Phishing Activity Trends Report

Q2/2008

APWG

Committed to Wiping Out
Internet Scams and Fraud

April – June 2008

Phishing Report Scope

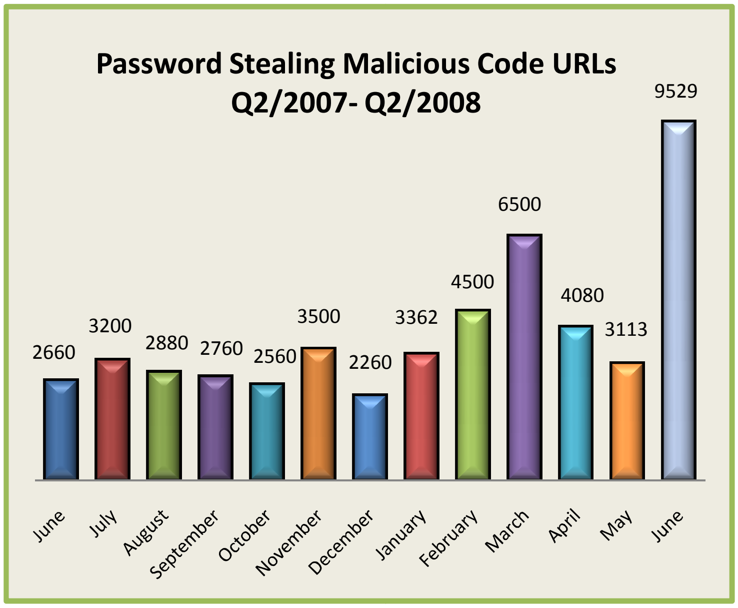
The quarterly *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, Global Research Partners, the organization's website at http://www.antiphishing.org and by email submissions to reportphishing@antiphishing.org. APWG also measures the evolution,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

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-Spreading Sites Rise Swiftly in Q2 – Highest Number Ever Recorded



The number of crimeware-spreading sites infecting PCs with password-stealing crimeware rose to a high of 9529 in June, fully 47% higher than the previous record of 6500 in March 2008 and 258% greater than the end of Q2/2008. Details on page 8.

Q2 2008 Phishing Activity Trends Summary

- Unique phishing attack reports submitted to APWG rose 13 percent during the quarter to 28,151 in June
- Unique phishing websites reported to APWG in June decreased more than 9 percent from April to 18,509
- May presented a record high of 294 hijacked brands and the quarter's 485 victimized brands is also a record high. [**Note**: reflects a change in APWG's data sample, explained on page 3.]
- The category of Other in the 'Targeted Industry Segment' measurement increased to 4 percent of the total due to attacks against social networking and national tax agencies. [**Note**: reflects a change in APWG's data sample, explained on page 3.]
- The number malicious application variants hit a record high of 442 in May
- The number of crimeware-spreading URLs exploded to a record high of 9529 at quarter's end, 258 percent higher than at the end in of Q2 2007

Methodology

APWG continues to refine and develop our tracking and reporting methodology and to incorporate new data sources into our quarterly reports. We have 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).

SPECIAL NOTE ON DATA SAMPLING: With this edition the APWG supplements the data sets utilized in establishing trend lines for the numbers of brands under phishing attack as well as the concentration of those attacks in targeted industrial sectors, incorporating phishing attack data from APWG member and phish attack data correspondent MarkMonitor. The *APWG Phishing Activity Trends Report* is incorporating specifically the company's 'Unique Brand' data and attack data delineating industry sectors targeted in those phishing attacks.

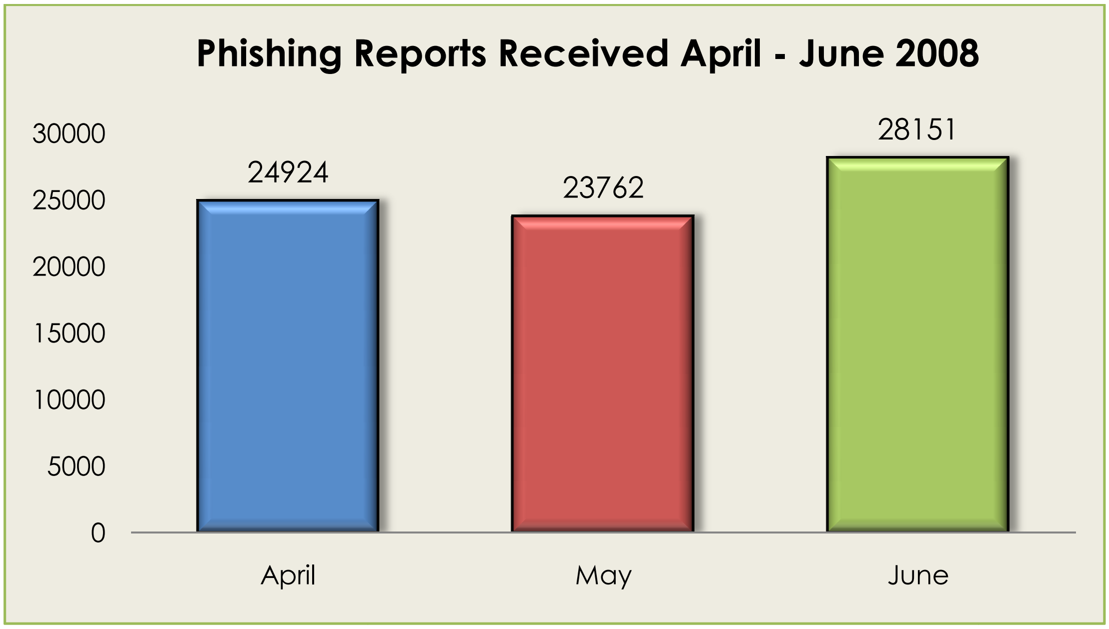
The supplemental data augments three report metrics covered in the *APWG Phishing Activity Trends Report.* Those are: 'Brands & Legitimate Entities Hijacked by Email Phishing Attacks' (Page 6), the 'Brand-Domain Pairs Measurement' (Page 5) and 'The Most Targeted Industry Sectors' (Page 7). The MarkMonitor targeted brand samples averaged around 85 percent more brands than the APWG's in 2008. The sample size is reflected in the hijacked brands measurement and the brand-domain pairs metric. The new targeted brand categorization divides the attack space into five sectors – financial services, auction services, payment services, retail and service companies and other (which includes government, charities, ISPs and unclassified brands), replacing the APWG's previous four categories of financial services, retail, ISPs and government and others.

Statistical Highlights for Q2 2008

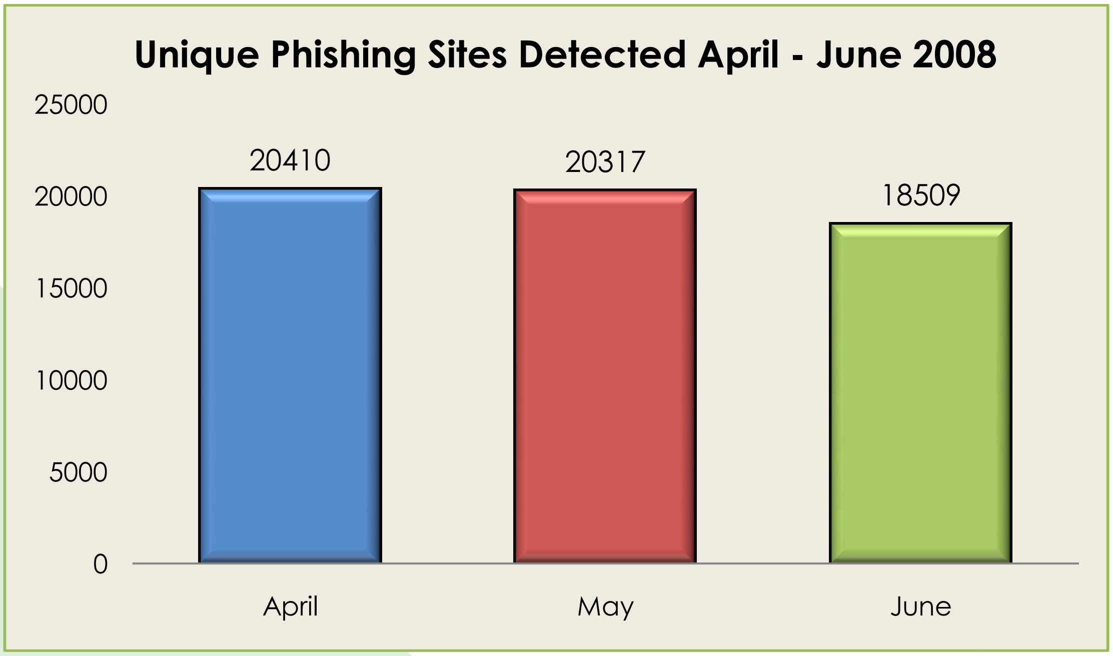
	April	May	June
Number of unique phishing email reports received by APWG from consumers	24,924	23,762	28,151
Number of unique phishing web sites detected	20,410	20,317	18,509
Number of brands hijacked by phishing campaigns	276	294	227
Country hosting the most phishing websites	China	Turkey	US
Contain some form of target name in URL	28.3%	23.2%	26.1%
No hostname; just IP address	5.5%	13.2%	4%
Percentage of sites not using port 80	.81%	.45%	.49%
Longest time online for website	30 days	31 days	30 days

Phishing Email Reports and Phishing Site Trends for Q2 2008

The number of unique phishing reports submitted to APWG in the second quarter of 2008 rose over the quarter by 13 percent ending at 28,151 in June, after declining to 23,762 in May. The number at the close of the quarter is off from the yearly high of 30,716 in February by more than 8 percent and 27 percent below the record high of 38,514 in September of 2007. This represents a count of unique phishing email reports received by the APWG.



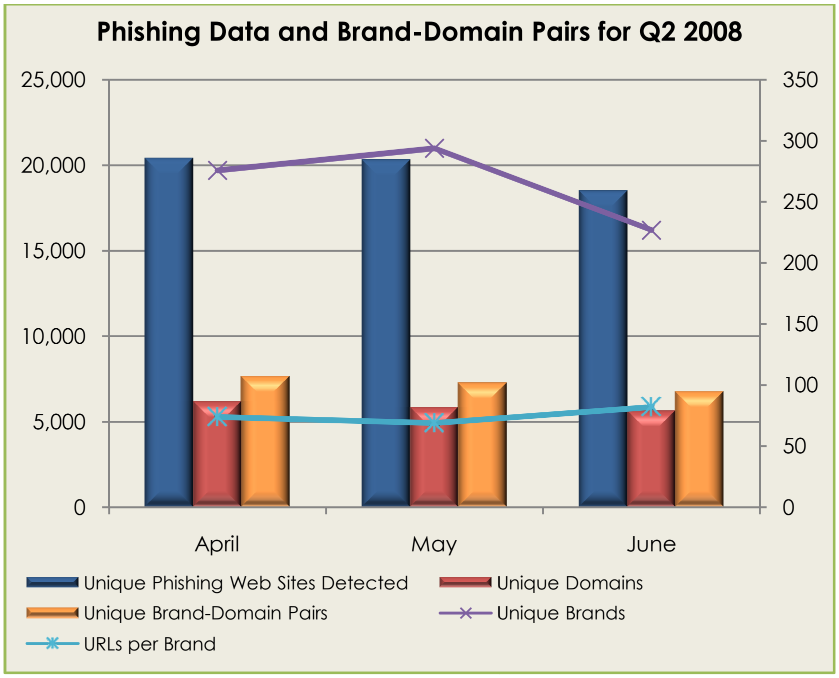
The number of unique phishing websites detected by APWG during the second quarter of 2008 saw a marginal decrease during the month of June to 18,509, a decrease of more than 9 percent from the beginning of the quarter.



Brand-Domain Pairs Measurement for Q2 2008

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. [**NOTE**: Please take note of special note on data sampling on page 3.]

Forensic utility: 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.



Unique brand-domain pairs steadily decreased during the period of April through June, from 7,656 to 6,768.

"While the number of unique Phish URL's declined in Q2, the number of brands targeted continues to rise," said Blake Hayward, Vice President of Product Marketing at MarkMonitor.

"This suggests that phishers are investing in sophisticated marketing tools and IT infrastructure in order to conduct more targeted spear phishing campaigns," Mr. Hayward said.

	April	May	June
Number of Unique Phishing Web Sites Detected	20,410	20,317	18,509
Unique Domains	6,176	5,849	5,633
Unique Brand-Domain Pairs	7,656	7,267	6,768
Unique Brands	276	294	227
URLs Per Brand	74	69	82

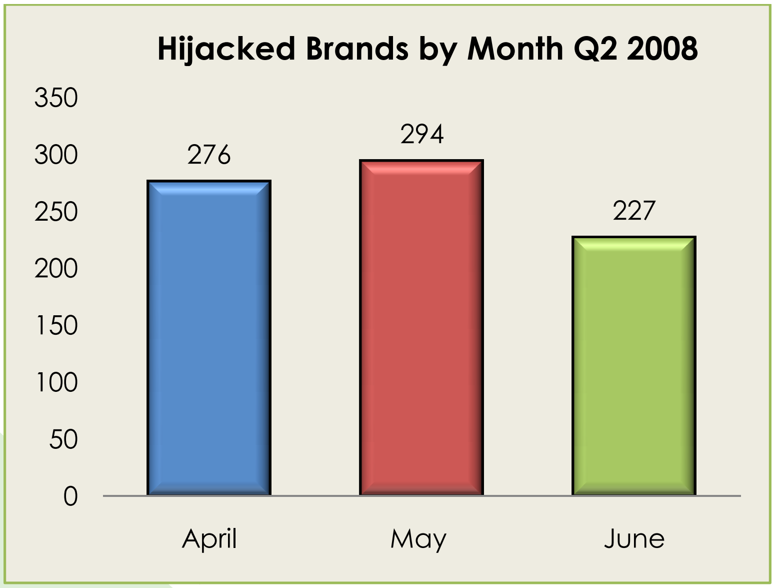
Most Used Ports Hosting Phishing Data Collection Servers in Q2 2008

The second quarter of 2008 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.

April		May		June	
Port 80	99.49%	Port 80	99.42%	Port 80	99.65%
Port 5443	.23%	Port 82	.16%	Port 443	.19%
Port 443	.22%	Port 84	.06%	Port 84	.06%
Port 8080	.06%	Port 85	.06%	Port 81	.03%
		Port 443	.06%	Port 9070	.03%
		5 other	.24%	1 other	.01%

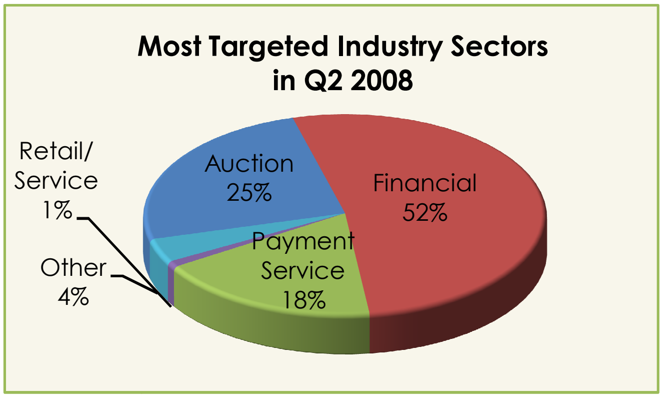
Brands and Legitimate Entities Hijacked by Email Phishing Attacks in Q2 2008

The second quarter of 2008 saw a decrease of 28 percent in hijacked brands from 276 at the beginning of the quarter to 227 brands victimized at period's end. In the data set used for this metric, May presented a record high of 294 and the quarter's 485 victimized brands is also a record high. [**NOTE**: Please take note of special note on data sampling on page 3.]



Most Targeted Industry Sectors in Q2 2008

Financial Services continues to be the most targeted industry sector during the second quarter of 2008. This is consistent with results since the APWG began tracking targeted industry sectors. The uptick in the 'Other' category is the increase in targeted attacks towards social networking sites such as MySpace and Facebook in addition to tax agencies. May and June also saw a massive increase in attacks aimed at cell phone providers and manufactures. [**NOTE**: Please take note of special note on data sampling on page 3.]



Countries Hosting Phishing Sites in Q2 2008

Turkey briefly took the top spot as the country hosting the largest number of phishing sites during the month of May. This rise is due to an ISP that was receiving extraordinarily large numbers of phishing attacks. A hacker abusing the ISP's IP space hosted a large number of fraudulent sites there. The United States remained in the top two of countries throughout the period, regaining the top spot in June. China made a quick and massive jump to the top spot in April after only rendering 3% of top countries hosting websites a month before in March.

April		May		June	
China	25.19%	Turkey	25.73%	United States	18.93%
United States	16.68%	United States	17.16%	Turkey	17.92%
Russia	8.23%	Japan	11.23%	Poland	13.56%
Poland	7.15%	China	9.17%	Greece	6.86%
Turkey	5.79%	Poland	7.41%	China	5.87%
Germany	3.97%	Russia	3.27%	Russia	4.28%
Republic of Korea	3.12%	Greece	2.11%	France	2.48%
Greece	2.61%	France	2.08%	Republic of Korea	2.38%
France	2.32%	Republic of Korea	1.60%	Bulgaria	2.28%
Romania	2.21%	Netherlands	1.60%	United Kingdom	2.16%

Crimeware Taxonomy and Samples According to Classification

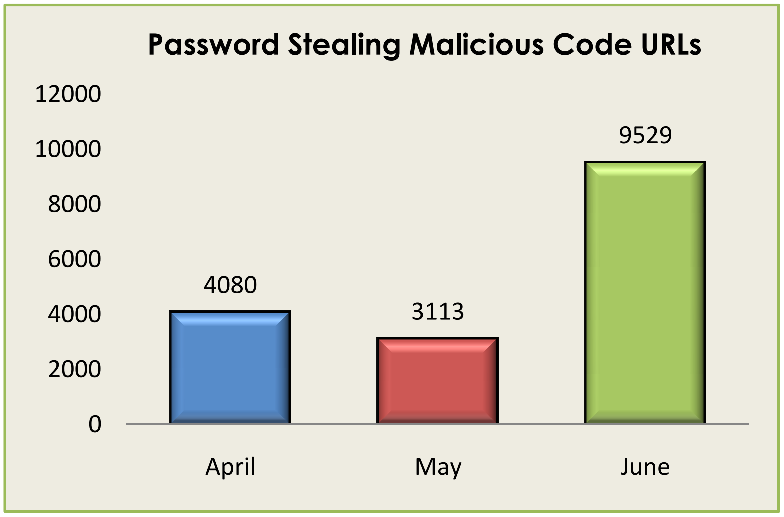
The APWG's Crimeware statistics categorizes crimeware attacks as follows, though the taxonomy will grow as variations in attack code are spawned:

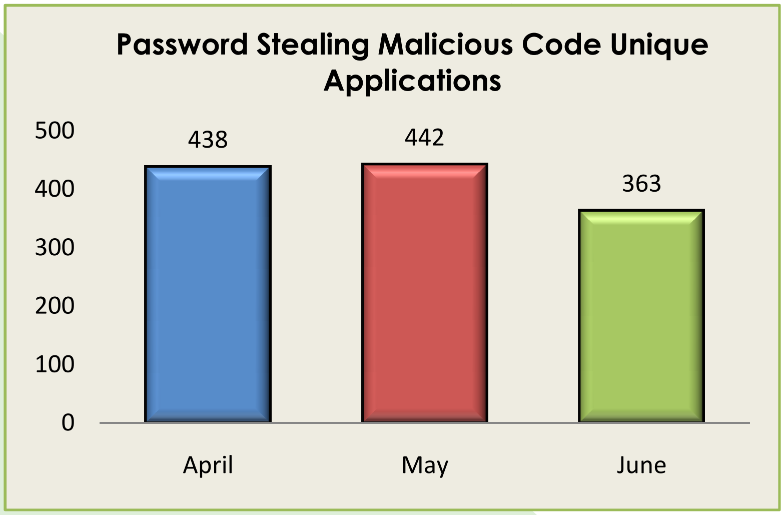
Definition: Crimeware code which is designed with the intent of collecting information on the end-user in order to steal those users' credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations, 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.

Phishing-based Trojans – Keyloggers in Q2 2008

The number of crimeware-spreading URLs detected rose from 4,080 in April to a record 9,529 in June. This rise represented an increase of nearly 47 percent from the previous record of 6,500 in March, 2008. The number at quarter's end is 258 percent higher than the end of Q2 2007.

Websense Chief Technology Officer and *APWG Phishing Activity Trends Report* contributing analyst Dan Hubbard said that the large boost is attributed mainly to malicious code being utilized in SQL injection attacks.





.

The number of unique keyloggers and crimeware-oriented malicious applications also reached an all-time high this quarter reaching 442 in May, 1 percent higher than the previous record the month before and 105 percent higher than in May 2007 when the number of crimeware variants detected was 216. Criminal hackers have apparently redoubled their efforts to develop new techniques and scripts to bypass security measures taken by consumers and enterprises – in addition to increasing the numbers of crimeware-spreading websites.

Phishing-based Trojans – Redirectors

Definition: Crimeware code which is designed with the intent of redirecting end-users' network traffic to a location where it was not intended to go to. This includes crimeware that changes hosts files and other DNS-specific information, crimeware browser-helper objects that redirect users to fraudulent sites, and crimeware that may install a network level driver or filter to redirect users to fraudulent locations. All of these must be installed with the intention of compromising information which could lead to identify theft or other credentials being taken with criminal intent.

Along with phishing-based keyloggers, we are seeing high increases in traffic redirectors. In particular, the highest volume is in malicious code which simply modifies your DNS server settings or your hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server. The fraudulent server replies with "good" answers for most domains; however, when they want to direct you to a fraudulent one, they simply modify their name server responses. This is particularly effective because the attackers can redirect any of the users requests at any time and the end-users have very little indication that this is happening as they could be typing in the address on their own and not following an email or Instant Messaging lure.

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

The chart below represents a breakdown of the websites which were classified during Q2 2008 as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger.

April		May		June	
United States	38.67%	United States	32.12%	United States	30.98%
China	9.68%	China	28.67%	China	24.95%
Russia	8.23%	Russia	6.06%	Italy	13.34%
Germany	4.10%	Brazil	4.71%	Russia	5.74%
Republic of Korea	3.81%	France	3.10%	Germany	2.56%
Canada	2.86%	Germany	2.91%	Brazil	2.45%
France	2.46%	Netherlands	2.45%	Republic of Korea	2.17%
Italy	1.96%	Republic of Korea	2.18%	France	1.99%
Romania	1.59%	Canada	1.61%	Canada	1.79%
Poland	1.52%	Italy	1.46%	United Kingdom	1.75%

Phishing Report Contributors

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

PandaLabs is an international network of research and technical support centers devoted to protecting users against malware.

Websense Security Labs' mission is to discover, investigate, and report on advanced internet threats to protect employee computing environments.

The Phishing Attack Trends Report is published quarterly by the APWG, an industry and law enforcement association focused on eliminating the identity theft and fraud that result from the growing problem of phishing, crimeware, and email spoofing. For further information, please contact APWG Deputy Secretary General Foy Shiver at 404.434.7282. For media inquiries please contact APWG Secretary General Peter Cassidy at 617.669.1123 or Cas Purdy at 858.320.9493 or cpurdy@websense.com or Te Smith at 831.818.1267 or Te.Smith@markmonitor.com. APWG thanks its contributing members, above, for 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 3,200 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.