	97.07	100.33

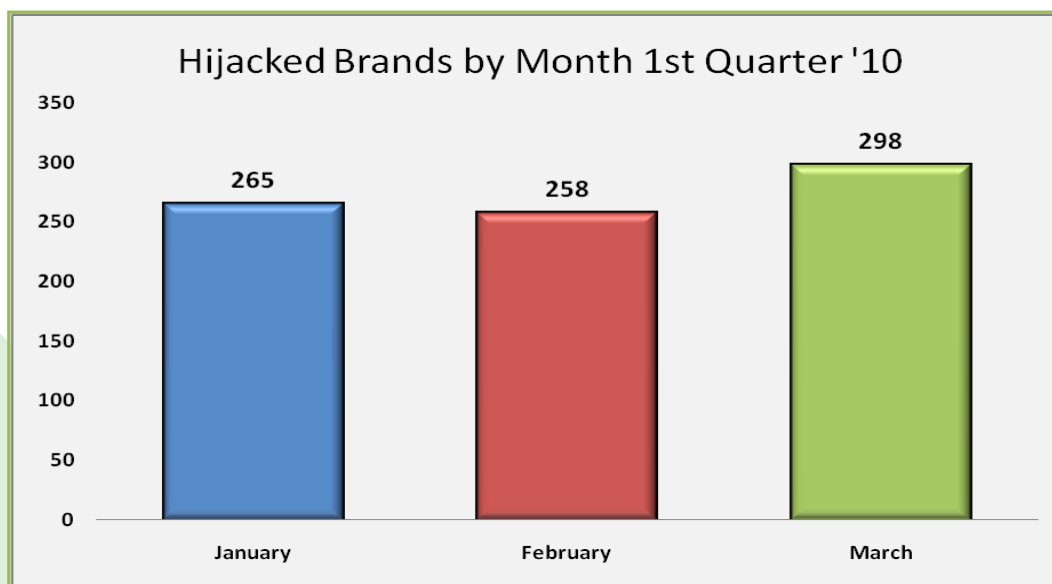
Most Used Ports Hosting Phishing Data Collection Servers – 1st Quarter 2010

The first quarter of 2010 saw a continuation of HTTP port 80 being the most popular port used of all phishing sites reported, a trend that has been consistent since APWG began tracking and reporting in 2003.

January		February		March	
Port 80	99.97%	Port 80	99.95%	Port 80	99.85%
Port 443	.01%	Port 21	.025%	Port 443	.07%
Port 8080	.005%	Port 443	.01%	Port 21	.04%
Port 88	.005%	Port 8080	.005%	Port 78	.01%
Port 6660	.005%	Port 32000	.005%	Port 280	.01%
Port 84	.005%	Port 8088	.005%	Port 29	.01%
				Port 9980	.005%
				Port 8081	.005%

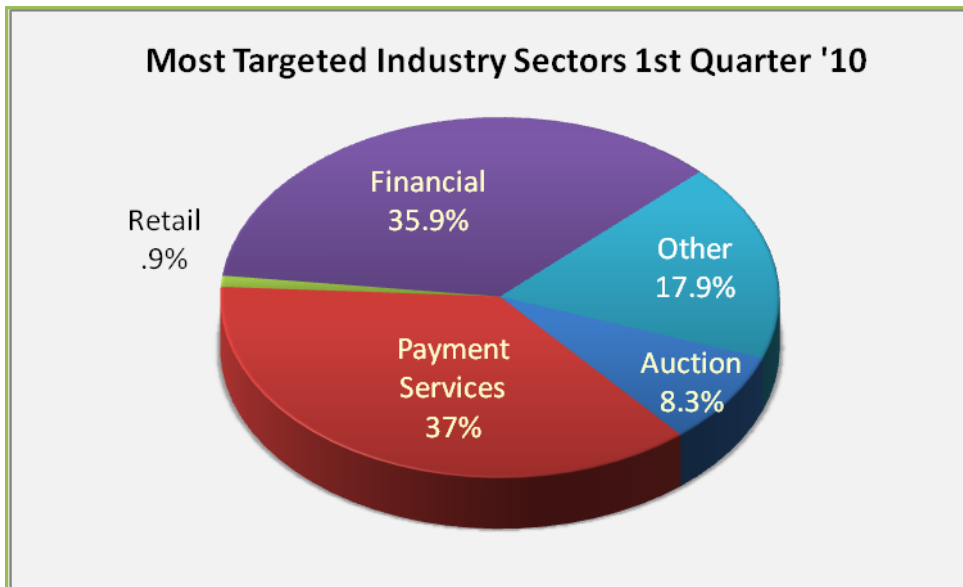
Brands and Legitimate Entities Hijacked by Email Phishing Attacks – 1st Quarter 2010

The first quarter of 2010 saw a high of 298 in March for the three month period, a decrease of 16 percent from the all-time high of 356 reached in October, 2009. As the numbers of brands has dropped, phishers still continue to expand their targets in other ways, such as focusing on executives and line employees with corporate treasury authority.



Most Targeted Industry Sectors – 1st Quarter 2010

Payment Services returned to being the most targeted industry sector after Financial Services held top position during H2 2009. However, the category of “Other” rose from 13 percent to nearly 18 percent from Q4 2009 to Q1 2010, an increase of nearly 38 percent. Ihab Shraim, MarkMonitor’s chief security officer and vice president, network and system engineering, and *Trends Report* contributing analyst said, “The increase in the ‘Other’ category is attributed to the sharp increase in attacks against the online classifieds, social networking and gaming industries.”



Countries Hosting Phishing Sites – 1st Quarter 2010

The United States continued its position as the top country hosting phishing sites during the first quarter of 2010 with China maintaining a top three listing during the three month period.

January		February		March	
USA	61.62%	USA	73.58%	USA	67.34%
China	4.35%	China	2.76%	Canada	3.63%
Germany	3.59%	UK	2.30%	China	3.10%
Rep. Korea	3.47%	Rep. Korea	2.13%	UK	2.80%
Canada	2.94%	Italy	1.83%	Hong Kong	2.56%
UK	2.61%	Germany	1.83%	Germany	2.47%
Hong Kong	2.58%	France	1.77%	Rep. Korea	2.38%
Russia	2.06%	Canada	1.67%	Russia	1.61%
France	1.80%	Mexico	1.38%	France	1.47%
Netherlands	1.52%	Russia	1.37%	Italy	1.33%

Crimeware Taxonomy and Samples According to Classification

The APWG's Crimeware statistics categorize crimeware attacks as follows, though the taxonomy will grow as variations in attack code are spawned

Definition: Crimeware code which is designed with the intent of collecting information on the end-user in order to steal those users' credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations, most importantly financial institutions, online retailers, and e-commerce merchants) in order to target specific information. The most common types of information are: access to financial-based websites, ecommerce sites, and web-based mail sites.

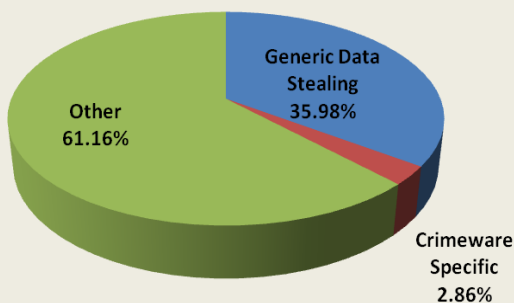
Measurement of Detected Crimeware – 1st Quarter 2010

Using data contributed from APWG member Websense, measuring proliferation of malevolent software, this metric measures proportions of three genera of malevolent code detected: *Crimeware* (data-stealing malicious code designed specifically to be used to victimize financial institutions' customers and to co-opt those institutions' identities); *Data Stealing and Generic Trojans* (code designed to send information from the infected machine, control it, and open backdoors on it); *Other* (the remainder of malicious code commonly encountered in the field such as auto-replicating worms, dialers for telephone charge-back scams, etc.)

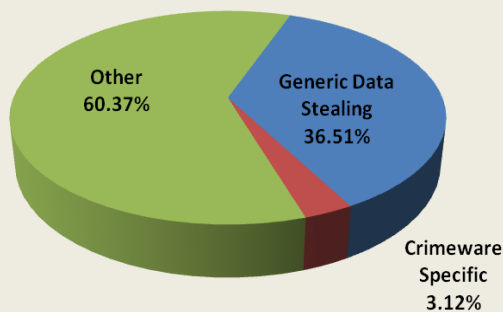
Over the quarter, the proportion of crimeware-specific malware (malicious code designed specifically to infect financial institutions' customers' PCs) remained consistent, while generic data-stealing malware grew month-to-month. Patrik Runald, Senior Manager, Security Research for Websense and a *Trends Report* contributing analyst said, "Malware that

steals information from users' computers are continuing to be a major problem as it happens in the background, without the users' knowledge. Without proper security protection in place, the user is totally unaware this is going on and the bad guys continue to profit because of it."

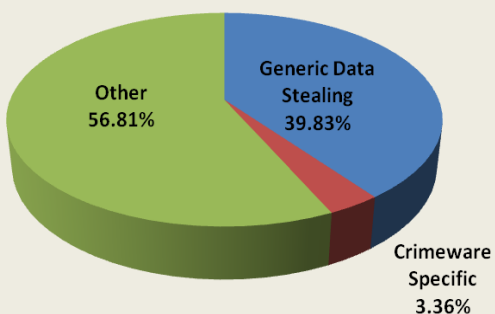
Malware Types - January 2010



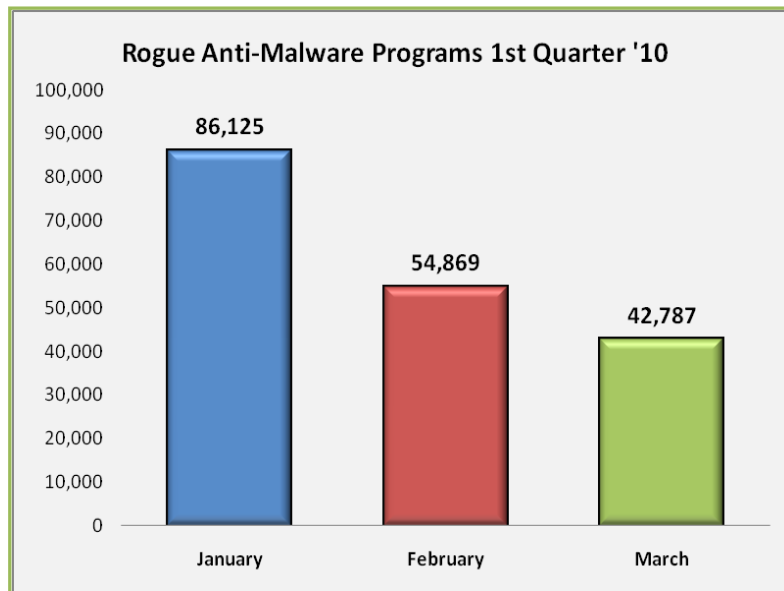
Malware Types - February 2010



Malware Types - March 2010



Rogue Anti-Malware Programs – 1st Quarter 2010



According to Luis Corrons, PandaLabs Technical Director and APWG *Trends Report* contributing analyst, there was a dramatic decrease in the number of rogueware samples detected in Q1 (183,781) compared to Q4 2009 (252,025). This represented a decrease of more than 37 percent quarter over quarter.

While in Q4, most of the samples came from the *Antivirus2008* family, in Q1 2010 that variant of crimeware almost disappeared, and it is not even in the top 10 in Q1. These are the most prevalent families, responsible of the creation of most of the samples detected:

Adware/MSAntiSpyware2009

Adware/TotalSecurity2009

Adware/PrivacyCenter

Adware/SystemGuard2009

Phishing-based Trojans and Downloader's Hosting Countries (by IP address)

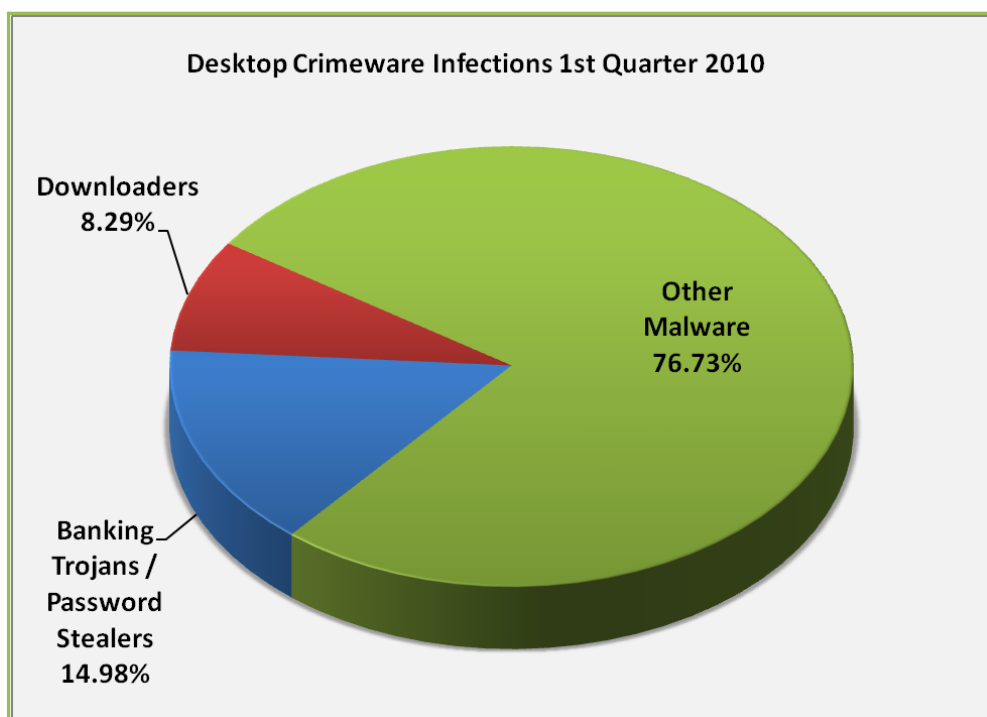
This chart represents a breakdown of the websites which were classified during the first quarter 2010 as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger. This quarter, and for the first time recorded by the APWG, the top four countries remained in ranked order throughout the entire three month period, consistently lead by the USA.

January		February		March	
USA	36.63%	USA	39.38%	USA	40.71%
China	15.37%	China	9.48%	China	13.17%
Russia	5.51%	Russia	9.23%	Russia	6.69%
Netherlands	5.35%	Netherlands	7.42%	Netherlands	5.39%
Germany	5.05%	Lithuania	4.35%	Germany	4.60%
Brazil	3.93%	Rep. Korea	3.87%	Rep. Korea	4.06%
Spain	3.36%	Spain	3.55%	Brazil	4.05%
Rep. Korea	2.66%	Germany	3.13%	Spain	3.81%
Ukraine	2.42%	Brazil	2.94%	Turkey	1.87%
France	2.15%	Ukraine	1.96%	UK	1.69%

Desktop Crimeware Infections – 1st Quarter 2010

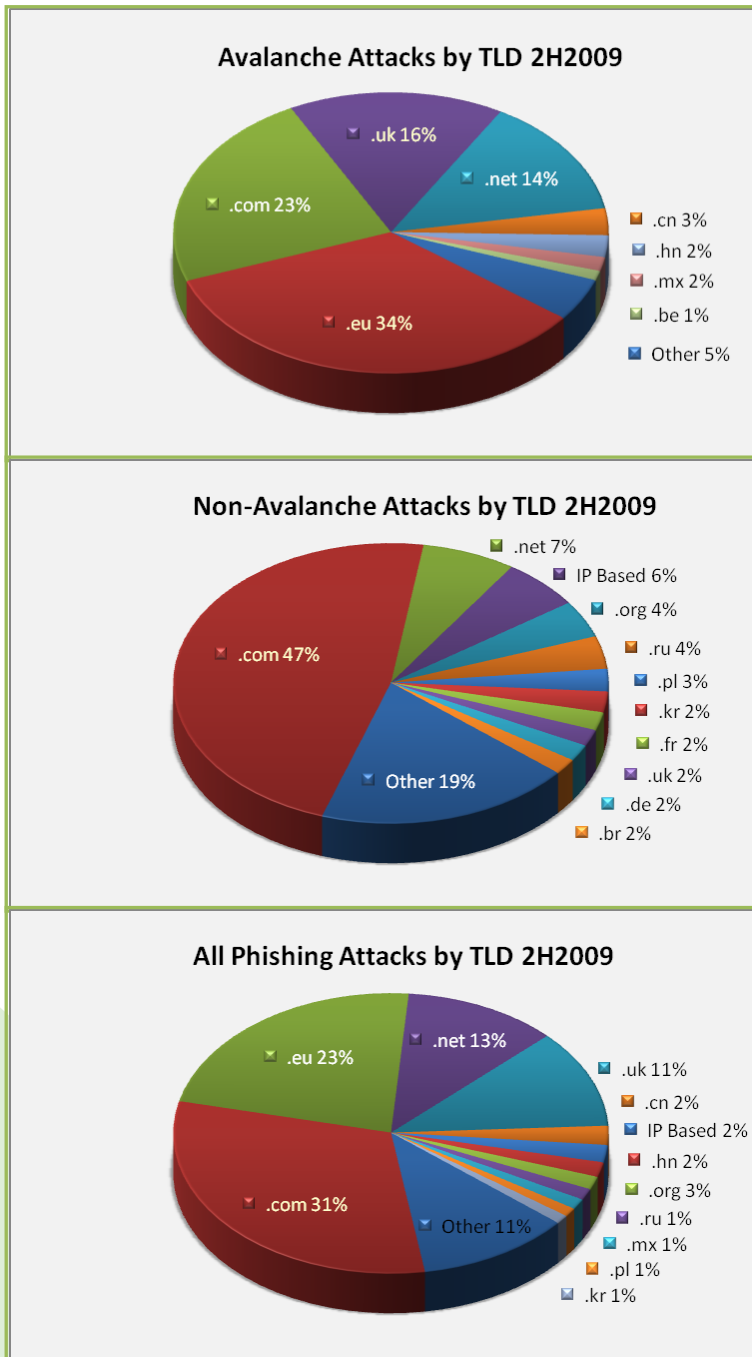
Scanning and Sampling Methodology: Panda Labs gathers data from millions of computers worldwide through its scanning service to give a statistically valid view of the security situation at the desktop. The scanned computers belong to both corporate and consumer users in more than 100 countries. Though the scanning system checks for many different kinds of potentially unwanted software, for this report, Panda Labs has segmented out 'Downloaders' and 'Banking Trojans/Password Stealers' as they are most often associated with financial crimes such as automated phishing schemes.

While the relative proportions of crimeware genera remained static during the surveyed term, the proportion of infected computers increased substantially from Q4 2009 to Q1 2010, growing from 10,305,805 in Q4 2009 to 11,384,640 in Q1 2010, rising from 47 percent to more than 53 percent in Q1 2010. This shift was an increase of more than 10 percent quarter over quarter.



Q1: Scanned Computers	21,203,020	
Infected Computers	11,384,640	53.69%
Non Infected Computers	9,818,380	46.31%
Banking Trojans / Password	3,176,177	14.98%
Downloaders	1,757,660	8.29%

Avalanche Attacks by Top-Level Domain 2nd Half 2009



A single electronic crime syndicate employing advanced malware was responsible for two-thirds of all the phishing attacks detected in the second half of 2009 - and was responsible for the overall increase in phishing attacks recorded across the Internet.

"Avalanche's impact was unprecedented," said Greg Aaron, Director of Key Account Management and Domain Security at Afilias and co-author of a study that rendered these statistical insights last year. "This one criminal group was responsible for two-thirds of the world's phishing

"Avalanche" is the name given to the world's most prolific phishing gang, and to the infrastructure it uses to host phishing sites, a system for deploying mass-produced phishing sites, and for distributing malware that gives the gang additional capabilities for theft.






Rod Rasmussen, founder and CTO of Internet Identity and co-author of the study, said, "Avalanche's relentless activities led to the development of some very effective counter-measures."

Rasmussen explained, "The data shows that the anti-phishing community -- including the target institutions, security responders, and domain name registries and registrars -- got very good at identifying and shutting down Avalanche's attacks on a day-to-day basis. Further, a coordinated action against Avalanche's infrastructure in November has led to an ongoing, significant reduction in attacks through April 2010."

The full report this data was drawn from can be found here:

http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf

APWG Phishing Activity Trends Report Contributors

 <p>Afilias is the world's leading provider of Internet infrastructure solutions that connect people to their data.</p>	 <p>Internet Identity (IID) is a US-based provider of technology and services that help organizations secure Internet presence.</p>	 <p>MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.</p>
 <p>Panda Security's mission is to keep our customers' information and IT assets safe from security threats, providing the most effective protection with minimum resource consumption.</p>	 <p>Websense, Inc. is a global leader in secure Web gateway, data loss prevention and email security solutions, protecting more than 43 million employees at organizations worldwide.</p>	

The *APWG Phishing Activity Trends Report* is published by the APWG, an industry, government and law enforcement association focused on eliminating the identity theft and frauds that result from the growing problem of phishing, crimeware, and email spoofing. For further information about the APWG, please contact APWG Deputy Secretary General Foy Shiver at 404.434.7282 or fshiver@antiphishing.org. For media inquiries related to the content of this report please contact APWG Secretary General Peter Cassidy at 617.669.1123; Te Smith of MarkMonitor at 831.818.1267 or Te.Smith@markmonitor.com; Luis Corrons of Panda at lcorrns@pandasoftware.es; Heather Read of Afilias at hread@afilias.info or 215.706.5777; for Websense, contact publicrelations@websense.com; and for Internet Identity contact pr@internetidentity.com or 253.590.4100

About the APWG

The APWG, founded as the Anti-Phishing Working Group in 2003, is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, and solutions providers. There are more than 1,800 companies and government agencies worldwide participating in the APWG and more than 3,500 members. Note that because phishing attacks and email fraud are sensitive subjects for many organizations that do business online, the APWG has a policy of maintaining the confidentiality of member organizations.

The website of the APWG is <http://www.antiphishing.org>. It serves as a resource for information about the problem of phishing and electronic frauds perpetrated against personal computers and their users. The APWG, a 501c6 tax-exempted corporation, was founded by Tumbleweed Communications, financial services institutions and e-commerce providers. APWG's first meeting was in November 2003 in San Francisco and in June 2004 was incorporated as an independent corporation controlled by its steering committee, its board of directors, and its executives.

Report data consolidation and editing completed by Ronnie Manning, Mynt Public Relations, since 2005.