Phishing Activity Trends Report

4th Quarter 2009

APWG

Committed to Wiping Out Internet Scams and Fraud

October – December 2009

Phishing Report Scope

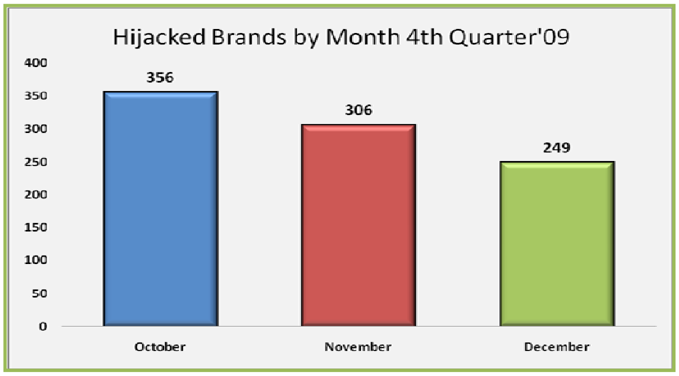
The quarterly *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.antiphishing.org and by email submissions to reportphishing@antiphishing.org. APWG also measures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

More Brands Under Attack Than Ever Before, Hitting Record High in Q4 2009



The fourth quarter of 2009 saw a rise in the number of hijacked brands to a record 356 in October, up nearly 4.4 per cent from the previous record of 341 in August 2009. [See page 6 for details.]

4th Quarter '09 Phishing Activity Trends Summary

- ● The number of unique phishing reports submitted to APWG in Q4, 2009 saw a decrease of nearly 29 percent from the all-time high of 40,621 in August, dropping to 28,897 reports in December. [p. 4]
- ● Member reports to APWG and research reviews reveal a substantial increase in phishing focused on high-value targets such as personnel with treasury authority. [p. 4]
- ● October's high of 46,522 unique phishing websites detected by the APWG was down 18 percent from the August, 2009 record high of 56,362. [p. 4]
- ● The number of unique brand-domain pairs rose to a quarter high of 23,380 in October, still down 4 percent from the all-time high of 24,438 in August, 2009. [p. 5]
- ● The United States continued its position as the top country hosting phishing sites in Q4, 2009. [p. 7]
- ● There was an increase in rogueware variations of 36 percent in Q4 (252,025), up from Q3 (158,980). [p. 9]
- ● The total number of infected computers dropped to 10,305,805 in Q4, representing more than 47.8% percent of the total sample of scanned computers, the lowest infection rate recorded in 2009. [p. 10]
- ● Similar to Q3, Financial Services remained the top of most targeted industry sectors in Q4 [p. 7]

Methodology

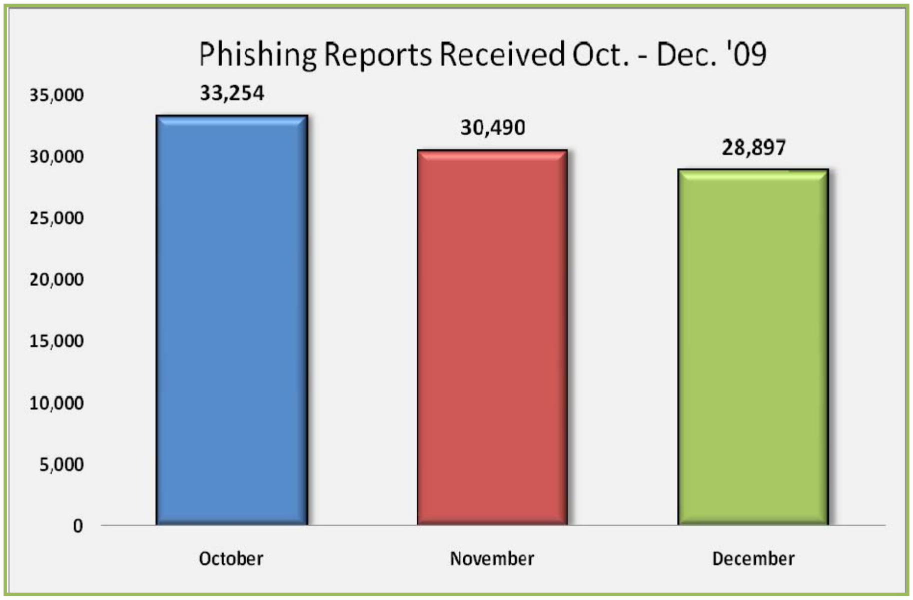
APWG continues to refine and develop its tracking and reporting methodology and to incorporate new data sources into our reports. APWG has re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent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

REPORT DEVELOPMENT NOTE: A new metric was added to the previous 1st half 2009 *Phishing Activity Trends Report* and we will continue using this statistic moving forward. Using data contributed from APWG member Websense, measuring proliferation of malevolent software, this metric measures proportions of three genera of malevolent code detected: *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); *Other* (the remainder of malicious code commonly encountered in the field such as auto-replicating worms, dialers for telephone charge-back scams, etc.) This metric replaced 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, APWG believes, provides a more precisely descriptive measure of malevolent code trends. [See page 8]

Statistical Highlights for 4th Quarter, 2009

	October	November	December
Number of unique phishing email reports received by APWG from consumers	33,254	30,490	28,897
Number of unique phishing web sites detected	46,522	44,907	46,190
Number of brands hijacked by phishing campaigns	356	306	249
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	67.49%	40.09%	42.14%
No hostname; just IP address	0.34%	.38%	1.65%
Percentage of sites not using port 80	0.03%	0.05%	0.15%

Phishing Email Reports and Phishing Site Trends – 4th Quarter 2009

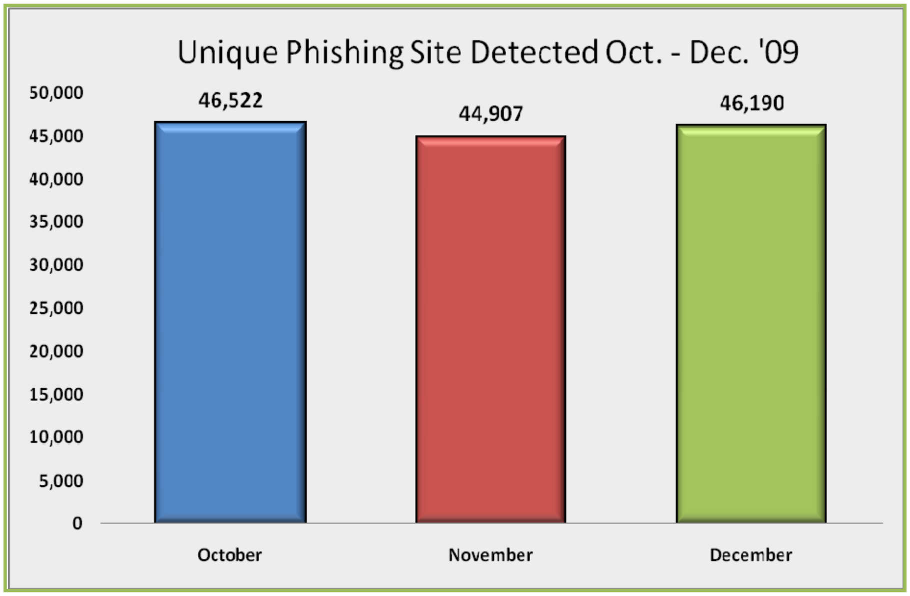


The number of unique phishing reports submitted to APWG in the Q4, 2009 saw a substantial drop off after reaching an all-time high of 40,621 in August, dropping to 28,897 reports in December, a decline of nearly 29 percent from that record high.

Member reports to APWG and research reviews in Q3 and Q4, however, reveal a substantial increase in phishing focused on high-value targets such as personnel with treasury authority.

APWG Chairman Dave Jevans said, "Spear-phishing and whale-phishing, where targeted individuals inside of corporations, or of high net worth, appears to be increasing. Phishers and malware attackers are sending emails to individuals in a highly targeted fashion, attempting to gain access to corporate online banking systems, corporate VPN networks, and other online resources.

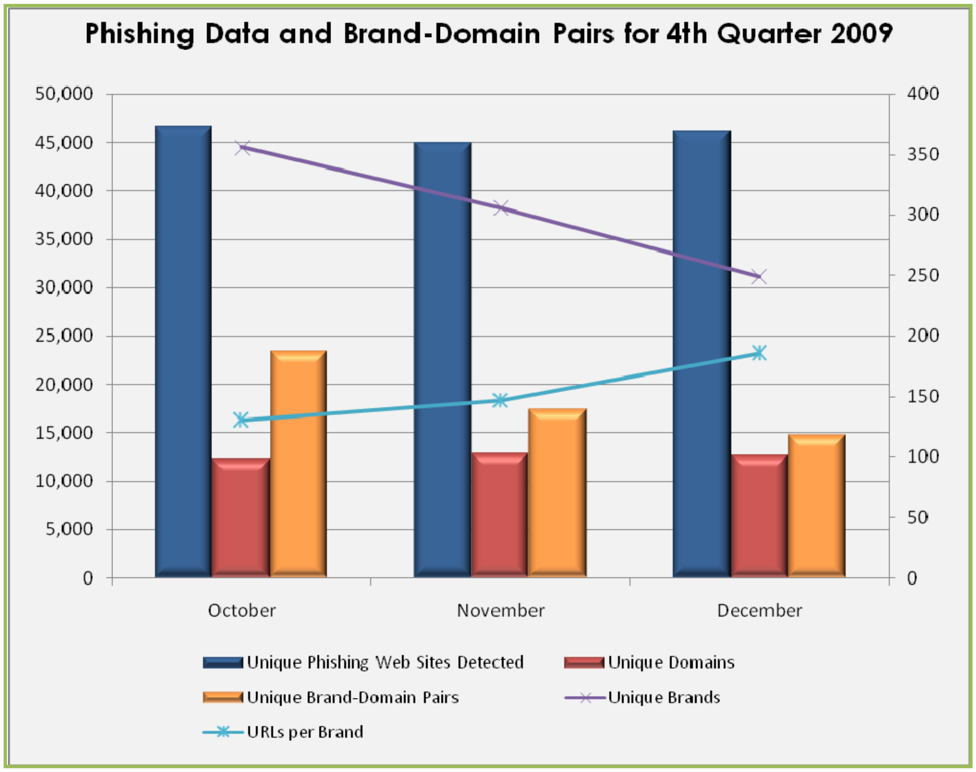
"These attacks do not contribute significantly to the overall number of unique phishing emails that are sent, as they are not using broad-based spam. Rather, the attackers customize their email messages to target individual users," Jevans said.



The number of unique phishing websites detected during the fourth quarter of 2009 remained steady, fluctuating by less than 1,300 between October and December. The quarter ended with 46,190 phishing sites detected in December, down some 18 percent from the record high of 56,362 unique phishing websites detected by the APWG in August, 2009.

Brand-Domain Pairs Measurement – 4th Quarter 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 recorded in October at 23,380 was the highest in the quarter but still represented a decline of more than four percent from the all-time high of 24,438 recorded in August of last year.



Ihab Shraim, chief security officer and vice president, network and system engineering at MarkMonitor and *Trends Report* contributing analyst said, "While phish attacks in Q4 2009, in general, continued at roughly the same rate as the previous quarter, the total number of phish attacks dropped slightly when compared with the previous period. The pattern of attacks per brand is particularly noteworthy. While the number of targeted brands declined in each month of the fourth quarter, the total number of brands targeted in phishing attacks actually increased from the previous quarter."

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.

	October	November	December
Number of Unique Phishing Web Sites Detected	46,522	44,907	46,190
Unique Domains	12,234	12,791	12,601
Unique Brand-Domain Pairs	23,380	17,408	14,729
Unique Brands	356	306	249
URLs Per Brand	130.68	146.75	185.50

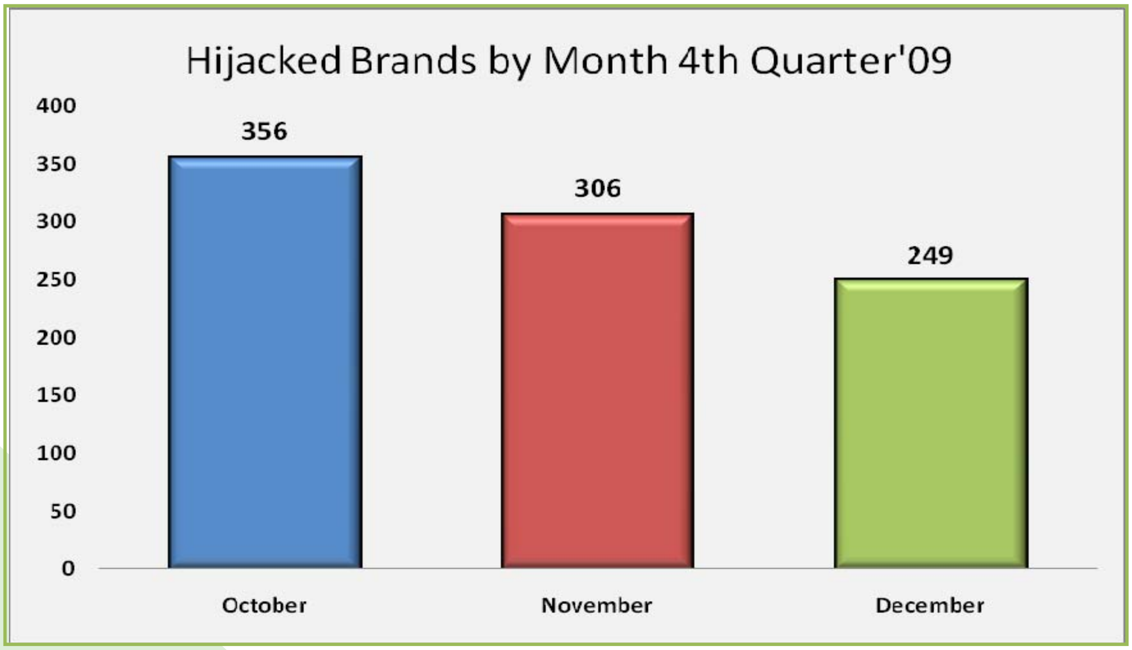
Most Used Ports Hosting Phishing Data Collection Servers – 4th Quarter 2009

The fourth quarter 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.

October		November		December	
Port 80	99.97%	Port 80	99.95%	Port 80	99.85%
Port 443	.01%	Port 21	.025%	Port 443	.07%
Port 8080	.005%	Port 443	.01%	Port 21	.04%
Port 88	.005%	Port 8080	.005%	Port 78	.01%
Port 6660	.005%	Port 32000	.005%	Port 280	.01%
Port 84	.005%	Port 8088	.005%	Port 29	.01%
				Port 9980	.005%
				Port 8081	.005%

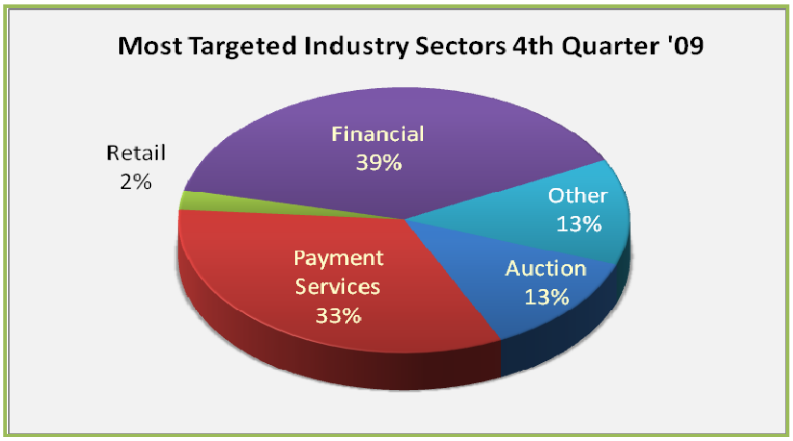
Brands and Legitimate Entities Hijacked by Email Phishing Attacks – 4th Quarter 2009

The fourth quarter of 2009 saw a rise in the number of hijacked brands to a record 356 in October, up nearly 4.4 percent from the previous record of 341 in August 2009. Phishers continue to expand their target base to attach new brands. [See MarkMonitor commentary on page 5 of this report for additional interpretation.]



Most Targeted Industry Sectors – 4th Quarter 2009

Similar to Q3, Financial Services remained the top of most targeted industry sectors in Q4. It should be noted however that earlier in the year, the Payment Services category was ranked as the most targeted industry in Q1 and Q2 of 2009. Those two quarters presented the first instances in which the Financial Services category lost the top position since APWG began tracking the proportions of phishing attacks directed at each industry sector.



Countries Hosting Phishing Sites – 4th Quarter 2009

The United States continued its position as the country hosting the most phishing sites during the fourth quarter of 2009. During the APWG H1 2009 report, Sweden reached the top spot in June but has not appeared in the top 10 after July. Patrik Runald, Senior Manager, Security Research for Websense and *APWG Phishing Trends Report* contributing analyst said, "United States continues to be the top country when it comes to hosting phishing sites although China temporarily took over the number one spot in November. We believe that China will disappear from the top 10 list due to the new paperwork requirements that CNNIC [China Internet Network Information Center, registry for the .CN Top Level Domain] introduced in December. During the first quarter of 2010 we will see the effect of this with China being replaced by other countries."

October		November		December	
USA	91.51%	USA	90.14%	USA	72.92%
Hong Kong	3.76%	Hong Kong	3.22%	China	5.24%
China	0.96%	China	1.73%	Canada	3.65%
Brazil	0.89%	Russia	1.01%	Germany	2.12%
Rep. Korea	0.47%	Rep. Korea	0.55%	Hong Kong	1.65%
Germany	0.40%	Germany	0.53%	Rep. Korea	1.47%
UK	0.29%	UK	0.28%	Russia	1.46%
Russia	0.20%	Canada	0.28%	UK	1.44%
France	0.18%	France	0.26%	Netherlands	1.23%
Canada	0.17%	Netherlands	0.17%	France	1.07%

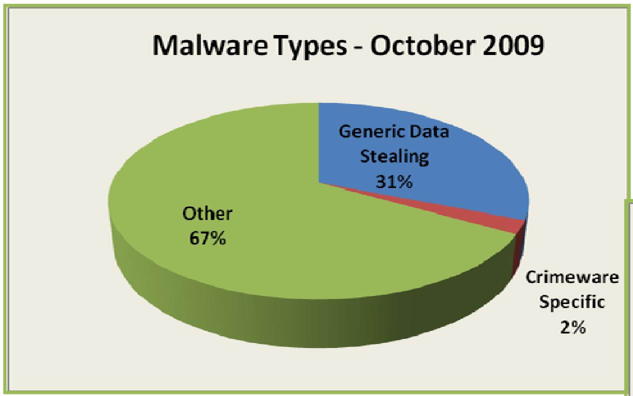
Crimeware Taxonomy and Samples According to Classification

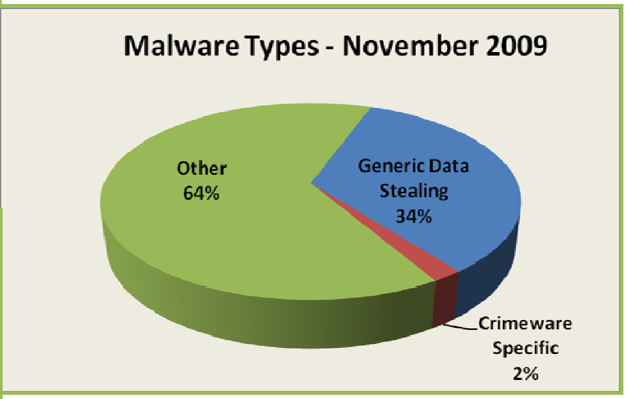
The APWG's Crimeware statistics categorize crimeware attacks as follows, though the taxonomy will grow as variations in attack code are spawned:

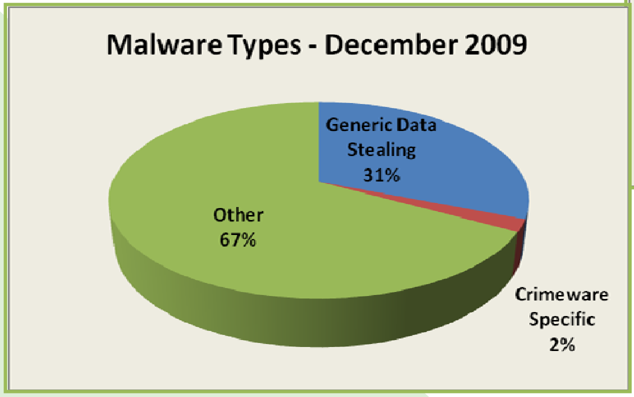
Definition: Crimeware code which is designed with the intent of collecting information on the end-user in order to steal those users' credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations,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

Measurement of Detected Crimeware – 4th Quarter 2009

The following metric has been added to the *Phishing Activity Trends Report* with this issue using data contributed from APWG member Websense, measuring proliferation of malevolent software. [See page 3 for more details on this metric.] Over the quarter, the proportion of crimeware-specific (malicious code designed specifically against financial institutions' customers) malware remained consistent, while data-stealing malware grew to 34 percent in November and settled back to the same proportion that it described at the quarter's start with 31 percent.



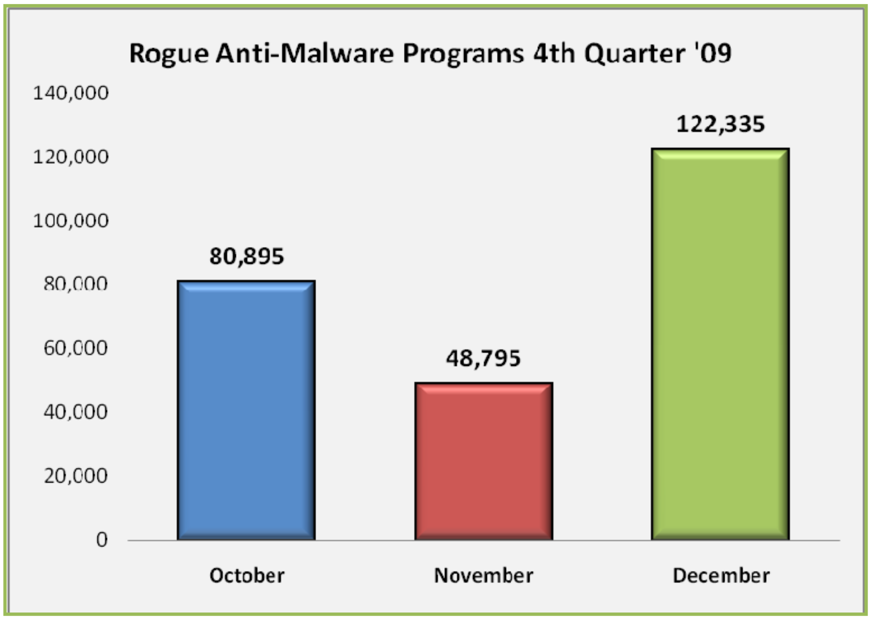




Patrik Runald, Senior Manager, Security Research for Websense and *Trends Report* Contributing analyst said, "Data stealing code continues to be an issue with over 35% of all attacks being aimed at stealing information from the user. This is due to the high success rate that hackers obtain when unleashing attacks with data stealing code. These types of attacks will most likely continue at this pace, and possibly increase as attack techniques evolve."

Rogue Anti-Malware Programs – 4th Quarter 2009

According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, there was a huge increase in the creation of rogueware variations in Q4 (252,025) compared to Q3 (158,980), a increase from quarter to quarter of 36 percent. The high for the quarter, in December with 122,335 variations recorded, is still down nearly 13 percent from the previous record high of 152,197 in June, 2009. This is mainly caused by a few rogueware families: in October, 40 percent of all the samples created belonged to the family TotalSecurity2009; and in December, a 66.85% belong to 2 different families: MSAntiSpyware2009 and Antivirus2009.



In fact, out of the 252,025 new samples in Q4, 233,965 (92.83%) belong to only four families:

- Adware/Antivirus2008
- Adware/MSAntiSpyware2009
- Adware/TotalSecurity2009
- Adware/SystemGuard2009

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

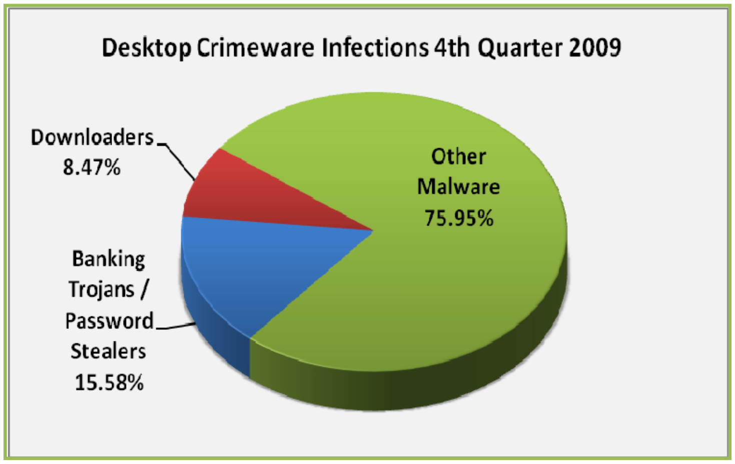
This chart represents a breakdown of the websites which were classified during the fourth quarter 2009 as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger. Similar to last quarter, in which China moved ahead of the United States during August-September, this quarter, China jumped to first place in this category during November.

October		November		December	
USA	28.18%	China	29.97%	USA	37.08%
China	26.65%	USA	28.19%	China	18.22%
Russia	11.17%	Netherlands	7.78%	Russia	4.90%
Germany	5.77%	Russia	5.78%	Spain	4.19%
Brazil	3.39%	Brazil	4.77%	Netherlands	4.18%
Sweden	2.97%	Germany	4.36%	Germany	3.06%
Netherlands	2.67%	Rep. Korea	2.70%	Brazil	3.01%
Rep. Korea	2.42%	Spain	1.97%	Jamaica	2.19%
Turkey	1.55%	Canada	1.56%	Luxembourg	2.02%
Canada	1.51%	France	1.33%	Rep. Korea	1.90%

Desktop Crimeware Infections – 4th Quarter 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.

In Q4, the proportion of infected computers has decreased from 48.35 percent in Q3 to 47.87 percent in Q4, the latter the lowest in 2009. In the same way, the proportion of banking Trojans has decreased from a 15.89 percent in Q3 to 15.58 percent in Q4. However, the proportion of downloaders has increased to 8.47 percent from 8.39 percent in Q3.



Q4: Scanned Computers	21,528,736	
Infected Computers	10,305,805	47.87%
Non Infected Computers	11,222,931	52.13%
Banking Trojans / Password	3,354,177	15.58%
Downloaders	1,823,483	8.47%

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® 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 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 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 617.669.1123 or Te Smith at MarkMonitor at 831.818.1267 or Te.Smith@markmonitor.com or Luis Corrons at Panda at lcorrons@pandasoftware.es or, for Websense, please contact publicrelations@websense.com. 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, crimeware 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 3,500 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.