Phishing Activity Trends Report

1st Half 2009

APWG

Committed to Wiping Out Internet Scams and Fraud

January – June 2009

Phishing Activity Trends Report, 1st Half / 2009

Phishing Report Scope

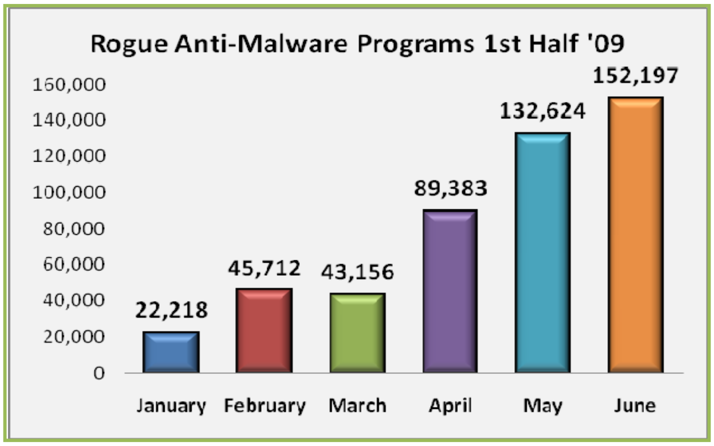
The quarterly *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.antiphishing.org and by email submissions to reportphishing@antiphishing.org. APWG also measures 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.

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

Rogue Anti-Malware Programs Growing at Unprecedented Pace Through H1 of 2009



Rogue anti-malware programs are proliferating at an unprecedented rate. In Q1, 2009, more new strains of rogue anti-malware were created than in all of 2008. In H1, 2009, the number of such programs grew 585 per cent. [See page 9 for details.]

1st Half '09 Phishing Activity Trends Summary

- Unique phishing reports submitted to APWG recorded a high of 37,165 in May, around 7 per cent higher than last year's high of 34,758 in October. [p. 4]
- The number of unique phishing websites detected in June rose to 49,084, the highest recorded since April, 2007's record of 55,643. [p. 4]
- Brand-domain pairs increased to a record 21,085 in June, up 92 per cent from the beginning of 2009. [p. 5]
- The number of hijacked brands ascended to a high of 310 at the end of Q1. [p. 6]
- Payment Services became phishing's most targeted sector, displacing Financial Services in Q1 & Q2. [p. 7]
- Banking trojan/password-stealing crimeware infections detected increased during more than 186 percent between Q4, 2008 and Q2, 2009. [p. 10]
- The total number of infected computers rose more than 66 percent between Q4 2008 and the end of the half, 2009 to 11,937,944, representing more than 54 percent of the total sample of scanned computers. [p. 10]
- Sweden moved ahead of the United States as the nation hosting the most phish websites at the half's end. [p. 7]
- China hosted the most websites harboring Trojans and Downloaders from March through June. [p. 9]

Methodology

APWG continues to refine and develop its tracking and reporting methodology and to incorporate new data sources into its 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.

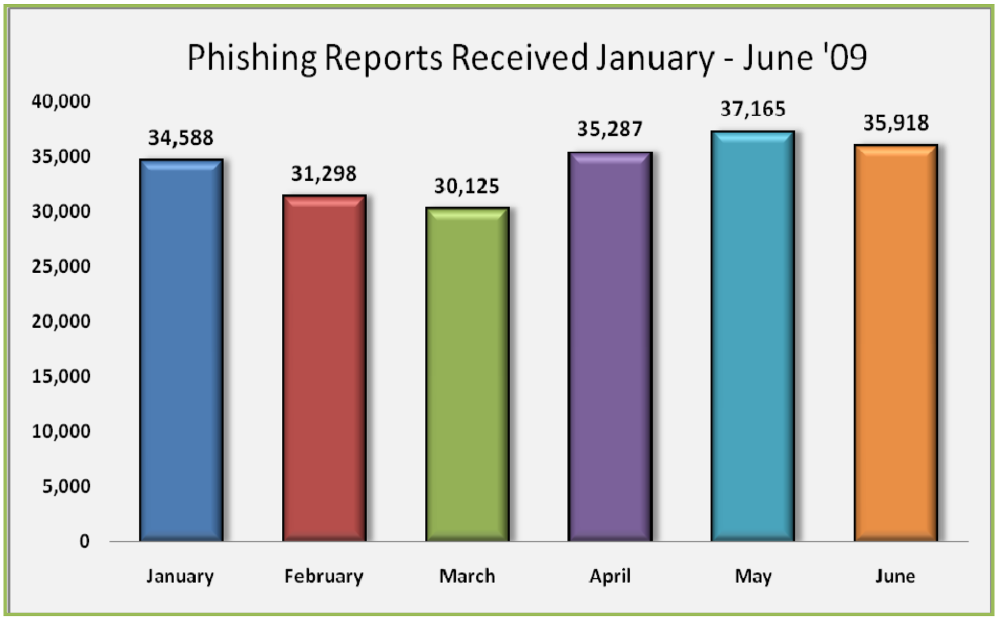
APWG additionally tracks crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample) as well as unique sites that are distributing crimeware (typically via browser drive-by exploits).

REPORT DEVELOPMENT NOTE: A new metric has been added to the APWG reports, using data contributed by Websense, measuring proliferation of malevolent software. [See page 8] This metric measures proportions of three genera of malevolent code: *Crimeware* (data-stealing malicious code designed to victimize financial institutions' customers and co-opt those institutions' identities); *Data Stealing and Generic Trojans* (designed to send information from the infected machine, control it, and open backdoors on it); and *Other* (commonly encountered in the field as auto-replicating worms, dialers for telephone charge-back scams, etc.) This metric replaces the monthly counts of "Password-Stealing Malicious Code URLs" and "Password Stealing Malicious Code - Unique Applications" which, due to multiplicity of counting methods and incongruent sources has proven systematically unreliable. The Measure of Detected Crimeware provides a more precisely descriptive measure of malevolent code trends.

Statistical Highlights for 1st Half, 2009

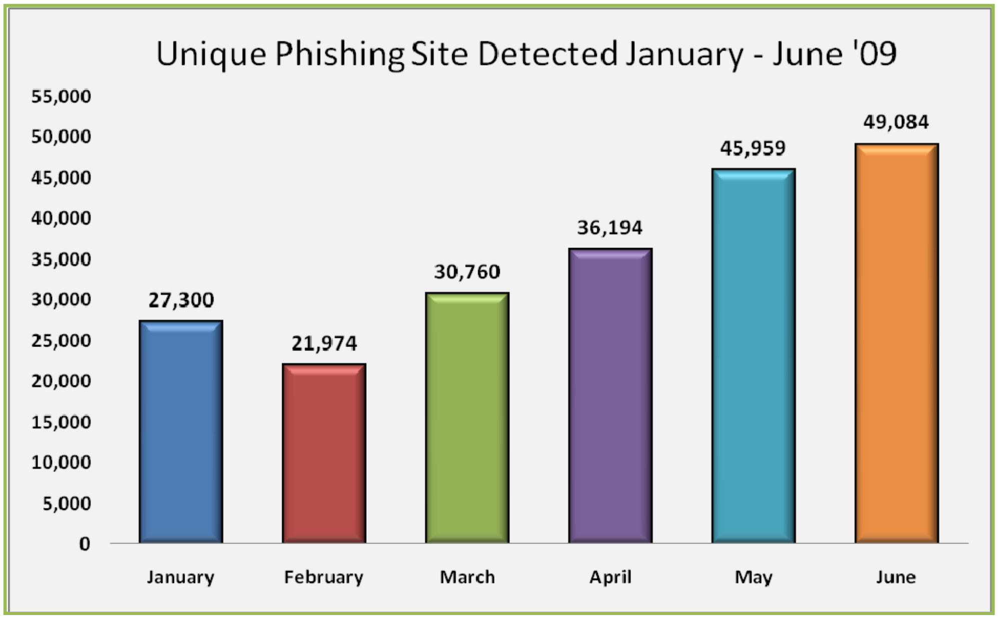
	Jan.	Feb.	March	April	May	June
Number of unique phishing email reports received by APWG from consumers	34,588	31,298	30,125	35,287	37,165	35,918
Number of unique phishing web sites detected	27,300	21,974	30,760	36,194	45,959	49,084
Number of brands hijacked by phishing campaigns	294	272	310	273	268	259
Country hosting the most phishing websites	USA	USA	USA	USA	USA	Sweden
Contain some form of target name in URL	69.01 %	64.44%	64.43%	63.25%	47.26%	33.12%
No hostname; just IP address	4.66%	8.69%	4.07%	2.33%	3.04%	1.86%
Percentage of sites not using port 80	0.05%	0.13%	0.09%	0.02%	0.10%	0.21%

Phishing Email Reports and Phishing Site Trends - 1st Half 2009



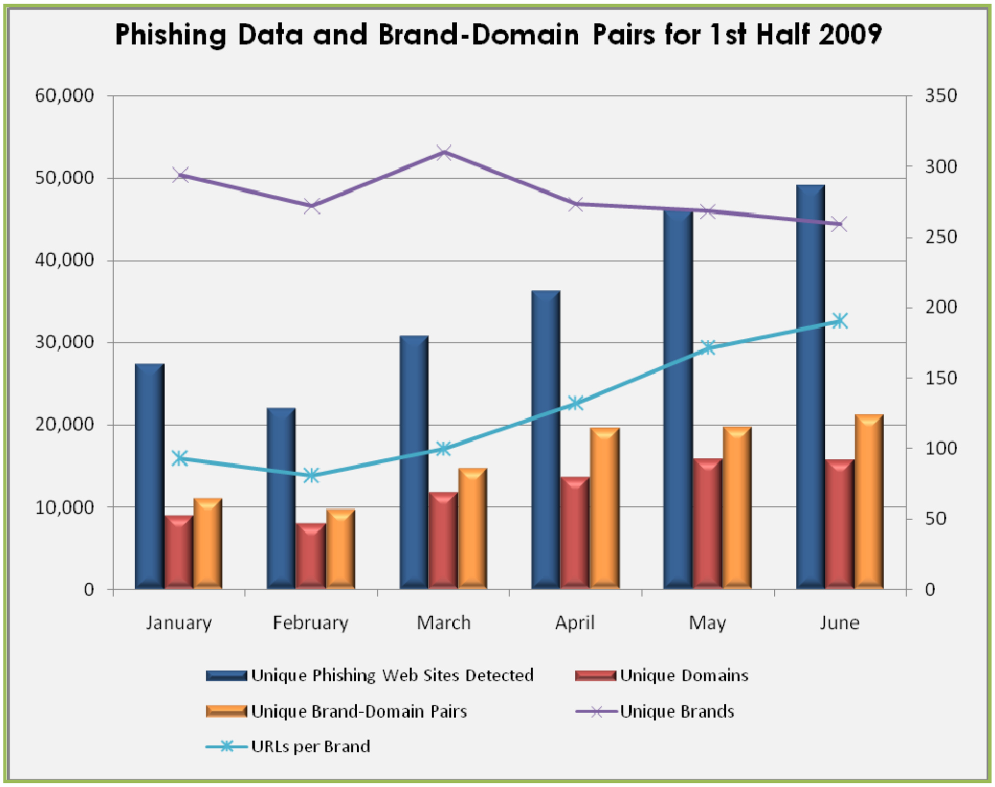
The number of unique phishing reports submitted to APWG in the first half of 2009 saw a steady decrease during the first three months of 2009, with a sharp return to previous levels in April. May's half-year high of 37,165 was an increase of nearly 7 per cent above last year's high of 34,758 in October. This data set represents a count of unique phishing email reports received by the APWG.

The number of unique phishing websites detected by APWG during the first half of 2009 fluctuated by nearly 30,000 between February and June. June's high for the half of 49,084 was 12 percent lower than the all-time high for this data set of 55,643 in April, 2007 – but still the second-highest number ever recorded for this measurement.



Brand-Domain Pairs Measurement - 1st Half 2009

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 rose to an all time high of 21,085 in June, increasing 92 per cent from January's reported 10,980.

"In Q2 we experienced a marked increase in phishing activity with record high brand-domain pairs and a near new high total unique phishing URL's detected. This increase in phishing activity can be attributed to more fast-flux phishing attacks." said Blake Hayward, Vice President, Product Marketing, MarkMonitor and *APWG Phishing Activity Trends Report* contributing analyst.

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.

	Jan.	Feb.	March	April	May	June
Number of Unique Phishing Web Sites Detected	27,300	21,974	30,760	36,194	45,959	49,084
Unique Domains	8,918	7,979	11,759	13,520	15,753	15,572
Unique Brand-Domain Pairs	10,980	9,620	14,635	19,503	19,610	21,085
Unique Brands	294	272	310	273	268	259
URLs Per Brand	93	81	100	132	171	190

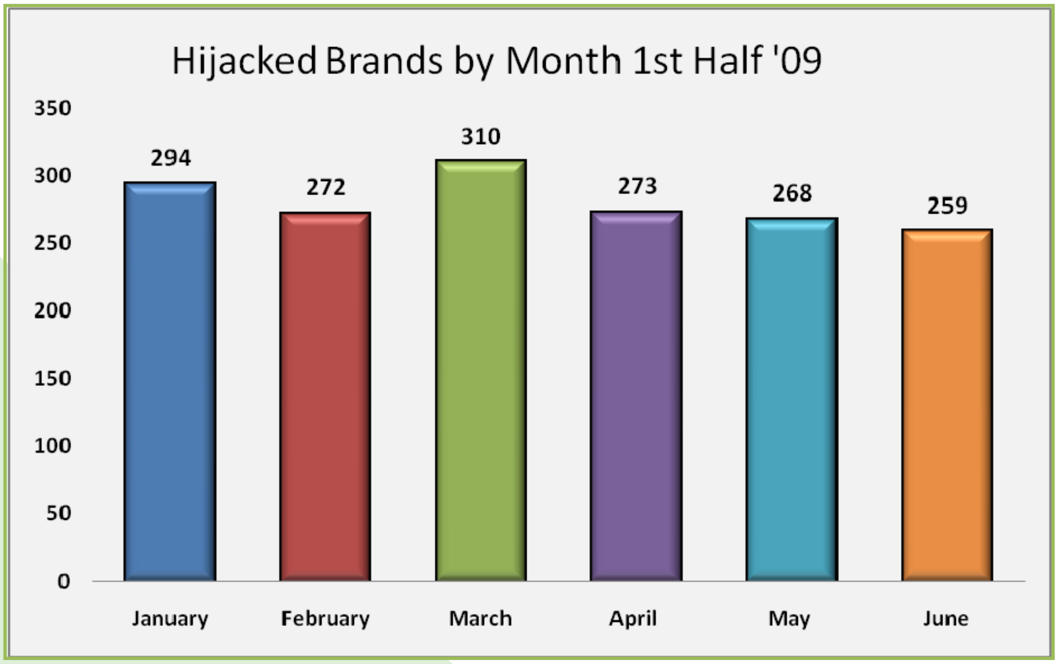
Most Used Ports Hosting Phishing Data Collection Servers - 1st Half 2009

The first half of 2009 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 this measurement.

January		February		March		April		May		June	
Port 80	99.96%	Port 80	99.88%	Port 80	99.91%	Port 80	99.98%	Port 80	99.90%	Port 80	99.85%
Port 443	.03%	Port 443	.05%	Port 443	.04%	Port 443	.01%	Port 443	.09%	Port 84	.05%
Port 82	.01%	Port 21	.03%	Port 21	.02%	Port 21	.01%	Port 21	.01%	Port 443	.04%
		Port 88	.02%	Port 88	.01%					Port 21	.03%
		Port 8085	.01%	Port 2480	.01%					Port 8080	.02%
		Port 82	.01%	Port 8086	.01%					Port 82	.01%

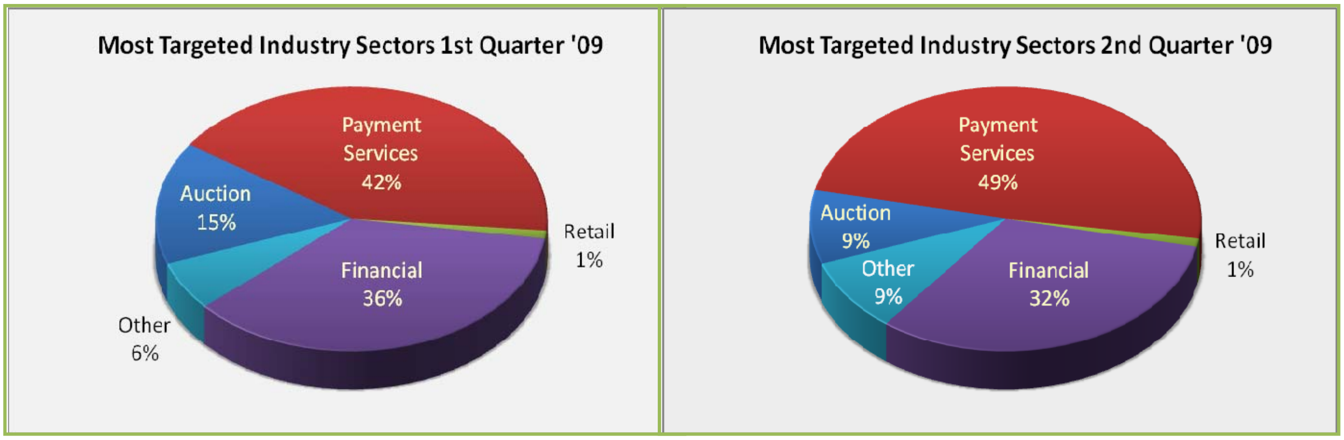
Brands and Legitimate Entities Hijacked by Email Phishing Attacks - 1st Half 2009

The first half of 2009 saw a rise in the number of hijacked brands to a record 310 in March, up more than 5 per cent from the record of 294 reached in May, 2008 and January, 2009. Phishers continue to expand the number and kind of brands they attack – and to employ fast-flux schemes to relocate phishing servers from one compromised host to another. Both techniques seek to maximize the longevity of phishing attacks: the former to prey on companies inexperienced in neutralizing campaigns and the latter to continually relocate phishers' counterfeit web sites and make them harder to take off line. [See MarkMonitor commentary on page 5 of this report for additional analysis.]



Most Targeted Industry Sectors - 1st Half 2009

Payment Services moved into the top position of targeted industry sectors in Q1 2009, rising over Financial Services for the first time since APWG began tracking the proportions of phishing attacks directed at each industry sector. The proportion of phishing campaigns directed against the Payment Services sector continued increasing through Q2, up some 16 percent from quarter to quarter, while the Financial Services sector's proportion dropped more than 10 percent during the same period.


Most Targeted Industry Sectors 1st Quarter '09

Most Targeted Industry Sectors 2nd Quarter '09

Countries Hosting Phishing Sites - 1st Half 2009

The United States continued its position as the top country hosting phishing sites during the first half of 2009 with the exception of June when Sweden reached the top. Sweden also took the top spot in September of last year as the country hosting the largest number of phishing sites and remains a top hosting country for phishing sites.

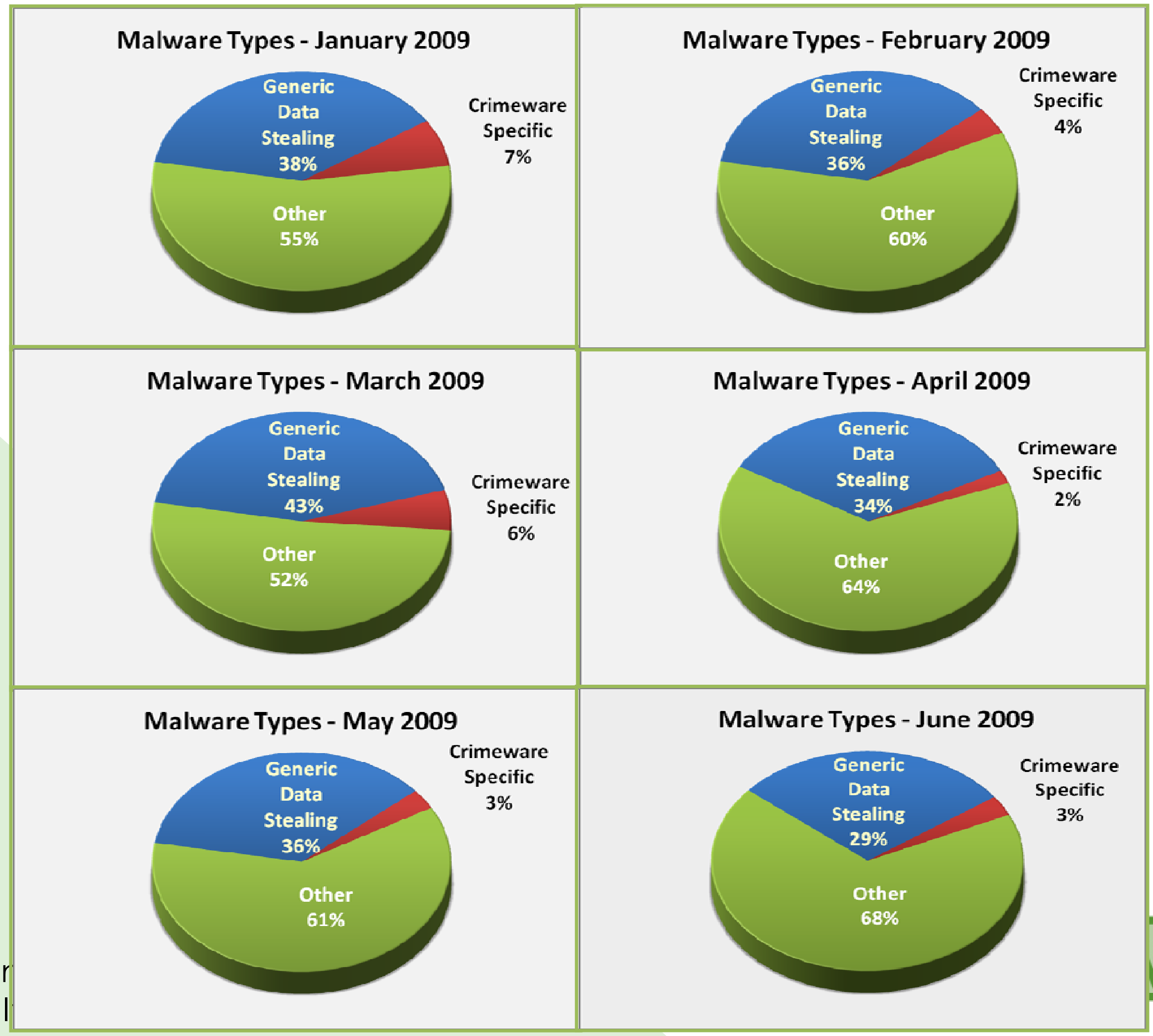
January		February		March		April		May		June	
USA	54.13%	USA	50.02%	USA	52.33%	USA	66.24%	USA	68.65%	Sweden	46.18%
Sweden	6.77%	Sweden	8.52%	China	15.21%	China	8.00%	China	6.33%	USA	42.39%
China	6.49%	China	7.10%	Sweden	8.48%	Sweden	7.76%	Canada	6.15%	Canada	3.52%
Canada	3.53%	Canada	3.29%	Canada	2.40%	Canada	2.67%	Germany	2.24%	China	1.57%
UK	2.96%	Germany	3.16%	Germany	2.09%	Germany	1.97%	UK	1.60%	Germany	0.88%
Germany	2.95%	Rep. Korea	2.75%	Russia	1.78%	UK	1.02%	Sweden	1.29%	UK	0.54%
Rep. Korea	2.10%	Netherlands	2.38%	Rep. Korea	1.56%	Netherlands	0.98%	Russia	1.23%	France	0.53%
France	2.04%	France	2.09%	France	1.54%	Rep. Korea	0.90%	France	1.19%	Rep. Korea	0.40%
Russia	1.95%	Taiwan	1.97%	Netherlands	1.39%	France	0.86%	Rep. Korea	1.17%	Netherlands	0.39%
Netherlands	1.73%	UK	1.94%	UK	1.39%	Russia	0.85%	Netherlands	1.01%	Russia	0.28%

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.
NOTE: The following metric has been added using data contributed from APWG member Websense, measuring proliferation of malevolent software. [See page 3 for full explanation of the change.] According to Dan Hubbard, APWG *Trends Report* contributing analyst and Websense Chief Technology Officer, "Due to evolution of attack sophistication, it is becoming increasingly difficult to separate and report on attacks that are specifically designed to steal customer banking information. Additionally, attacks that only look for credentials from popular social networking, web mail, and even gaming sites, can lead to attacks for banking theft and crimeware."

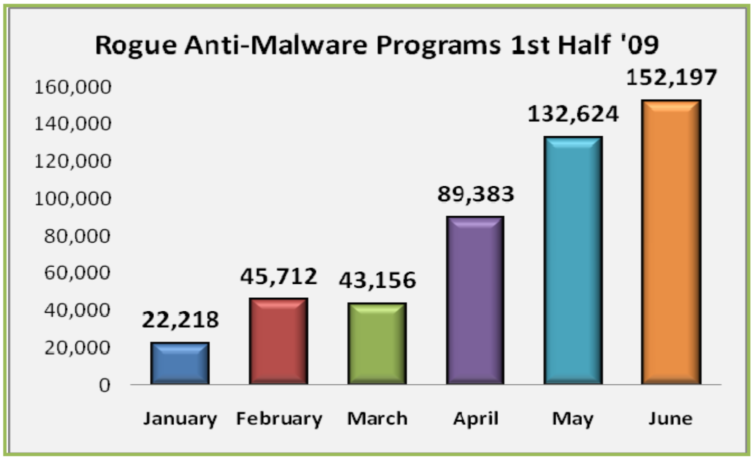
Measurement of Detected Crimeware - 1st Half 2009

Generally, over the half, the proportion of crimeware-specific malicious code (designed specifically against financial institutions' customers) and data-stealing malware receded as the proportion of other kinds of malware rose during this period.



Rogue Anti-Malware Programs - 1st Half 2009

According to Luis Corrons, PandaLabs Technical Director and APWG *Trends Report* contributing analyst, rogue anti-malware program proliferation "is experiencing an exponential growth. In the first quarter of 2009 alone, more new strains were created than in all of 2008. The second quarter painted an even bleaker picture, with the emergence of four times as many samples as in all of 2008.



"The primary reason for the creation of so many variants is to avoid signature-based detection by legitimate antivirus programs. The use of behavioral analysis is of limited use in this type of malware because the programs themselves do not act maliciously on computers, other than displaying false information," Corrons explained.

Several methods are being used to create the many variants. One of the most widespread techniques is known as server-side polymorphism, a technique in which every iteration of the fake antivirus software that is downloaded presents a slightly different binary file, making it harder for authentic anti-virus systems to recognize.

"This kind of threat is following the same behavior as other kinds of malware in the past (Trojans, etc.). At the beginning there were just a few gangs. The business model worked so new gangs got in the rogueware business. Right now, we have more than 200 different gangs. Some of them started to generate a flood of samples to bypass signature-based detections (10 of these gangs are responsible for the creation of 77.47% of the samples)," Corrons said.

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

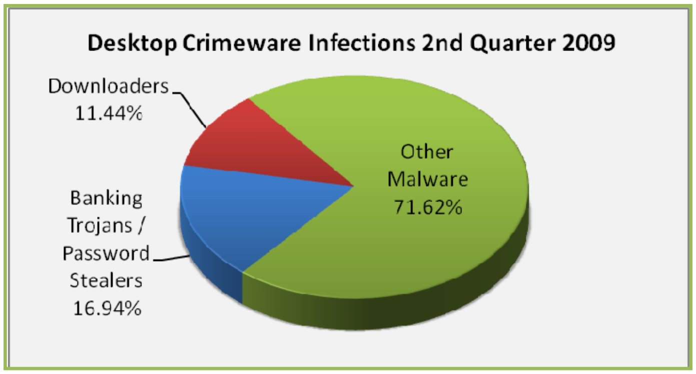
This chart represents a breakdown of the websites which were classified during 1st half 2009 as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger. China moved ahead of United States, the long-standing leaders in this category, holding it from March to June, 2009.

January		February		March		April		May		June	
USA	24.69%	USA	31.85%	China	32.86%	China	46.78%	China	34.30%	China	36.01%
China	20.80%	China	25.14%	USA	30.99%	USA	24.18%	USA	29.86%	USA	29.02%
Latvia	18.35%	Latvia	6.35%	Russia	3.81%	Latvia	5.58%	Ukraine	5.28%	Ukraine	5.16%
Gibraltar	10.60%	Brazil	5.19%	Brazil	3.78%	Russia	3.30%	Canada	4.29%	Brazil	4.19%
Brazil	3.99%	Russia	4.97%	Germany	3.49%	Ukraine	2.83%	Brazil	3.65%	Russia	3.81%
Germany	3.59%	Rep. Korea	3.55%	Rep. Korea	3.49%	Germany	2.64%	Russia	3.23%	Canada	3.44%
Russia	3.38%	Netherlands	3.02%	Netherlands	3.13%	Rep. Korea	2.05%	Romania	2.60%	Germany	3.38%
Rep. Korea	2.42%	Germany	2.97%	Latvia	3.00%	Brazil	1.66%	Germany	2.27%	Netherlands	2.17%
Canada	1.77%	Ukraine	2.44%	Ukraine	2.71%	Netherlands	1.60%	Spain	1.61%	France	1.15%
Netherlands	1.27%	UK	1.82%	Canada	2.23%	Canada	1.49%	Turkey	1.48%	Rep. Korea	1.04%

Desktop Crimeware Infections - 1st Half 2009

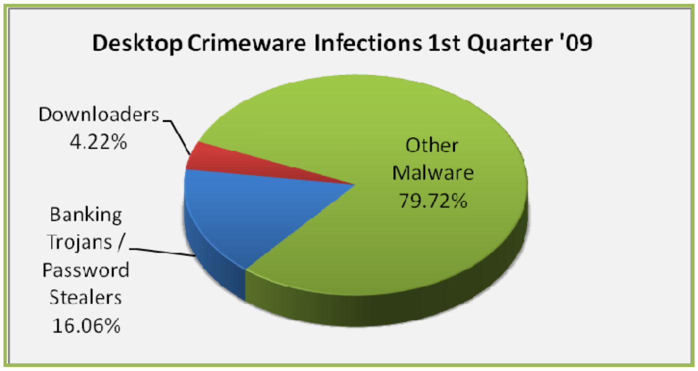
Scanning and Sampling Methodology: Panda Labs gathers data from millions of computers worldwide through its scanning service to give a statistically valid view of the security situation at the desktop. The scanned computers belong to both corporate and consumer users in more than 100 countries. Though 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.

The total number of infected computers rose more than 66 percent between Q4 2008 and the end of the half, 2009 to 11,937,944, representing more than 54 percent of the total sample of scanned computers, up from 35 percent in Q4, 2008. Banking trojan/password stealing crimeware infections detected increased during more than 186 percent between Q4, 2008 and Q2, 2009.



Q2: Scanned Computers	21,856,361	
Infected Computers	11,937,944	54.62%
Non Infected Computers	9,918,417	45.38%
Banking Trojans / Password	626,409	16.94%
Downloaders	423,053	11.44%

Q1: Scanned Computers	20,399,717	
Infected Computers	11,118,809	54.50%
Non Infected Computers	9,280,908	45.50%
Banking Trojans / Password	507,295	16.06%
Downloaders	133,223	4.22%



In Q2 there was also an increase in detected downloaders of more than 217 percent from Q1 to Q2, 2009. This is mainly due to a downloader called Zlob.LH in Q2, according to Panda Labs, which recorded 274,510 samples of this Trojan, which downloads and installs rogue anti-virus software.

APWG Phishing Activity Trends Report Contributors

MarkMonitor

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.

PANDA SECURITY

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.

websense ESSENTIAL INFORMATION PROTECTION™

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.

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 +1 404.434.7282 or fshiver@antiphishing.org. For media inquiries related to the content of this report please contact APWG Secretary General Peter Cassidy at +1 617.669.1123; Cas Purdy, Websense at +1 858.320.9493 or cpurdy@websense.com; Te Smith at +1 831.818.1267 or Te.Smith@markmonitor.com; or Luis Carrons at lcorrons@pandasoftware.es. APWG thanks its contributing members, above, for the data and analyses in this report.

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. The organization provides a forum to discuss phishing issues, define the scope of the phishing problem in terms of hard and soft costs and consequences, and to share information and best practices for eliminating the problem.

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 participating in the APWG and more than 3,300 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.