Phishing Activity Trends Report

1st Half 2011

APWG

Unifying the
Global Response
To Cybercrime

January – June 2011

Phishing Report Scope

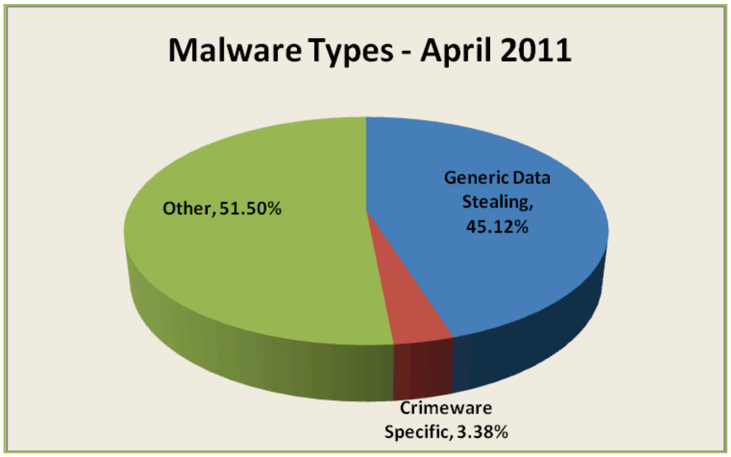
The *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org and by email submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation and propagation of crimeware drawing from the research of our member companies.

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

Data-Stealing Malware Growth Reaches New Plateau in H1 2011



Data-stealing and generic Trojan malware, typically designed to send information from the infected machine, control it, and open backdoors on it, reached an all-time high in H1 2011, comprising almost half of all malware detected. [p. 9]

1st Half 2011 Phishing Activity Trends Summary

- The half's high for unique phishing reports submitted to APWG of 26,402 in March was down 35 percent from the all-time high of 40,621 in August, 2009 [p. 4]
- Unique phishing websites detected reached a high for the half in March with 38,173, down more than 32 percent from the record of 56,362 in August 2009 [p. 4]
- Phishing attacks are focusing increasingly on brands in Latin America, the Middle East and Asia [p. 5]
- The number of phished brands reached a high in the half of 339 in January, down 5 percent from the all-time high of 356 reached in October, 2009 [p.6]
- After cracking into the top 10 last November, Egypt has ranked in the top three hosting countries for four out of the first six months of 2011 [p. 7]
- Trojans were 72 percent of malware detected in H1, 2011, up from 55 percent in H2, 2010 [p. 8]
- The top 10 most prevalent families of fake anti-virus software are responsible for nearly 70 percent of the infections caused by rogueware [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.

Statistical Highlights for 1st Half, 2011

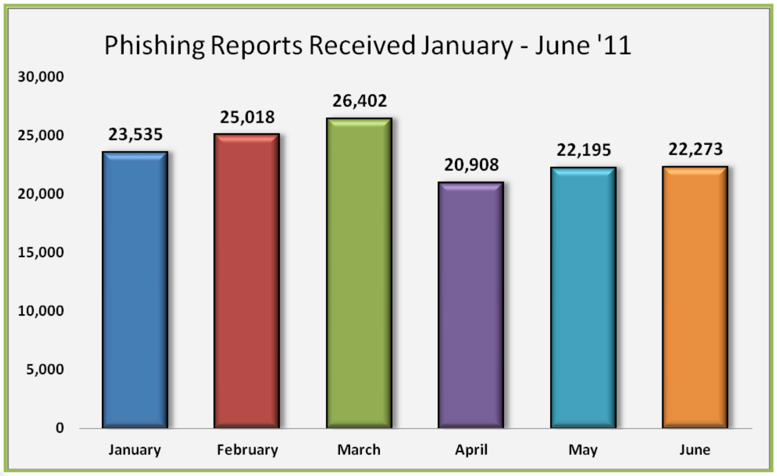
	Jan.	Feb.	March	April	May	June
Number of unique phishing email reports received by APWG from consumers	23,535	25,018	26,402	20,908	22,195	22,273
Number of unique phishing web sites detected	29,815	31,544	38,173	33,008	35,213	28,148
Number of brands hijacked by phishing campaigns	339	335	313	333	331	310
Country hosting the most phishing websites	USA	USA	USA	USA	USA	USA
Contain some form of target name in URL	69.82%	74.97%	72.38%	72.16%	78.82%	76.55%
No hostname; just IP address	3.18%	3.31%	3.38%	4.15%	4.14%	3.38%
Percentage of sites not using port 80	0.59%	0.52%	1.11%	0.78%	0.44%	0.45%

Phishing Email Reports and Phishing Site Trends – 1st Half 2011

Phishing attacks targeted at consumers on the Internet remain at high levels, with some 20,000 to more than 25,000 unique phishing campaigns recorded each month though the half. Each campaign can target hundreds of thousands or sometimes millions of users. There are thousands of fake phishing websites established online every day, luring any number of consumers to trouble and loss.

However, the most concerning contemporary threat during H1, 2011 was spear-phishing campaigns. These are hyper-focused, often personalized phishing attacks directed against specific company executives, IT personnel and management personnel with corporate treasury authority and/or access to company online bank accounts. These emails tend to evade spam filters, unlike the broad-based consumer phishing email campaigns. The spear-phishing emails either contain an attachment that can infect the recipients computer with sophisticated financial malware, or contain a link to a website that can infect the recipient's computer with financial malware and trojans.

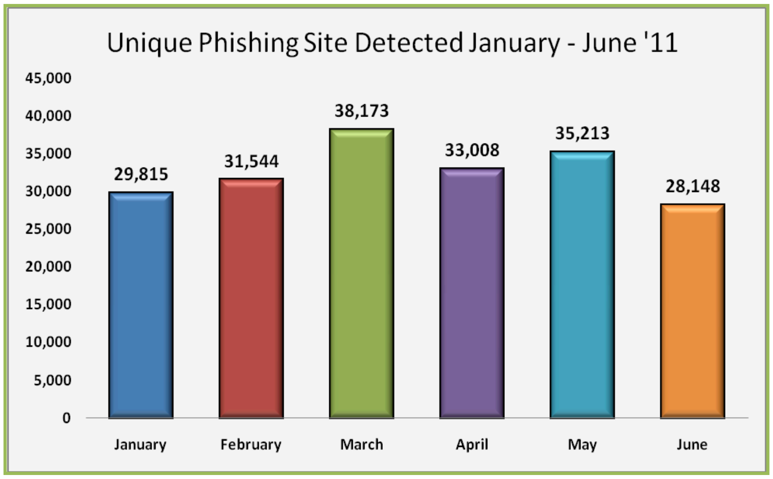
In H1, 2011 APWG members and correspondents have reported high profile spear-phishing attacks against security companies, defense contractors and financial institutions. In some cases, these have resulted in cyber criminals infiltrating companies' networks and stealing information worth tens of millions of dollars – and more.



These spear-phishing attacks are a key part of the Advanced Persistent Threats (APTs) that companies and governments are facing today. Responders, industries and governments engaging these threats have entered a new era and need new ways to detect them, measure their proliferation – and defend against them.

The number of unique phishing reports submitted to APWG in H1, 2011 reached a high of 26,402 in March, dropping to the half-year low of 20,908 in April. March's high was down 35 percent from the all-time high in August 2009 of 40,621 reports.

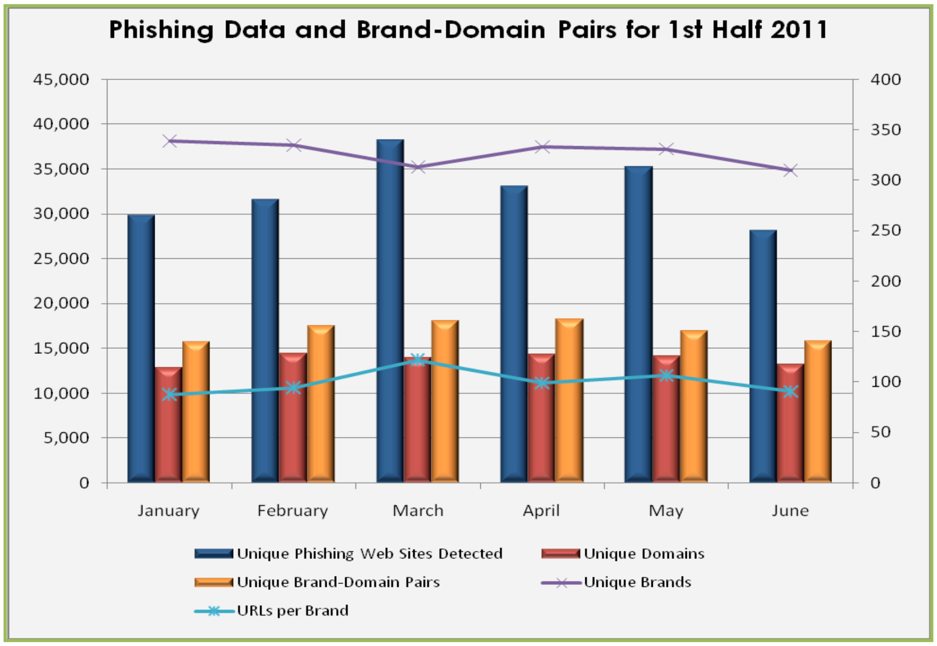
The number of unique phishing websites detected by APWG during H1, 2011 fluctuated by over 10,000 websites within the half year. Reaching the highest point in March with 38,173, the half-year low was in June with 28,148. The half-yearly high in March was down more than 32 percent from the record high of 56,362 recorded in August 2009.



Brand-Domain Pairs Measurement – 1st Half 2011

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 fluctuated during the first half of 2011. The high for the half year, 18,056 brand-domain pairs in March, was down 26 percent from the record of 24,438 recorded in August, 2009.



"In the first half of 2011, MarkMonitor saw a significant rise of phishing attacks when compared with 2010," said Ihab Shraim, Chief Security Officer and Vice President, Network and Systems Engineering and *Trends Report* contributing analyst.

"Furthermore, phishing attacks are increasingly targeting brands worldwide and, notably, in emerging markets such as Latin America, Middle East and Asia."

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	29,815	31,544	38,173	33,008	35,213	28,148
Unique Domains	12,750	14,417	13,907	14,289	14,131	13,152
Unique Brand-Domain Pairs	15,697	17,446	18,056	18,207	16,920	15,757
Unique Brands	339	335	313	333	331	310
URLs Per Brand	87.94	94.16	121.95	99.12	106.38	90.81

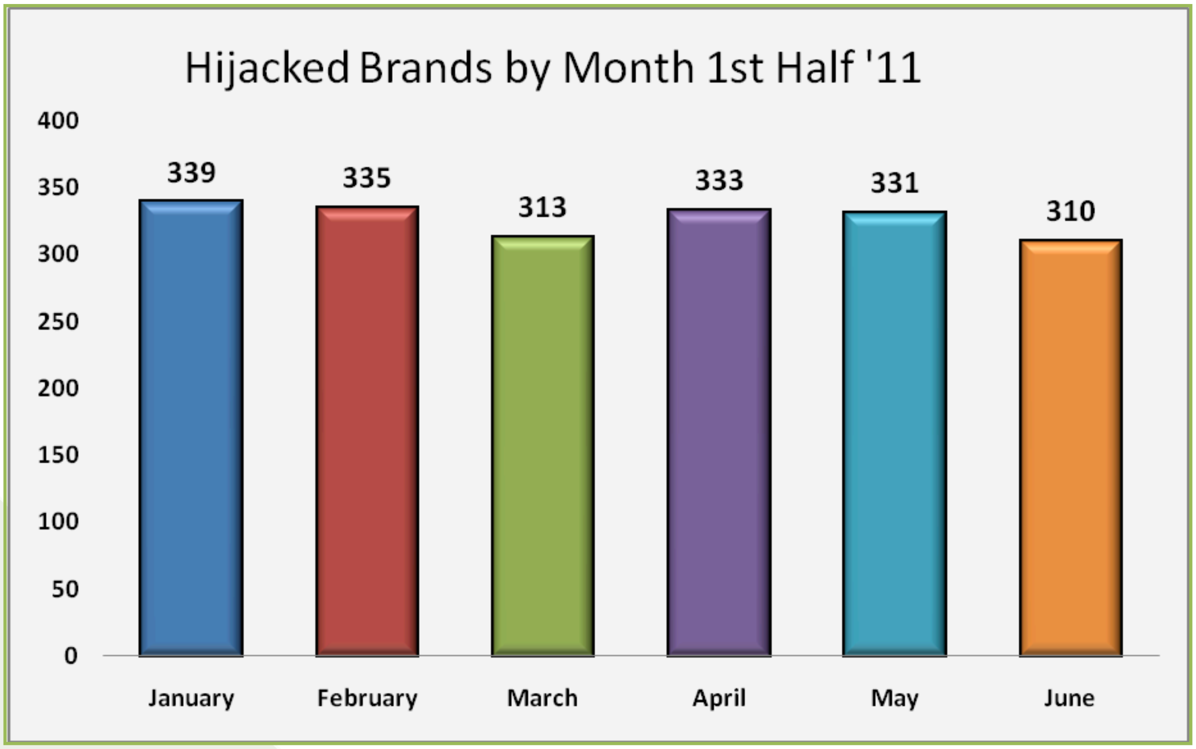
Most Used Ports Hosting Phishing Data Collection Servers – 1st Half 2011

The first half of 2011 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		April		May		June	
Port 80	99.553%	Port 80	99.481%	Port 80	98.895%	Port 80	99.226%	Port 80	99.563%	Port 80	99.553%
Port 443	.447%	Port 443	.461%	Port 443	.992%	Port 443	.668%	Port 443	.364%	Port 443	.447%
		Port 21	.058%	Port 21	.113%	Port 21	.106%	Port 21	.073%		

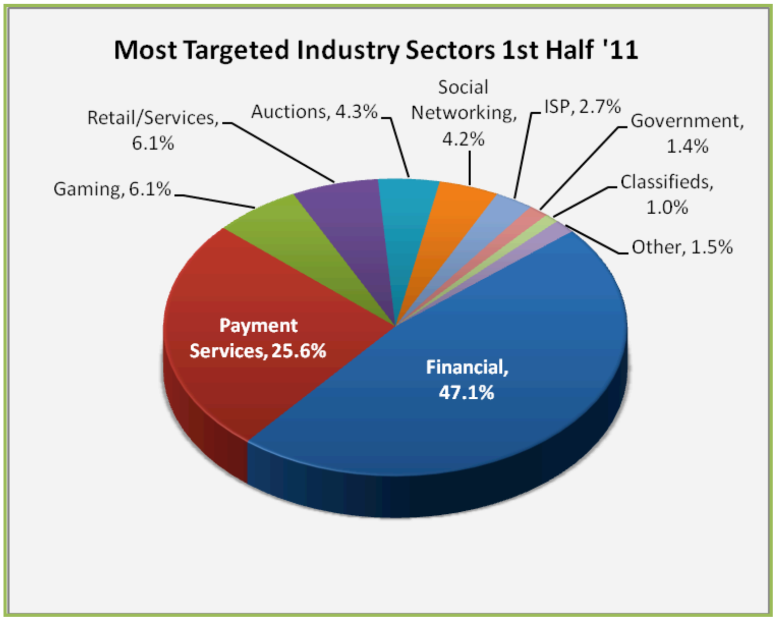
Brands and Legitimate Entities Hijacked by Email Phishing Attacks – 1st Half 2011

The first half of 2011 saw a high of 339 in January during the six-month period, a decrease of 5 percent from the all-time high of 356 reached in October, 2009.



Most Targeted Industry Sectors – 1st Half 2011

Financial Services continued to be the most targeted industry sector in the first half of 2011. Financial Services was previously eclipsed by Payment Services in Q2, 2010, which last eclipsed Financial Services in Q2, 2010, remained the second highest industry sector for targeted attacks. [*Data sampling note*: the reported retail sector proportion of the target base in H1, 2011 increased markedly to 6.1 percent from 1 percent in Q4, 2010, due to the addition of new data feeds from the Asia Pacific region by APWG research correspondent MarkMonitor.]



Countries Hosting Phishing Sites – 1st Half 2011

The United States continued to be the top country hosting phishing sites during the first half of 2011. After cracking into the top 10 last November, Egypt has ranked in the top three hosting countries for four out of six months of 2011.

January		February		March		April		May		June	
USA	48.66%	USA	53.68%	USA	46.50%	USA	52.42%	USA	51.65%	USA	46.42%
Canada	6.81%	Canada	10.88%	Canada	18.06%	Germany	4.74%	Egypt	7.70%	Egypt	10.53%
Egypt	6.59%	Egypt	5.90%	Germany	7.04%	UK	4.00%	Canada	5.57%	Canada	7.23%
Germany	5.45%	UK	4.67%	UK	3.96%	Canada	3.60%	Netherlands	4.25%	Germany	4.87%
UK	4.43%	Germany	4.03%	Netherlands	3.23%	France	3.29%	UK	4.07%	Netherlands	3.95%
Netherlands	2.96%	Netherlands	2.59%	Rep. Korea	3.13%	Egypt	3.19%	Germany	3.94%	Rep. Korea	3.01%
Russia	2.38%	Rep. Korea	1.66%	France	1.71%	Bulgaria	3.11%	France	2.43%	Russia	2.52%
Rep. Korea	1.97%	Russia	1.61%	Brazil	1.27%	Netherlands	2.70%	Russia	2.01%	UK	2.43%
Brazil	1.86%	France	1.50%	Russia	1.22%	Russia	1.73%	Rep. Korea	1.94%	France	2.16%
Romania	1.71%	Brazil	0.97%	Australia	1.02%	China	1.54%	China	1.39%	Brazil	1.45%

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, such as financial institutions, 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.

Malware Infected Countries – 1st Half 2011

From January to June 2011, PandaLabs has registered 11,777,775 new malware samples, which is 13 percent more than the number of samples registered in H2, 2010 of 10,425,663. This figure reflects the total number of different malware samples that were intercepted during this period in terms of different files. This is important to note, as cybercriminals commonly issue the same samples over and over, obfuscated in slightly revised variations, employing polymorphism (server side/binary side), greatly increasing numbers of recorded samples in this metric.

According to Luis Corrons, PandaLabs Technical Director and APWG *Trends Report* contributing analyst, 72 percent of the new samples created in H1, 2011 are Trojans, the favorite cyber-weapon used by cybercriminals, a substantial increase from H2, 2010 when the proportion was 55 percent. Trojans are followed by traditional viruses at 15 percent of the total. Even though viruses may seem like a thing of the past, their recent revival stems from the appearance of a few but highly active families with new variants aimed at infecting a large number of users. New viruses such as Sality or Viking have Trojan-like features and are capable of stealing user information. Worms were the third most-detected malware, followed by Rogueware.

Type of Malware Created	Percent
Trojans	71.94%
Virus	15.10%
Worms	9.01%
Rogueware	2.40%
Other	1.55%

The overall infection rate of computers in this period is 39 percent, down from a level of more than 50 percent in H2, 2010. The percentage of infections varies depending on the country. Below are the lists of the top 10 and bottom 10 infected countries (out of 50 sampled and reported out by Panda Labs):

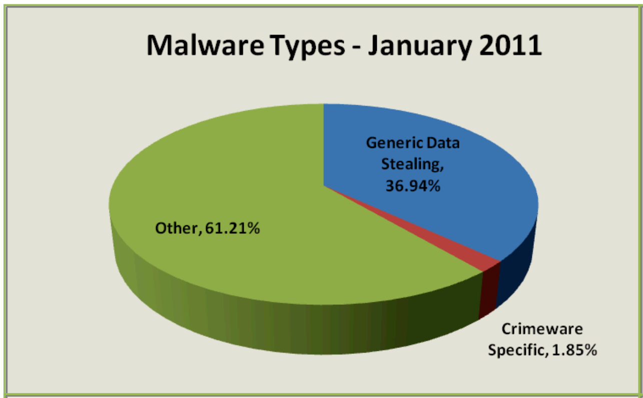
Ranking	Country	Infection Rate
1	China	62,65%
2	Thailand	58,44%
3	Taiwan	54,68%
4	Korea	52,40%
5	Turkey	51,51%
6	Russian Federation	49,39%
7	Brazil	45,74%
8	Poland	42,22%
9	Costa Rica	41,61%
10	Argentina	40,93%

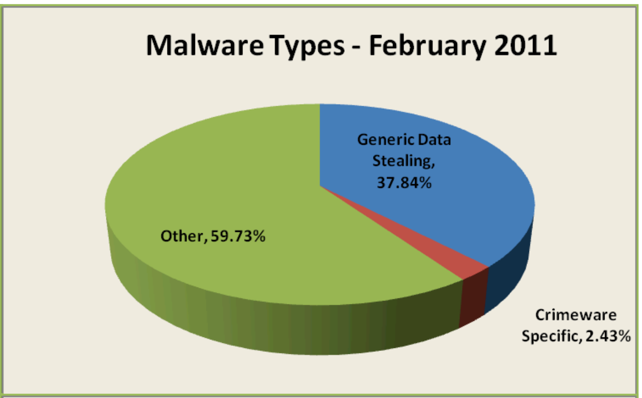
Ranking	Country	Infection ratio
41	Uruguay	44.48%
42	Honduras	44.47%
43	South Korea	44.08%
44	Hungary	42.99%
45	Belgium	42.93%
46	Guatemala	42.86%
47	El Salvador	42.62%
48	Slovakia	42.61%
49	Austria	42.58%
50	Czech Republic	41.82%

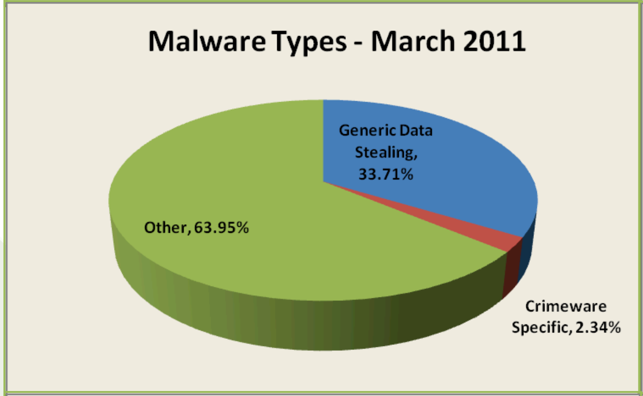
Measurement of Detected Crimeware – 1st Half 2011

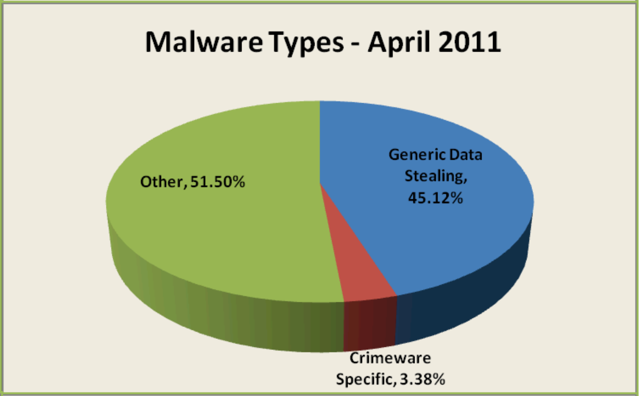
Using data contributed from APWG founding member Websense on proliferation of malevolent software, this metric measures proportions of three genera of malevolent code: *Crimeware* (data-stealing malicious code designed specifically to be used to victimize financial institutions' customers and to co-opt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

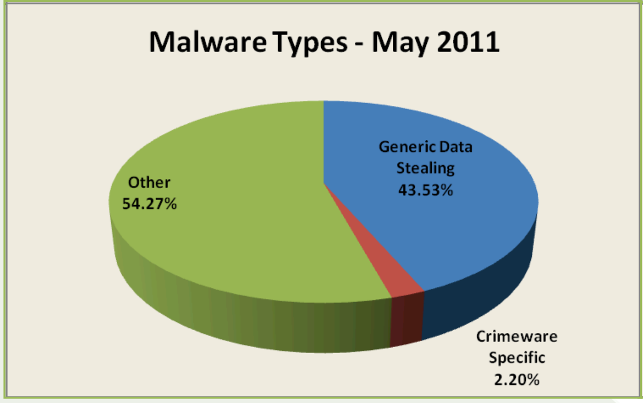
"The first half of 2011 saw an increase in not only the amount of malicious samples received but more importantly, malware files going after confidential information such as credit card data, social security numbers and credentials to financial websites," said Patrik Runald, Senior Manager, Security Research for Websense and a *Trends Report* contributing analyst. "With cybercrime being an industry generating hundreds of millions of dollars for the bad guys it's clear that this is a trend we will see for a long time."

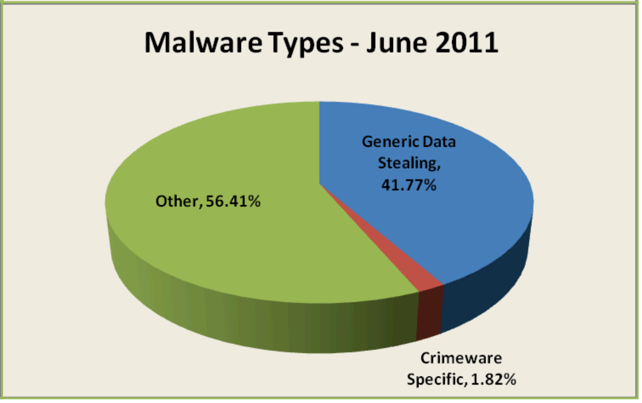

Malware Types - January 2011


Malware Types - February 2011


Malware Types - March 2011

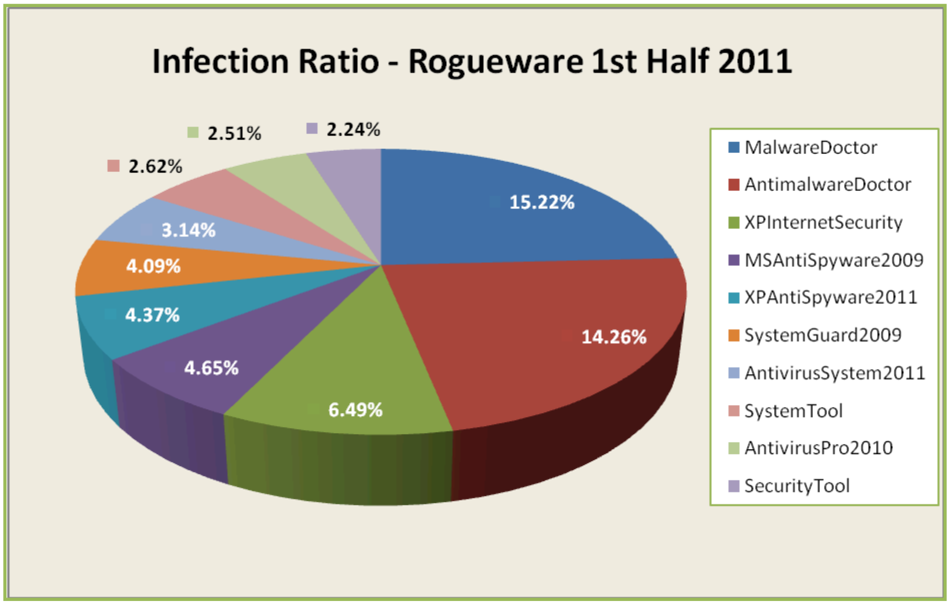

Malware Types - April 2011


Malware Types - May 2011


Malware Types - June 2011

Rogue Anti-Malware Programs – 1st Half 2011

According to Luis Corrons, PandaLabs Technical Director and APWG *Trends Report* contributing analyst, there were 131 different rogueware families causing infections during H1, 2011. The top 10 most prevalent families are responsible for more than 69.92 percent of the infections caused by rogueware, listed below in the chart and table:



Rogueware Family	%age
MalwareDoctor	15.22%
AntimalwareDoctor	14.26%
XPInternetSecurity	6.49%
MSAntiSpyware2009	4.65%
XPAntiSpyware2011	4.37%
SystemGuard2009	4.09%
AntivirusSystem2011	3.83%
SystemTool	3.58%
AntivirusPro2010	3.42%
SecurityTool	3.00%

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 half 2011 as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger. During the six month period the USA remained the top hosting country and the British Virgin Islands cracked the top 10 for the first time ever in June 2011.

January		February		March		April		May		June	
USA	39.40%	USA	55.15%	USA	38.96%	USA	43.20%%	USA	49.42%	USA	47.16%
China	11.40%	Germany	6.57%	UK	15.54%	China	9.25%	China	11.94%	China	9.16%
Russia	8.31%	Russia	5.32%	China	14.19%	Russia	6.94%	Germany	3.98%	Spain	8.83%
Canada	7.24%	China	5.20%	Russia	4.65%	Germany	6.64%	Brazil	3.73%	Germany	4.84%
Netherland	5.16%	Rep. Korea	3.19%	Brazil	3.95%	Brazil	5.37%	Russia	3.68%	B. Virgin. Il.	4.54%
Rep. Korea	4.16%	Egypt	2.57%	Canada	3.95%	Rep. Korea	3.80%	Rep. Korea	3.48%	Russia	4.13%
Brazil	3.30%	Brazil	2.51%	Rep. Korea	2.52%	Canada	3.65%	Spain	3.40%	Rep. Korea	4.11%
Ukraine	2.91%	Canada	2.43%	Ukraine	2.32%	Ukraine	2.76%	UK	3.07%	Brazil	2.48%
Germany	2.82%	Ukraine	2.05%	Germany	1.66%	Spain	2.38%	France	2.00%	Canada	1.89%
Spain	2.48%	UK	1.72%	Spain	1.62%	UK	1.71%	Canada	1.87%	Netherlands	1.72%

APWG Phishing Activity Trends Report Contributors

Afilias

Afilias is the world's leading provider of Internet infrastructure solutions that connect people to their data.

IID

Internet Identity (IID) is a US-based provider of technology and services that help organizations secure Internet presence.

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 Yes! 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. For further information about the APWG, please contact APWG Deputy Secretary General Foy Shiver at 404.434.7282 or foy@apwg.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 lcorrons@pandasoftware.es; for Websense, contact publicrelations@websense.com.

About the APWG

APWG, founded as the Anti-Phishing Working Group in 2003, is focused on eliminating the identity theft and frauds that result from the growing problem of phishing, crimeware, and email spoofing. Membership is open to qualified financial institutions, retailers, ISPs, solutions providers, the law enforcement community, government agencies, multi-lateral treaty organizations and NGOs. There are more than 2,000 enterprises worldwide participating in the APWG. Because electronic crime is a sensitive subject, APWG maintains a policy of confidentiality of member organizations.

Websites of APWG public-service enterprises include its public website, <http://www.antiphishing.org>; the Website of public awareness program, Stop. Think. Connect. Messaging Convention <http://www.stopthinkconnect.org> and the APWG's research website <http://www.ecrimeresearch.org>. These serve as resources about the problem of phishing and electronic frauds perpetrated against personal computers and their users – and resources for countering these threats. 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 board of directors, its executives and its steering committee.

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