Phishing Activity Trends Report

2nd Half 2010

APWG

Unifying the Global Response to Cybercrime

July – December 2010

Phishing Activity Trends Report, 2nd Half / 2010

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 APWG 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

Crimeware Development and Contagion Surging Worldwide in Second Half of 2010

Ranking	Country	Infection ratio
1	Thailand	66.97%
2	China	62.82%
3	Taiwan	59.90%
4	Latvia	55.75%
5	Saudi Arabia	55.42%
6	Russian Federation	54.32%
7	Israel	53.30%
8	Lithuania	53.22%
9	Turkey	51.55%
10	Poland	50.35%

More than 10 million malware samples were detected in H2, 2010 – close to 20 percent of the total number collected since 1990 by PandaLabs [p. 8]

2nd Half '10 Phishing Activity Trends Summary

- Unique phishing reports submitted to APWG in H2, 2010 steadily decreased over the half, after reaching a previous high for 2010 in June with 33,617 [p. 4]

- Unique phishing websites detected by APWG during H2, 2010 saw a fluctuation of more than 5,000 sites month to month within the half-year period [p. 4]

- The high number of unique brand-domain pairs, 16,767 in November, was down nearly 32 percent from the record of 24,438 in August, 2009 [p. 5]

- The number of phished brands reached a high of 335 in September during the half, a decrease of 6 percent from the all-time high of 356 in October, 2009 [p.6]

- Financial Services returned to being the most targeted industry sector in the 3rd and 4th quarters of 2010 [p. 7]

- Sweden jumped to the top of countries hosting phishing sites reported during Q3, 2010 with 83.12% of all hosting sites reported in August [p. 7]

- The top 10 most prevalent families of fake anti-virus software are responsible for more than 59 percent of rogueware infections [p. 10]

Methodology and Instrumented Data Sets

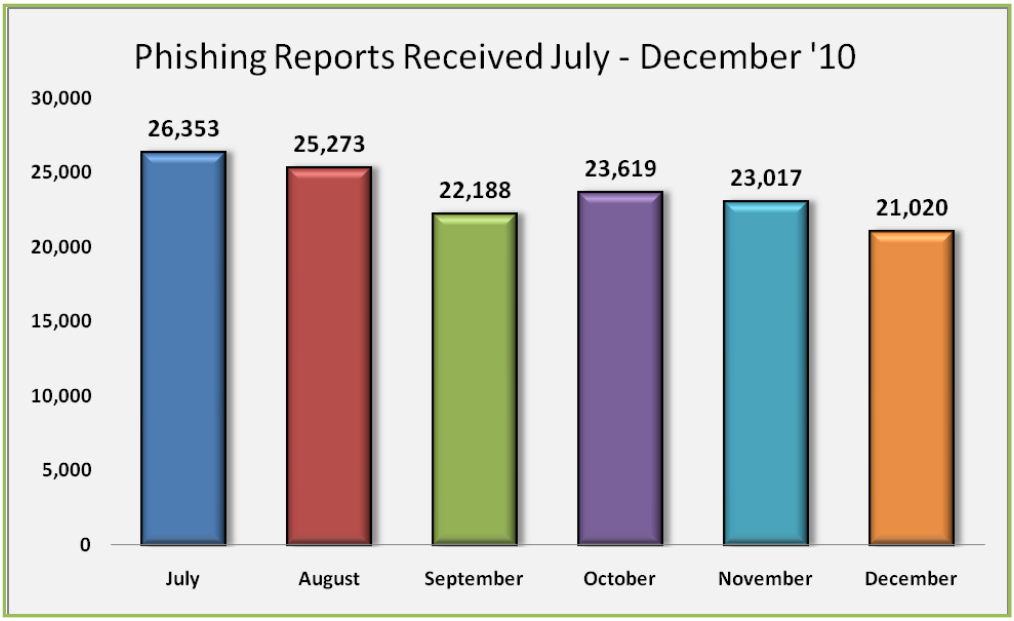
APWG continues to refine and develop its tracking and reporting methodology and to incorporate new data sources into our reports. APWG has re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent 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* 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 2nd Half, 2010

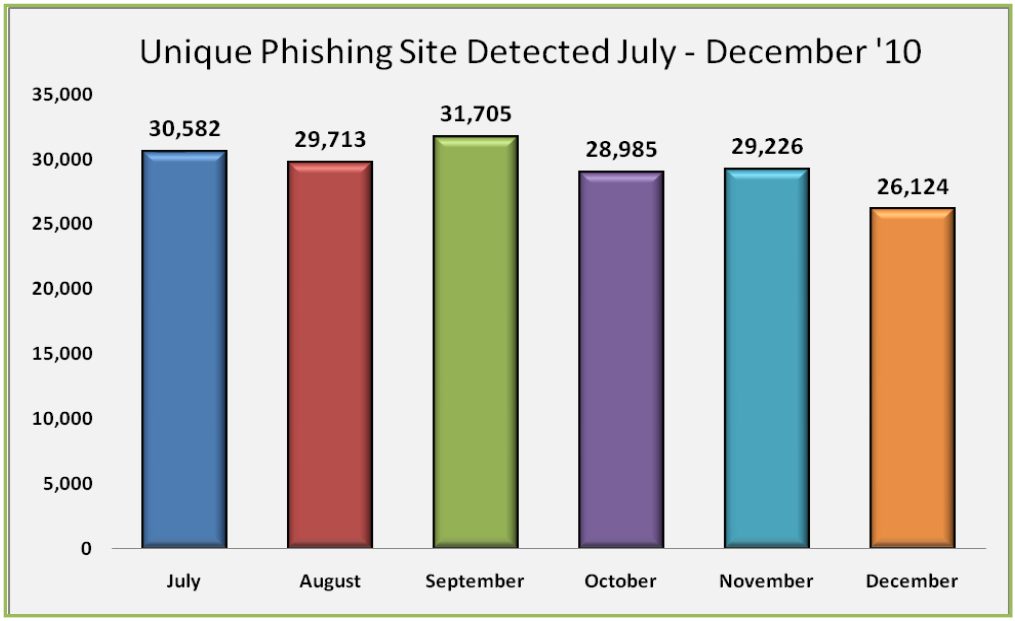
	July	Aug.	Sept.	Oct.	Nov.	Dec.
Number of unique phishing email reports received by APWG from consumers	26,353	25,273	22,188	23,619	23,017	21,020
Number of unique phishing web sites detected	30,582	29,713	31,705	28,985	29,226	26,124
Number of brands hijacked by phishing campaigns	274	301	335	317	305	279
Country hosting the most phishing websites	Sweden	Sweden	Sweden	USA	USA	USA
Contain some form of target name in URL	82.82%	95.13%	92.94%	79.93%	76.44%	75.86%
No hostname; just IP address	1.45%	0.84%	1.93%	3.89%	15.11%	3.05%
Percentage of sites not using port 80	0.12%	0.10%	0.23%	0.60%	0.43%	0.48%

Phishing Email Reports and Phishing Site Trends – 2nd Half 2010



The number of unique phishing reports submitted to APWG in the second half 2010 reflected a steady decrease after reaching a previous high for 2010 in June of 33,617. The H2, 2010 high of 26,353 in July was down 35 percent from the all-time high in August 2009 of 40,621 reports. The half-yearly low for this metric, in December, with 21,020, was down 48 percent from the all-time high.

The number of unique phishing websites detected by APWG during the second half 2010 fluctuated by more than 5,000 websites from month to month within the half year. Reaching the highest point in September with 31,705, the remaining three months saw a steady decrease down to 26,124 in December. The half-yearly high in September was down more than 44 percent from the record high of 56,362 in August 2009.

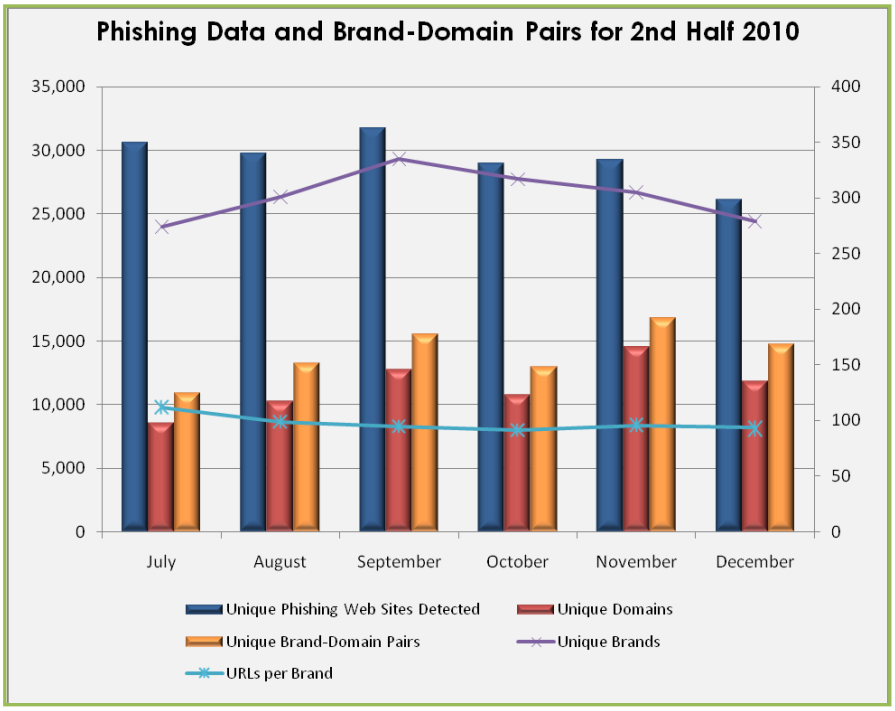


In the latter months of 2010 APWG witnessed an increase in so-called "spear-phishing" attacks in which individuals inside companies and government agencies are targeted by cybercriminals who send individualized fake emails to their victims - often with crimeware payloads - to gain access into a corporation's network by infecting the targeted employee's computer. These emails, designed to evade spam and anti-virus filters, are very effective at infecting a user's computer. This trend is accelerating in 2011, and is responsible for some high-profile corporate data breaches.

Brand-Domain Pairs Measurement – 2nd Half 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 fluctuated during the second half of 2010. The high for the half year, 16,767 brand-domain pairs in November, was down nearly 32 percent from the record of 24,438 recorded in August, 2009.



"The second half of 2010 saw a 6 percent drop in total phishing attacks from the first half. However, the number of brands targeted went up by over 7 percent and there was an increase of almost 6 percent in unique Brand-Domain pairs," said Ihab Shraim, chief security officer and vice president, network and systems engineering, MarkMonitor and *Trends Report* contributing analyst. "This data suggests that phishers are utilizing more targeted tactics in order to achieve a better ROI on their phishing campaigns."

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.

	July	Aug.	Sept.	Oct.	Nov.	Dec.
Number of Unique Phishing Web Sites Detected	30,582	29,713	31,705	28,985	29,226	26,124
Unique Domains	8,565	10,255	12,753	10,734	14,509	11,803
Unique Brand-Domain Pairs	10,917	13,220	15,487	12,974	16,767	14,753
Unique Brands	274	301	335	317	305	279
URLs Per Brand	111.61	98.71	94.64	91.43	95.82	93.64

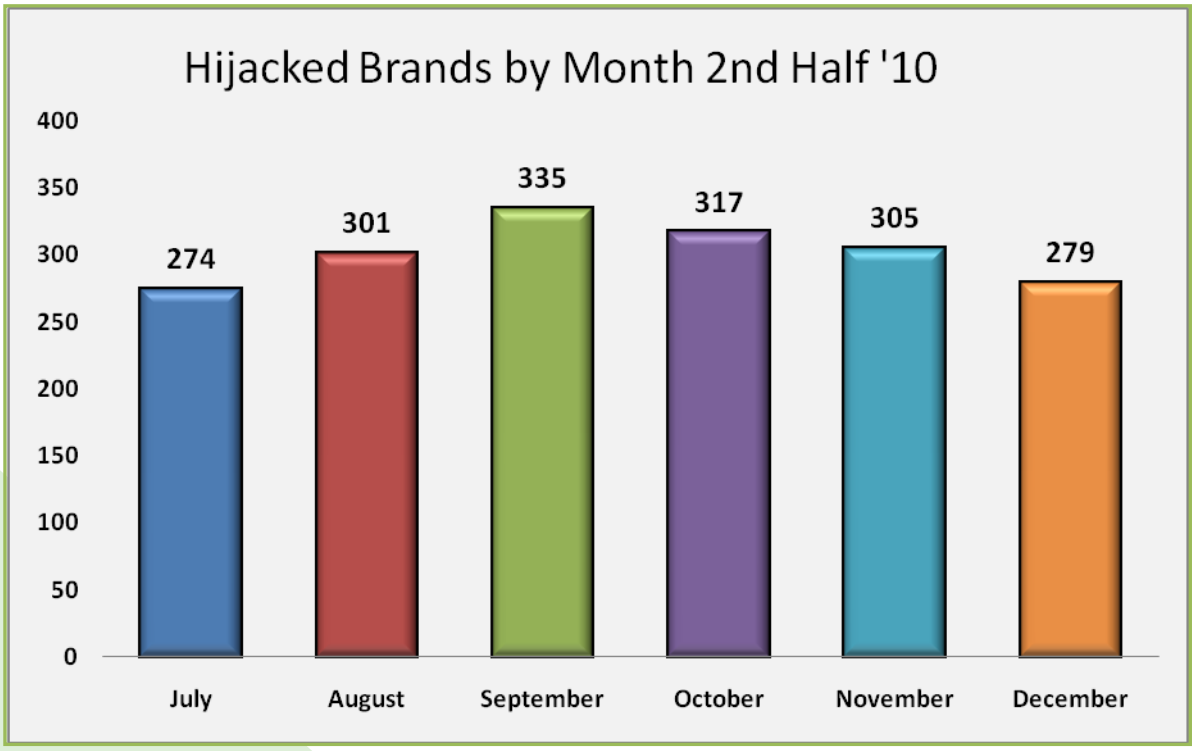
Most Used Ports Hosting Phishing Data Collection Servers – 2nd Half 2010

The second half 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.

July		August		September		October		November		December	
Port 80	99.882%	Port 80	99.902%	Port 80	99.771%	Port 80	99.402%	Port 80	99.579%	Port 80	99.525%
Port 443	.090%	Port 443	.076%	Port 443	.139%	Port 443	.475%	Port 443	.395%	Port 443	.470%
Port 21	.027%	Port 21	.020%	Port 21	.089%	Port 21	.122%	Port 21	.024%	Port 21	.004%

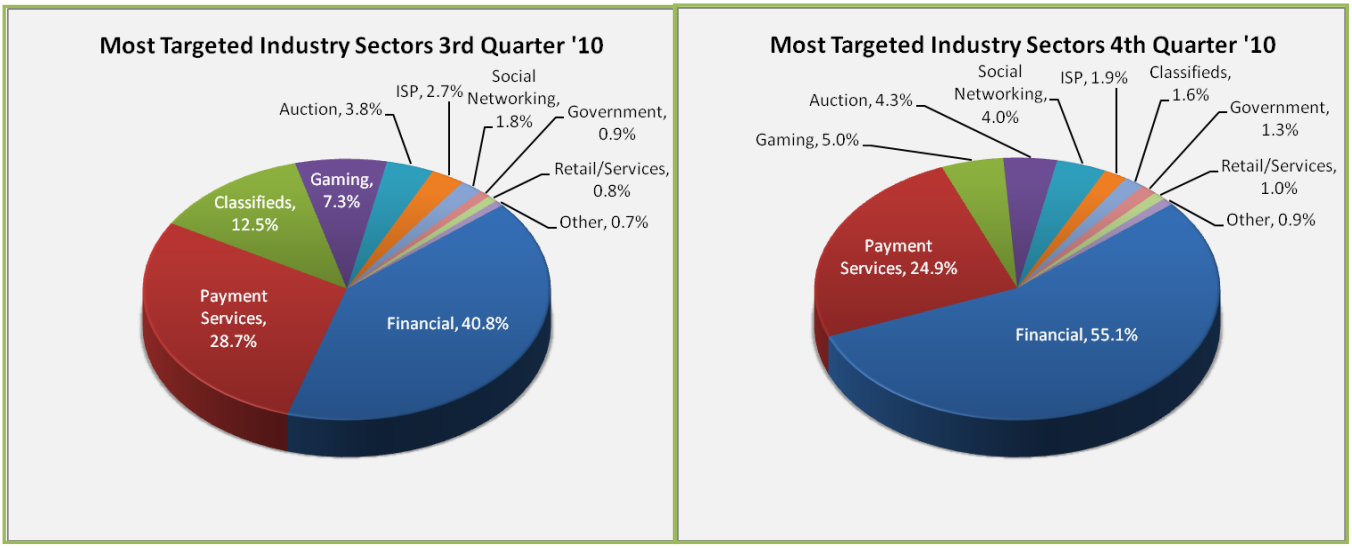
Brands and Legitimate Entities Hijacked by Email Phishing Attacks – 2nd Half 2010

The second half of 2010 saw a high of 335 in September during the six month period, a decrease of 6 percent from the all-time high of 356 reached in October, 2009.



Most Targeted Industry Sectors – 2nd Half 2010

Financial Services again became the most targeted industry sector in Q3 and Q4 of 2010, after being eclipsed by Payment Services in Q2, 2010. Classifieds, following a trend from Q2, 2010 saw a large uptick in Q3 surging to more than 12 percent of attacks, before falling back off in Q4 to less than 2 percent.



Countries Hosting Phishing Sites – 2nd Half 2010

Sweden rose to the top of countries hosting phishing sites during Q3, 2010, with a proportionally commanding 83.12 percent of all hosting sites reported in August, 2010. The United States saw itself back in familiar ground in the 2nd half of 2010 as the top country hosting phishing sites.

July		August		September		October		November		December	
Sweden	53.64%	Sweden	83.12%	Sweden	65.06%	USA	52.42%	USA	52.06%	USA	62.00%
USA	30.71%	USA	9.10%	USA	20.89%	Germany	4.74%	Ireland	11.89%	Canada	7.52%
Italy	2.32%	Canada	0.88%	Canada	1.57%	UK	4.00%	Egypt	5.67%	Egypt	4.11%
Germany	2.15%	Ireland	0.66%	UK	1.47%	Canada	3.60%	Germany	3.69%	UK	3.20%
UK	1.24%	France	0.63%	Germany	1.30%	France	3.29%	Canada	3.53%	Germany	2.94%
Canada	1.16%	Germany	0.61%	France	1.22%	Egypt	3.19%	UK	3.13%	Netherlands	2.43%
France	0.95%	UK	0.55%	Netherlands	0.65%	Bulgaria	3.11%	Hong Kong	2.37%	Rep. Korea	1.75%
Rep.	0.69%	Netherlands	0.41%	Rep. Korea	0.58%	Netherlands	2.70%	Netherlands	1.99%	China	1.36%
China	0.65%	China	0.39%	Russia	0.57%	Russia	1.73%	France	1.53%	Philippines	1.34%
Brazil	0.54%	Russia	0.36%	China	0.55%	China	1.54%	Philippines	1.27%	Hong Kong	1.24%

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.

Top 50 Malware Infected Countries – 2nd Half 2010

From July to December 2010, PandaLabs has registered 10,425,663 new malware samples. With a total malware collection of 60 million, the 2nd half of 2010 produced 17 percent of all malware variants recorded at the lab since it began collecting in 1990. This figure reflects the total number of different malware samples that appeared during this period. (It is important to note cybercriminals commonly obfuscate and re-use the same samples over and over, employing polymorphism - server side or binary side – subsequently increasing numbers of variants recorded.)

According to Luis Corrons, PandaLabs Technical Director and APWG *Trends Report* contributing analyst, 55 percent of the new samples created in the 2nd half of 2010 are Trojans, the favorite weapon used by cybercriminals to infect consumers' computers. However, the number of malware samples doesn't reflect the infection levels. The overall infection rate for computers scanned by PandaLabs in this period is 50.33 percent. But the percentage of infections varies greatly depending on the country.

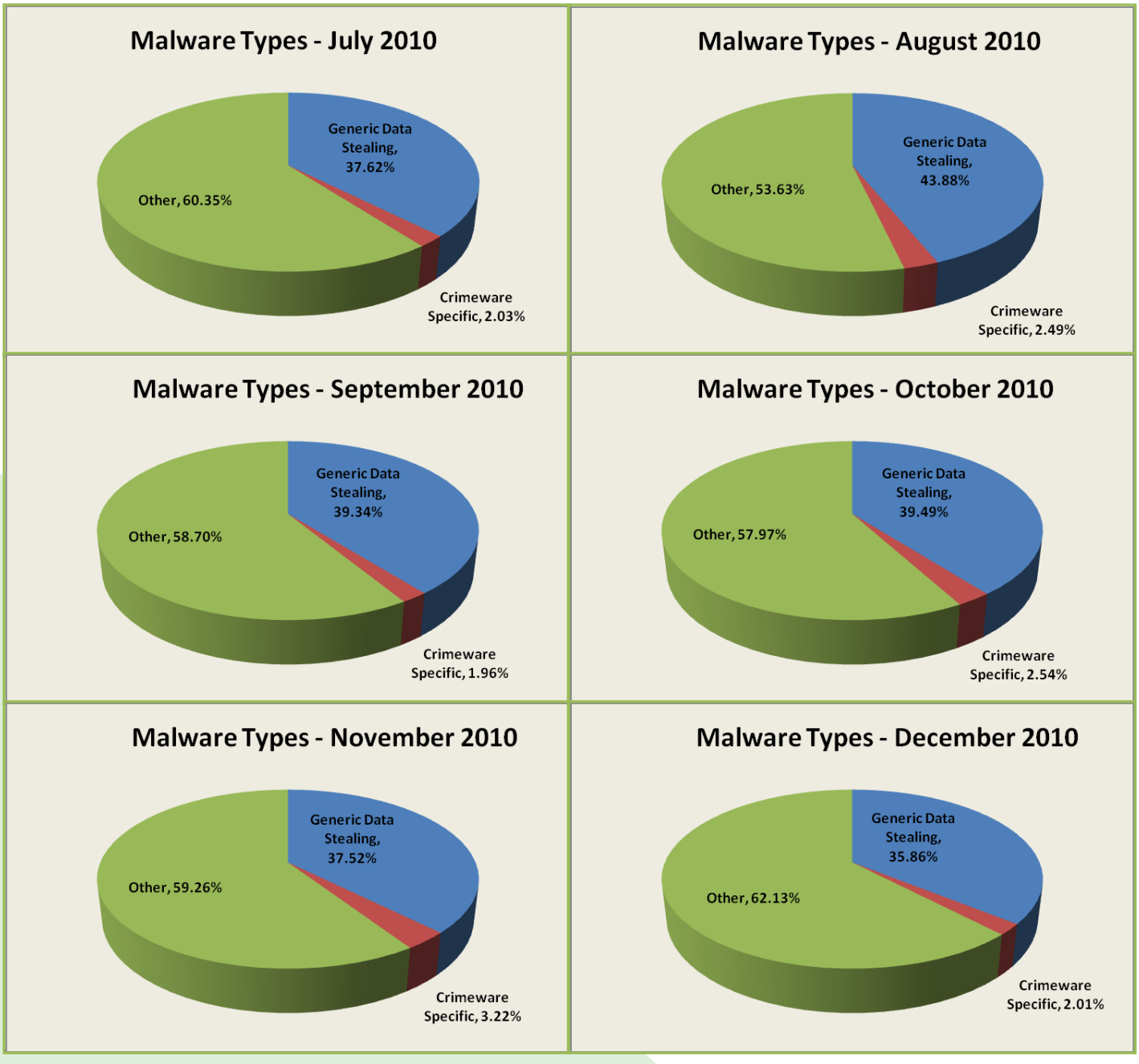
Ranking	Country	Infection ratio
1	Thailand	66.97%
2	China	62.82%
3	Taiwan	59.90%
4	Latvia	55.75%
5	Saudi Arabia	55.42%
6	Russian Federation	54.32%
7	Israel	53.30%
8	Lithuania	53.22%
9	Turkey	51.55%
10	Poland	50.35%
11	Slovenia	49.97%
12	Brazil	49.81%
13	Argentina	49.74%
14	Spain	49.62%
15	Italy	48.23%
16	France	47.54%
17	Ecuador	47.37%
18	Panama	47.19%
19	Colombia	46.78%
20	Chile	46.67%
21	Peru	45.41%
22	United States	45.32%
23	Costa Rica	45.29%
24	Estonia	45.20%
25	Venezuela	45.12%

Ranking	Country	Infection ratio
26	Uruguay	44.48%
27	Honduras	44.47%
28	South Korea	44.08%
29	Hungary	42.99%
30	Belgium	42.93%
31	Guatemala	42.86%
32	El Salvador	42.62%
33	Slovakia	42.61%
34	Austria	42.58%
35	Czech Republic	41.82%
36	Australia	41.21%
37	Ireland	41.10%
38	Finland	40.74%
39	Netherlands	40.45%
40	Canada	40.32%
41	Mexico	40.16%
42	United Kingdom	40.07%
43	Germany	39.89%
44	Denmark	38.90%
45	Portugal	37.50%
46	Greece	37.36%
47	Norway	37.20%
48	Japan	36.96%
49	Switzerland	34.60%
50	Sweden	33.68%

Measurement of Detected Crimeware – 2nd Half 2010

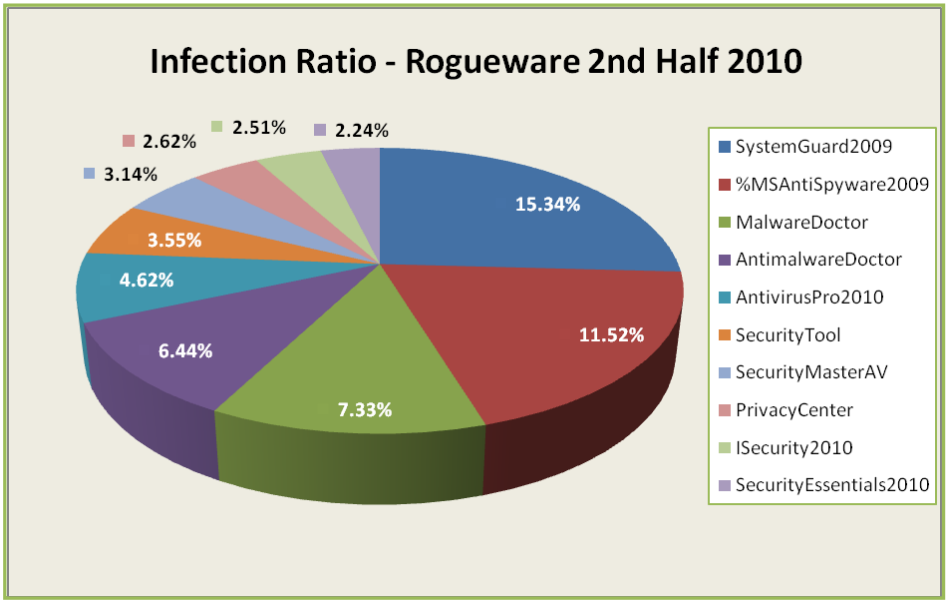
Using data contributed from APWG founding member Websense on proliferation of malevolent software, this metric measures proportions of three genera of malevolent code: *Crimeware* (data-stealing malicious code designed specifically to be used to victimize financial institutions' customers and to co-opt 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.)

"During the second half of 2010 we saw a small drop, percentage-wise, in malware aimed specifically at stealing data but an increase in the total amount of samples compared to the first half of 2010," said Patrik Runald, Senior Manager, Security Research for Websense and a *Trends Report* contributing analyst. "Downloaders are used in many of these cases and the end goal is still to steal data - but using *several* components instead of including this functionality in the main component."



Rogue Anti-Malware Programs – 2nd Half 2010

According to Luis Corrons, PandaLabs Technical Director and APWG *Trends Report* contributing analyst, during the 2nd half of 2010, a total of 169 different families have caused computer infections. However, most of the infections by rogueware programs come from a small number of crimeware families. The top 10 most prevalent families are responsible for more than 59 percent of the infections caused by rogueware, listed below in the chart and table:



Rogueware Family	
SystemGuard2009	15.34%
%MSAntiSpyware2009	11.52%
MalwareDoctor	7.33%
AntimalwareDoctor	6.44%
AntivirusPro2010	4.62%
SecurityTool	3.55%
SecurityMasterAV	3.14%
PrivacyCenter	2.62%
ISecurity2010	2.51%
SecurityEssentials2010	2.24%

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

This chart represents a breakdown of the websites which were classified during the second half 2010 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.

July		August		September		October		November		December	
USA	84.12%	USA	84.12%	USA	84.12%	USA	84.12%	USA	68.17%	USA	84.12%
China	1.57%	UK	1.57%	UK	1.57%	Canada	1.57%	Canada	3.94%	Canada	1.57%
UK	1.50%	Germany	1.50%	Germany	1.50%	UK	1.50%	UK	3.40%	UK	1.50%
Rep.	1.21%	Canada	1.21%	Canada	1.21%	Germany	1.21%	Germany	3.15%	Germany	1.21%
Germany	1.16%	France	1.16%	France	1.16%	France	1.16%	France	3.04%	France	1.16%
France	1.03%	China	1.03%	China	1.03%	China	1.03%	China	1.98%	China	1.03%
Netherlan	0.83%	Brazil	0.83%	Brazil	0.83%	Rep.	0.83%	Rep.	1.53%	Rep.	0.83%
Canada	0.74%	Australia	0.74%	Australia	0.74%	Netherlan	0.74%	Netherlan	1.44%	Netherlan	0.74%
Hong	0.72%	Netherlan	0.72%	Netherlan	0.72%	Brazil	0.72%	Brazil	1.39%	Brazil	0.72%
Italy	0.66%	Rep.	0.66%	Rep.	0.66%	Hong	0.66%	Hong	1.09%	Hong	0.66%

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 fshiver@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; and 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, research universities, multi-lateral treaty organizations and NGOs. There are more than 2,000 enterprises worldwide participating in the APWG. Because 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.apwg.org>; the Website of the 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 steering committee, its board of directors, and its executives.

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