



Phishing Activity Trends Report

**2nd Half
2011**

APWG

Unifying the
Global Response
To Cybercrime

July – December 2011

Published April 2012

Phishing Activity Trends Report, 2nd Half 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 e-mail submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation, and propagation of crimeware by 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, designed to lead consumers to counterfeit websites that 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 2 nd Half, 2011	3
Phishing E-mail Reports and Phishing Site Trends	4
Brand-Domain Pairs Measurement	5
Most Used Ports Hosting Phishing Data	
Collection Servers in 2 nd Half 2011	4
Brands & Legitimate Entities Hijacked by	
E-mail Phishing Attacks	6
Most Targeted Industry Sectors	7
Countries Hosting Phishing Sites	7
Top Malware Infected Countries	8
Measurement of Detected Crimeware	9
Phishing-based Trojans & Downloader's Host	
Countries (by IP address)	10
APWG Phishing Trends Report Contributors	11

Number of Phishing Reports Surged Though Q4 2011



The number of unique phishing reports submitted to APWG in 2H2011 climbed to 32,979 in December, but was below the all-time high. [p. 4]

2nd Half 2011 Phishing Activity Trends Summary

- Trojan malware has continued to proliferate, becoming the dominant technology of choice for e-criminals. [p. 8]
- During the second half of 2011, phishing attacks increased as the holiday season approached. There were 23 percent more phishing attacks than in the first half of 2011. [p. 5]
- Financial Services continued to be the most-targeted industry sector in the second half of 2011. [p.7]
- During the six-month period, most phishing-based Trojans were hosted in the USA. [p. 10]
- From July to December 2011, 14 million new malware samples were recorded, making a total of 26 million new malware samples in 2011. [p. 8]
- Some 39 percent of the world's PCs are infected with malware of some type. Chinese PCs are infected more frequently than anywhere in the world, while Europe has the lowest infection rate. [p. 8]

Phishing Activity Trends Report, 2nd Half 2011

Methodology and Instrumented Data Sets

The APWG continues to refine 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 (e-mail campaigns) in addition to unique phishing sites. An e-mail campaign is a unique e-mail 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 e-mails as those in a given month with the same subject line in the e-mail.

The 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 related topics.

Statistical Highlights for 2nd Half 2011

	July	Aug.	Sept.	Oct.	Nov.	Dec.
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	24,129	23,327	18,388	19,606	25,685	32,979
Number of unique phishing websites detected	32,451	35,314	34,475	36,733	44,030	48,410
Number of brands hijacked by phishing campaigns	317	316	329	311	348	362
Country hosting the most phishing websites	USA	USA	USA	USA	USA	USA
Contain some form of target name in URL	67.07%	56.15%	54.74%	66.61%	55.72%	56.94%
No hostname; just IP address	2.67%	1.06%	1.34%	1.37%	1.25%	0.92%
Percentage of sites not using port 80	0.55%	0.39%	0.42%	0.27%	0.28%	0.64%

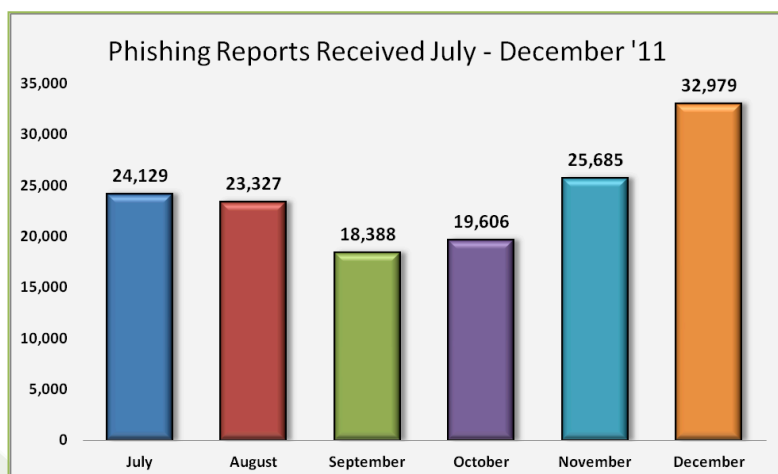
Phishing Activity Trends Report, 2nd Half 2011

Phishing E-mail Reports and Phishing Site Trends – 2nd Half 2011

Phishing attacks targeting consumers remain at high levels, with 20,000 to more than 32,000 unique phishing e-mail campaigns documented each month through the half. Each campaign can involve hundreds of thousands or millions of e-mails sent to consumers. There are hundreds of phishing websites established online every day, luring any number of consumers to trouble and loss.

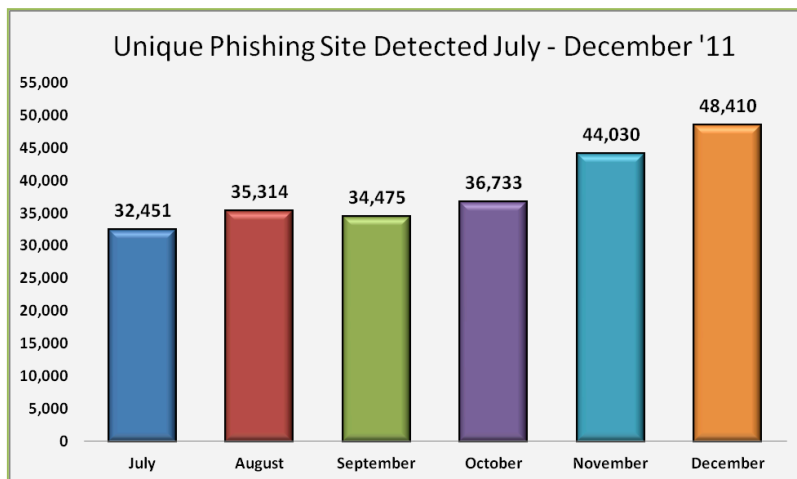
"Over the last half of 2011 there was a visible trend of phishers and scammers seeking to hide their intentions. Even fewer phishing websites are using the oh-so-obvious IP host to host their fake login pages, instead preferring to host on a compromised domain," said Carl Leonard, Websense Security Labs. "There has been a 16 percent drop in the number of phishing URLs containing the spoofed company name in the URL. These combined trends show how phishers are adapting to users becoming more informed and knowledgeable about the traits of a typical phish."

Leonard also warned consumers about mobile device use. "A great many of us use our mobile phones to check our bank account balances using the plethora of applications available. We saw malware authors seeking to exploit this in 2011, and it could turn out to be an increasingly attractive attack vector in 2012 as tablets and smartphones are adopted not just for personal use but for corporate use also," concluded Leonard.



The number of unique phishing reports submitted to APWG in 2H2011 reached a high of 32,979 in December. December's high was 19 percent lower than the all-time high of 40,621 reports, recorded in August 2009.

The number of unique phishing sites detected by APWG during 2H2011 fluctuated by more than 15,000 websites within the half year. The half-year low was 32,451 in July, ramping up to 48,410 in December. The December figure was 14 percent lower than the record high of 56,362 recorded in August 2009.

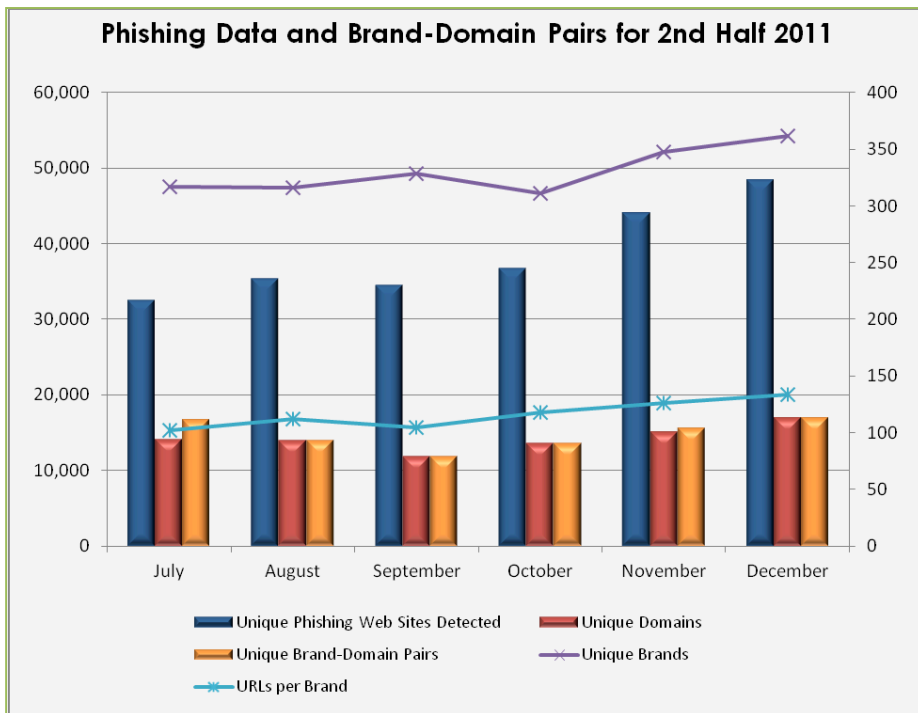


Phishing Activity Trends Report, 2nd Half 2011

Brand-Domain Pairs Measurement – 2nd 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 second half of 2011. The high for the half year, 16,650 brand-domain pairs in July, was down 32 percent from the record of 24,438 recorded in August, 2009.



“As expected, during the second half of 2011, phishing attack campaigns continued to increase as we approached the holiday season,” said Ihab Shraim, CISO and VP, AntiFraud Operations and Engineering, MarkMonitor and *Trends Report* contributing analyst. “We detected 23 percent more phishing attacks in the second half of 2011 than we saw in the first half of 2011.”

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 e-mail 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	32,451	35,314	34,475	36,733	44,030	48,410
Unique Domains	14,045	13,950	11,825	13,599	15,100	16,911
Unique Brand-Domain Pairs	16,650	13,950	11,825	13,599	15,510	16,911
Unique Brands	317	316	329	311	348	362
URLs Per Brand	102.37	111.75	104.79	118.11	126.52	133.73

Phishing Activity Trends Report, 2nd Half 2011

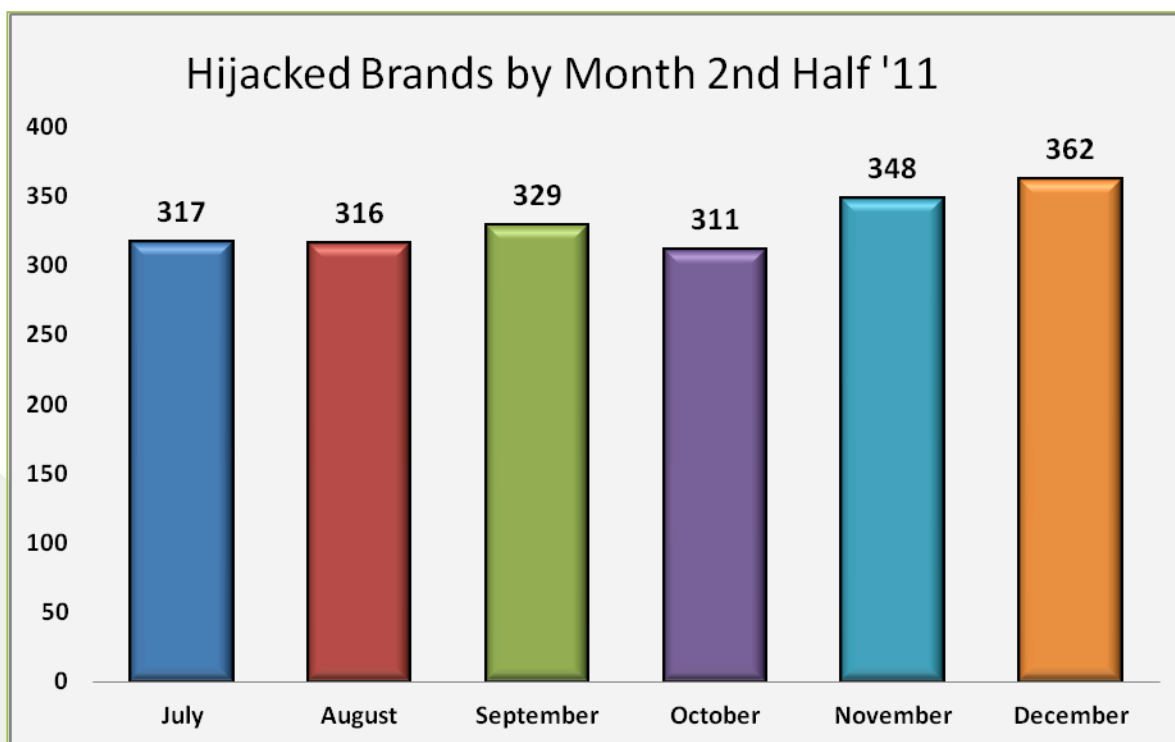
Most Used Ports Hosting Phishing Data Collection Servers – 2nd Half 2011

The second 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.

July		August		September		October		November		December	
Port 80	99.449%	Port 80	99.605%	Port 80	98.573%	Port 80	99.723%	Port 80	99.716%	Port 80	99.350%
Port 443	.551%	Port 443	.390%	Port 443	.427%	Port 443	.277%	Port 443	.284%	Port 443	.650%
		Port 21	.005%								

Brands and Legitimate Entities Hijacked by E-mail Phishing Attacks – 2nd Half 2011

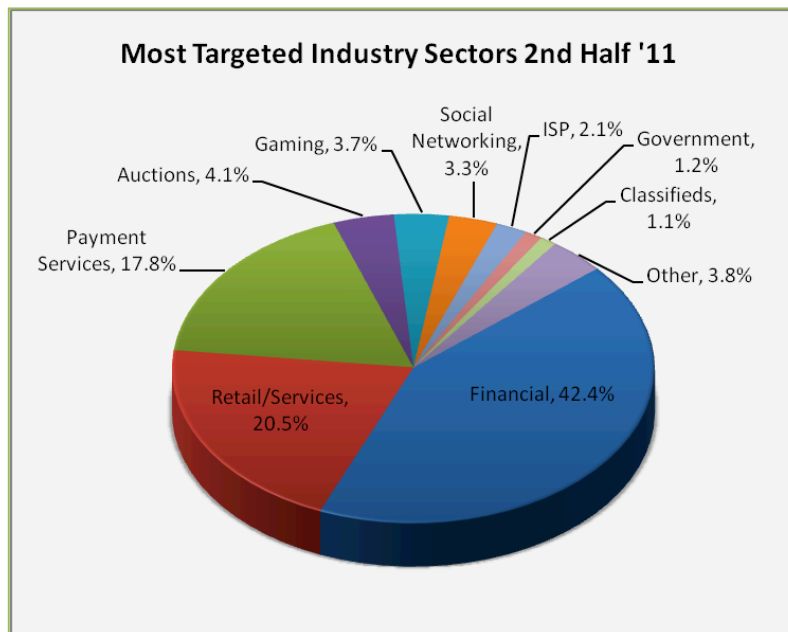
In December 2011, MarkMonitor saw an all-time high of 362 brands targeted, an increase of nearly two percent (1.7%) from the previous all-time high of 356 reached in October 2009.



Phishing Activity Trends Report, 2nd Half 2011

Most Targeted Industry Sectors – 2nd Half 2011

Financial Services continued to be the most targeted industry sector in the second half of 2011. During this six-month period, Retail/Services eclipsed Financial Services to come in as the second-highest industry sector for targeted attacks.



Countries Hosting Phishing Sites – 2nd Half 2011

The United States continued to be the top country hosting phishing sites during the second half of 2011. Egypt remained one of the top three ranking countries for five out of six months in the second half of 2011.

July		August		September		October		November		December	
USA	58.30%	USA	69.81%	USA	66.33%	USA	57.51%	USA	69.75%	USA	63.67%
Canada	7.30%	Sweden	6.38%	Canada	7.78%	Canada	12.12%	Canada	13.52%	Canada	17.96%
Egypt	5.06%	Egypt	5.53%	Egypt	7.24%	Egypt	11.17%	Germany	2.11%	Egypt	9.91%
Netherlands	3.81%	Canada	5.11%	Israel	3.18%	Israel	3.27%	Israel	1.77%	Germany	0.88%
Germany	3.48%	Rep. Korea	1.88%	Germany	2.15%	Germany	1.84%	Netherlands	1.36%	UK	0.59%
Rep. Korea	2.80%	Germany	1.58%	Netherlands	1.37%	Poland	1.84%	China	1.00%	Russia	0.57%
UK	2.28%	Netherlands	1.10%	UK	1.30%	Netherlands	1.50%	Romania	0.89%	Netherlands	0.53%
France	1.80%	UK	0.87%	China	1.11%	UK	1.10%	UK	0.88%	Rep. Korea	0.53%
Brazil	1.36%	Russia	0.67%	Romania	0.98%	Romania	0.93%	Rep. Korea	0.85%	Brazil	0.50%
Romania	1.28%	Brazil	0.66%	Czech Rep.	0.80%	France	0.58%	Poland	0.84%	France	0.43%

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 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 – 2nd Half 2011

From July to December 2011, PandaLabs has registered 14 million new malware samples, and a total of 26 million new malware samples in 2011 overall. This figure reflects the total number of different malware samples appeared on this period in terms of different files, some 73,000 strains per day. The following table describes relative proportions of the types of new malware samples identified in the last 6 months:

Type of Malware Identified	Percent
Trojans	73.31%
Virus	14.24%
Worms	8.13%
Rogueware	2.90%
Other	1.43%

According to Luis Corrons, PandaLabs Technical Director and APWG *Trends Report* contributing analyst, Trojans continued to account for most of the new threats, growing spectacularly. In 2009, Trojans made up 60 percent of all malware, whereas the percentage dropped to 56 percent in 2010. This second half of 2011 they have jumped up to 73 percent, so that nearly three out of every four new malware strains created in 2011 were Trojans. All other malware categories have lost ground with respect to Trojans, once again the weapon of choice for cyber-crooks' intrusion and data theft efforts.

The average number of malware-infected PCs across the globe stands at 39.38 percent, with the most infected country being China (57.13 percent of PCs there are infected), followed by Thailand (50.52 percent) and Taiwan (49.95 percent). As the table shows, there are high infection countries in almost every continent, but most of them are located in Asia and South America. The list of least-infected nations is topped by European countries, with the exception of Japan. Sweden came in lowest, with only a 24.58 percent of its PCs attacked by malware.

Ranking	Country	Infection Rate
1	China	57.13%
2	Thailand	50.52%
3	Taiwan	49.95%
4	Turkey	45.53%
5	Russia	43.82%
6	Costa Rica	42.05%
7	Poland	40.67%
8	Brazil	38.88%
9	Argentina	38.79%
10	Peru	38.49%

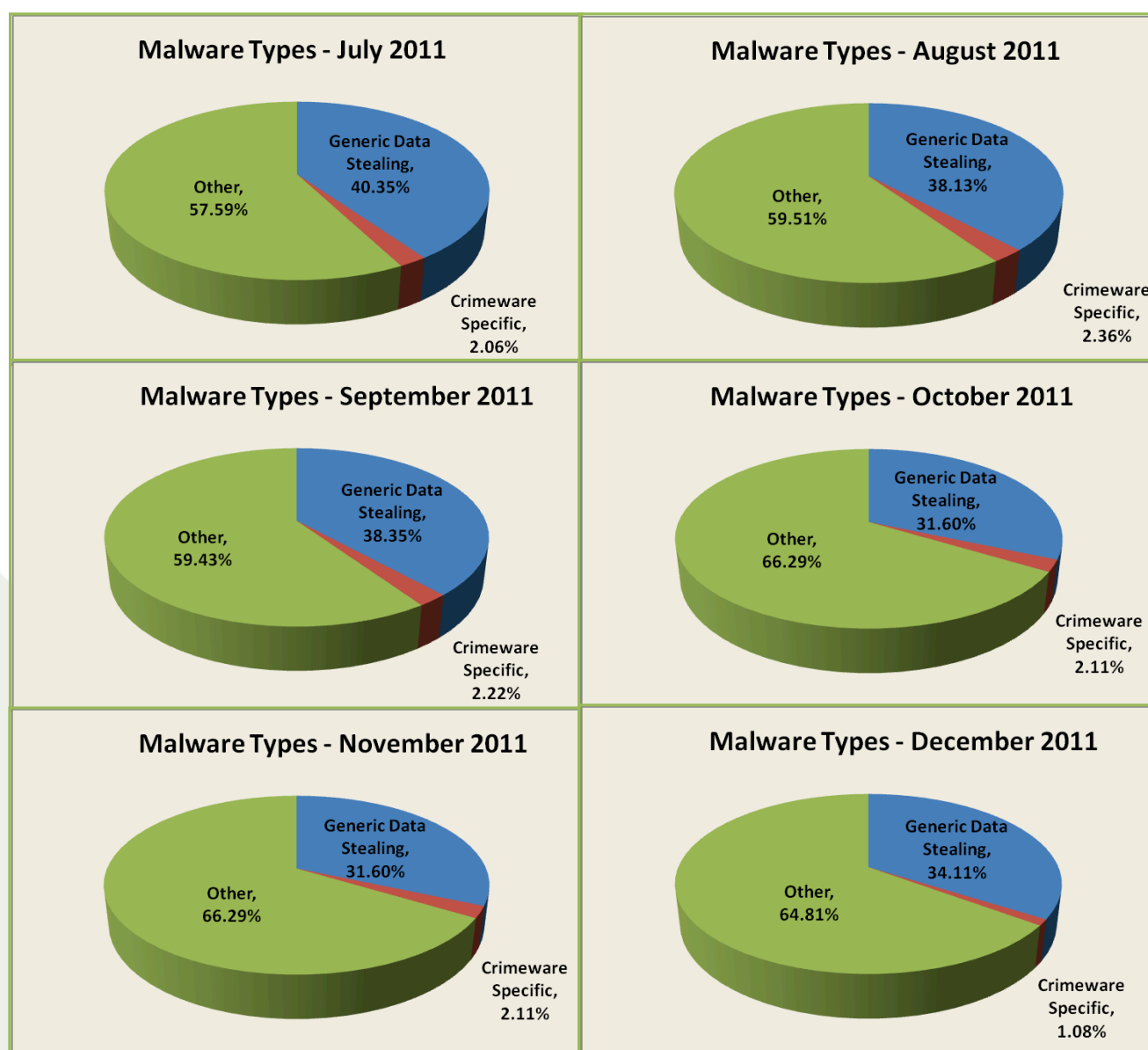
Ranking	Country	Infection ratio
41	Portugal	29.02%
42	Denmark	28.85%
43	Japan	28.63%
44	Belgium	28.60%
45	Germany	28.07%
46	United Kingdom	25.62%
47	Austria	24.46%
48	Switzerland	24.22%
49	Norway	23.86%
50	Sweden	20.58%

Phishing Activity Trends Report, 2nd Half 2011

Measurement of Detected Crimeware – 2nd Half 2011

Using data contributed from APWG founding member Websense regarding the 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 trend from the first half of 2011 continues - malware authors are out to steal data - most likely through a Trojan or drive-by download that has the capabilities to exfiltrate data or passwords from a compromised machine. Quite simply users would not know that they are being phished," said Carl Leonard of Websense Security Labs and *Trends Report* contributing analyst.



Phishing Activity Trends Report, 2nd Half 2011






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 of 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 of phishing-based Trojans, and Kazakhstan cracked the top 10 for the first time ever, in December 2011.

July		August		September		October		November		December	
USA	43.55%	USA	66.90%	USA	66.90%	USA	61.30%	USA	65.38%	USA	64.39%
Spain	17.06%	China	4.88%	Germany	4.88%	China	6.63%	Spain	7.74%	Russia	6.43%
China	6.62%	Spain	4.86%	China	4.86%	Netherlands	5.52%	Netherlands	5.10%	Canada	3.72%
Germany	4.89%	Germany	2.88%	Russia	2.88%	Russia	4.71%	Russia	4.48%	Germany	3.59%
Rep. Korea	4.53%	Russia	2.77%	Rep. Korea	2.77%	Germany	2.79%	China	4.31%	France	2.86%
Russia	4.41%	Rep. Korea	2.37%	Netherlands	2.37%	Rep. Korea	2.76%	Rep. Korea	2.42%	Netherlands	2.83%
B. Virgin. Il.	3.05%	Brazil	2.33%	Canada	2.33%	Brazil	2.32%	UK	1.53%	China	2.12%
Brazil	2.74%	B. Virgin Il.	1.90%	B. Virgin Il.	1.90%	B. Virgin Il.	2.00%	Germany	1.46%	Rep. Korea	1.76%
Canada	1.53%	UK	1.87%	UK	1.87%	France	1.97%	B. Virgin Il.	1.26%	Kazakhstan	1.37%
Netherlands	1.20%	Netherlands	1.47%	Brazil	1.47%	Canada	1.93%	Brazil	1.14%	Ukraine	1.31%

Phishing Activity Trends Report, 2nd Half 2011

APWG Phishing Activity Trends Report Contributors

 Illumintel Inc. provides advising and security services to top-level-domain registry operators and other Internet companies.	 Internet Identity (IID) is a US-based provider of technology and services that help organizations secure their Internet presence.	 MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.
 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, Inc. is a global leader in secure Web gateway, data loss prevention, and e-mail security solutions, protecting more than 43 million employees at organizations worldwide.	

The *APWG Phishing Activity Trends Report* is published by the APWG. 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 lcorrns@pandasoftware.es; or Websense at publicrelations@websense.com.

About the APWG

Founded in 2003, the Anti-Phishing Working Group (APWG) is a not-for-profit industry association focused on eliminating the identity theft and frauds that result from the growing problem of phishing, crimeware, and e-mail 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.

Statistical analysis by Greg Aaron, [Illumintel](http://www.illumintel.com); Trends Report editing by Ronnie Manning, [Mynt Public Relations](http://www.myntpublicrelations.com).