Phishing Activity Trends Report

2nd Half 2008

APWG

Committed to Wiping Out Internet Scams and Fraud

July – December 2008

Phishing Activity Trends Report, 2nd Half / 2008

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.

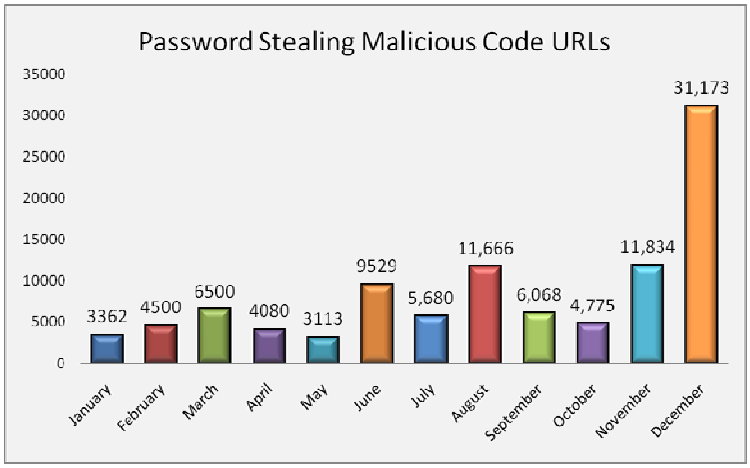
Phishing Defined

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

Statistical Highlights for 2nd Half, 2008	**3**
Phishing Email Reports and Phishing Site Trends	**4**
Brand-Domain Pairs Measurement	**5**
Most Used Ports Hosting Phishing Data Collection Servers in 2nd Half 2008	**6**
Brands & Legitimate Entities Hijacked by Email Phishing Attacks	**6**
Most Targeted Industry Sectors	**7**
Countries Hosting Phishing Sites	**7**
Phishing-based Trojans – Keyloggers	**8**
Rogue Anti-Malware Programs	**9**
Desktop Crimeware Infections	**10**
Phishing-based Trojans & Downloader's Host Countries (by IP address)	**11**
APWG Phishing Trends Report Contributors: *Websense, MarkMonitor, & Panda Security*	**12**

Year-end Number of Crimeware Sites Surges in Largest Jump Ever in Dec. 2008



The number of crimeware-spreading sites infecting PCs with password-stealing crimeware reached an all time high of 31,173 in December, an 827 percent increase from January of 2008. See details for this metric on page 8 of this report.

2nd Half 2008 Phishing Activity Trends Summary

- Unique phishing reports submitted to APWG recorded a yearly high of 34,758 in October
- Unique phishing websites detected by APWG during the second half of 2008 saw a constant increase from July with October having the high for the half at 27,739
- The number of unique keyloggers and crimeware-oriented malicious applications rose to an all-time high in July reaching 1,519
- The number of phishing attacks against payment services increased more than 34 percent between Q3 and Q4
- The Half high of 269 targeted brands in November is just 8.5 percent lower than in May's all-time high of 294
- Rogue anti-malware programs increased 225 percent from 2,850 in July to 9,287 in December
- In September, for the first time ever, Sweden briefly took the top spot as the country hosting the largest number of phishing sites

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).

REPORT DEVELOPMENT NOTE: Two new statistical sets have been added to the *Phishing Activity Trends Report*, using data contributed from APWG member Panda Labs. Those statistics measure trends in Rogue Anti-Malware Programs (fake anti-malware products that can be used for automated phishing, extortion or, most commonly up until recently, the fraudulent sale of a worthless purported anti-virus product), [See page 9] and the levels of desktop malware infection and protection as determined through Panda Labs' Scanning Vulnerability Testing program [See charts and analyses on page 10].

Statistical Highlights for 2nd Half, 2008

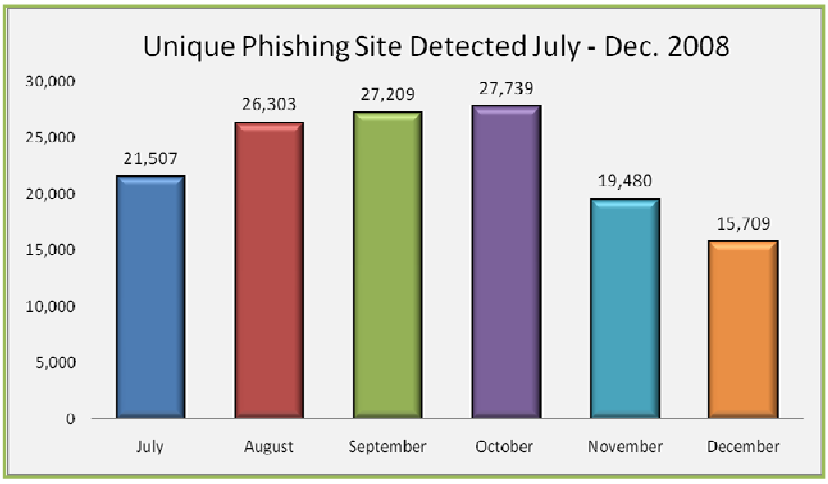
	July	Aug.	Sept.	Oct.	Nov.	Dec.
Number of unique phishing email reports received by APWG from consumers	24,007	33,928	33,261	34,758	24,357	23,187
Number of unique phishing web sites detected	21,507	26,303	27,209	27,739	19,480	15,709
Number of brands hijacked by phishing campaigns	237	231	229	264	269	252
Country hosting the most phishing websites	USA	USA	Sweden	USA	USA	USA
Contain some form of target name in URL	52.52 %	89.13%	63.18%	60.87%	16.62%	67.89%
No hostname; just IP address	5.94%	0.74%	0.29%	0.26%	1.17%	5.80%
Percentage of sites not using port 80	0.43%	0.06 %	0.01%	0.01%	0.03%	0.13%

Phishing Email Reports and Phishing Site Trends for 2nd Half 2008

The number of unique phishing reports submitted to APWG in the second half of 2008 saw a yearly high of 34,758 reached in October. However, a yearly low of 23,187 was reported only two months later in December, a decrease of 33 percent. This data set represents a count of unique phishing email reports received by the APWG.

The number of unique phishing websites detected by APWG during the second half of 2008 saw a constant increase from July – October with a high of 27,739. (That high was still down 23 percent from the 2008 high of 36,002 in February and off by 50 percent from the all-time high for this data set of 55,643 in April, 2007.)

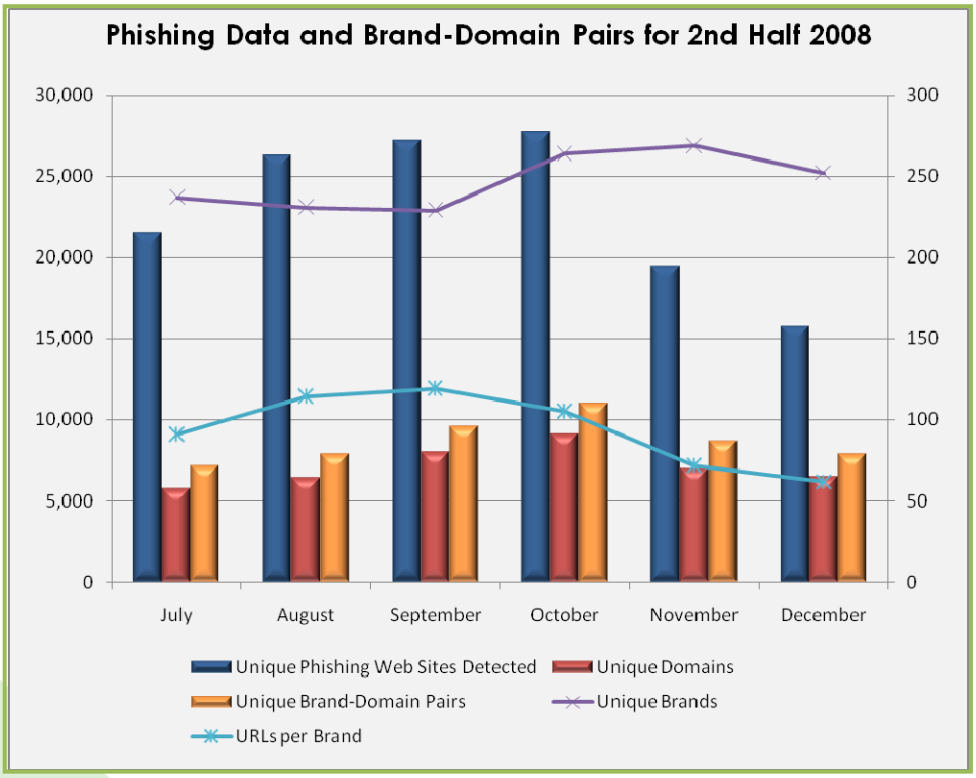
Following the trend of unique phishing reports submitted to APWG, the number of phishing sites detected also saw a drop-off during the end of the quarter to 15,709, the lowest number detected since August 2006 when it dropped to 10,091.



Brand-Domain Pairs Measurement for 2nd Half 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.

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.



The number of unique brand-domain pairs rose to a high of 11,006 in October, falling some 28 percent to 7,885 in December.

"The jump in phishing URLs from August to October can be attributed to phishers preying upon the uncertainty in the financial markets while the drop off in November and December is a seasonal trend," said Blake Hayward, Vice President, Product Marketing, MarkMonitor and *APWG Phishing Activity Trends Report* contributing analyst.

"The continued rise in targeted brands suggests that phishers are scaling their operations to conduct multi-brand attacks," concluded Hayward.

	July	Aug.	Sept.	Oct.	Nov.	Dec
Number of Unique Phishing Web Sites Detected	21,507	26,303	27,209	27,739	19,480	15,709
Unique Domains	5,740	6,412	8,020	9,112	6,931	6,448
Unique Brand-Domain Pairs	7,116	7,878	9,565	11,006	8,638	7,885
Unique Brands	237	231	229	264	269	252
URLs Per Brand	91	114	119	105	72	62

Most Used Ports Hosting Phishing Data Collection Servers in 2nd Half 2008

The second half 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.

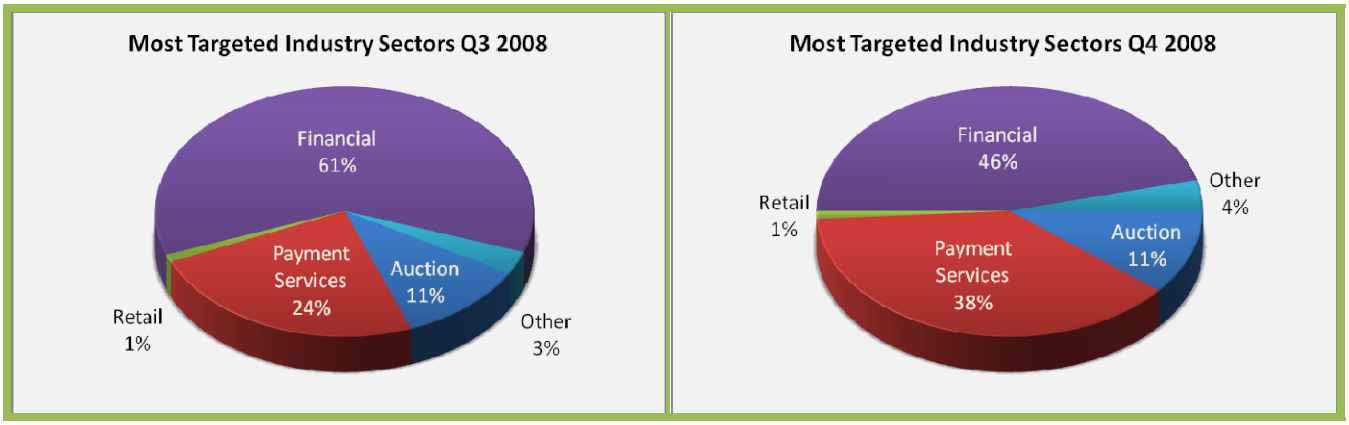
July		August		September		October		November		December	
Port 80	99.57%	Port 80	99.94%	Port 80	99.99%	Port 80	99.99%	Port 80	99.97%	Port 80	99.87%
Port 443	.29%	Port 443	.03%	Port 81	.01%	Port 8011	.01%	Port 443	.02%	Port 443	.10%
Port 1986	.07%	Port 4449	.02%					Port 8011	.01%	Port 8083	.01%
Port 84	.04%	Port 21	.01%							Port 8084	.01%
Port 21	.03%									Port 8181	.01%
Port 81	.01%										

Brands and Legitimate Entities Hijacked by Email Phishing Attacks in 2nd Half 2008

The second half of 2008 saw a fluctuation of hijacked brands ranging from a low of 229 in September to the half year high of 269 in November. In the data set used for this metric, the November high in the 2nd half was just 8.5 percent lower than in May's all-time high of 294 brands near the end of the 1st half of 2008. [See MarkMonitor commentary on page 5 of this report for interpretation.]

Most Targeted Industry Sectors in 2nd Half 2008

Financial Services continues to be the most targeted industry sector during the second half of 2008. This is consistent with results since the APWG began tracking targeted industry sectors. The continual uptick in the 'Other' category can be attributed to the increase in targeted attacks towards social media and networking sites such as MySpace and Facebook. Payment Services saw the most dramatic change with an increase of more than 34 percent in the number of e-crime attacks against this sector from Q3 to Q4.



Countries Hosting Phishing Sites in 2nd Half 2008

In September, Sweden briefly took the top spot as the country hosting the largest number of phishing sites. This rise is due to phishers using a few hosts in that particular region to mount large numbers of their phishing sites.

July		August		September		October		November		December	
USA	49.53%	USA	59.37%	Sweden	62.55%	USA	80.08%	USA	51.69%	USA	55.75%
Netherlands	11.44%	Netherlands	6.92%	USA	32.29%	Australia	6.97%	China	22.11%	China	12.32%
Russia	8.83%	Germany	6.79%	Netherlands	1.39%	China	2.65%	Australia	4.68%	Sweden	9.30%
Germany	8.69%	Russia	5.74%	Germany	0.60%	Netherlands	2.62%	Netherlands	3.91%	Germany	4.73%
France	5.35%	France	5.39%	France	0.59%	Canada	1.66%	Germany	3.44%	Canada	4.03%
UK	4.28%	UK	3.62%	Rep. Korea	0.59%	Germany	1.44%	Canada	3.35%	Rep. Korea	3.33%
Canada	3.79%	Sweden	3.30%	Japan	0.56%	Rep. Korea	1.42%	UK	3.13%	France	2.94%
Italy	2.85%	Canada	3.17%	UK	0.52%	France	1.13%	Rep. Korea	3.09%	Russia	2.88%
Rep. Korea	2.79%	China	2.90%	Spain	0.51%	UK	1.09%	Italy	2.39%	UK	2.63%
Luxembourg	2.45%	Rep. Korea	2.81%	Taiwan	0.40%	Malaysia	0.94%	France	2.21%	Netherlands	2.09%

Crimeware Taxonomy and Samples According to Classification

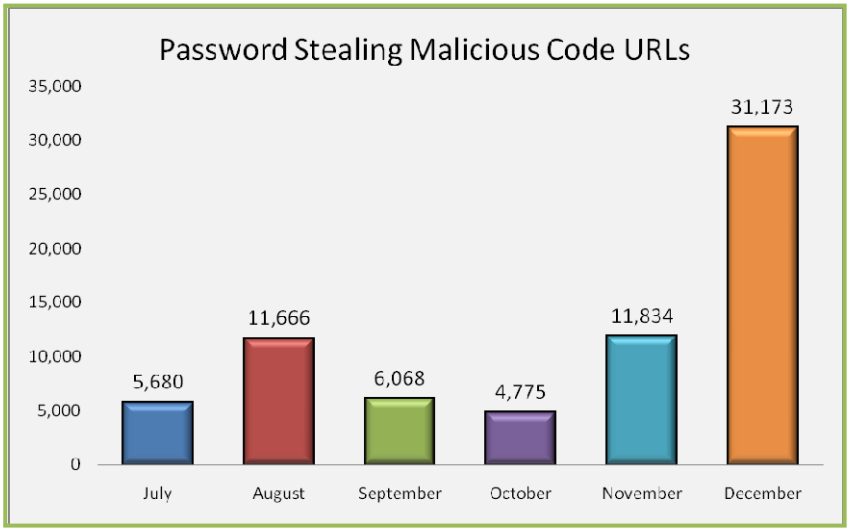
The APWG's Crimeware statistics categorize crimeware attacks as follows, though the taxonomy will grow as variations in attack code are spawned:

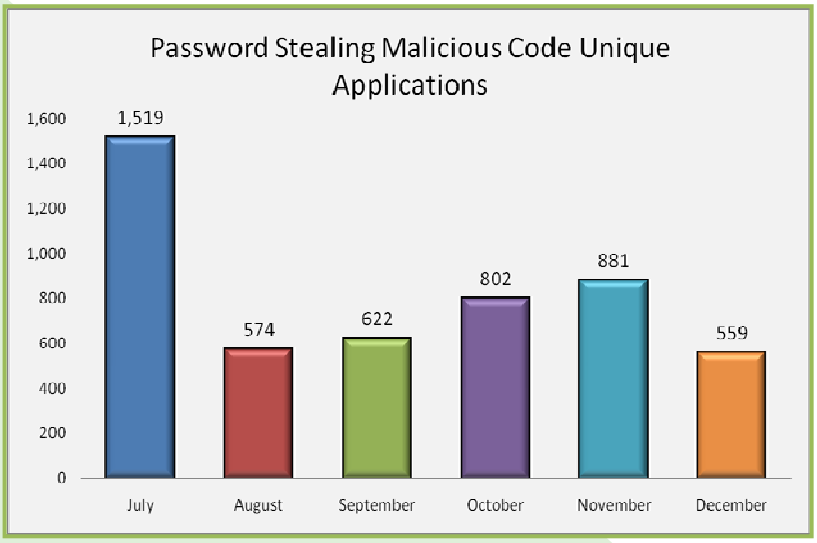
Definition: Crimeware code which is designed with the intent of collecting information on the end-user in order to steal those users' credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations,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

Phishing-based Trojans – Keyloggers in 2nd Half 2008

The number of crimeware-spreading URLs detected reached an all time high of 31,173 in December, a startling 827% increase from the beginning of 2008 in January at 3,362.

Websense Chief Technology Officer and *APWG Phishing Activity Trends Report* contributing analyst Dan Hubbard said that the major uptick of malicious code URLs was mostly due to some large attacks that were using huge amounts of random websites for phishing campaigns that were spoofing classmates' websites.





The number of unique keyloggers and crimeware-oriented malicious applications also reached an all-time high of 1,519 in July, but then quickly dropped off, leveling off to 559 in December.

Rogue Anti-Malware Programs in 2nd Half 2008

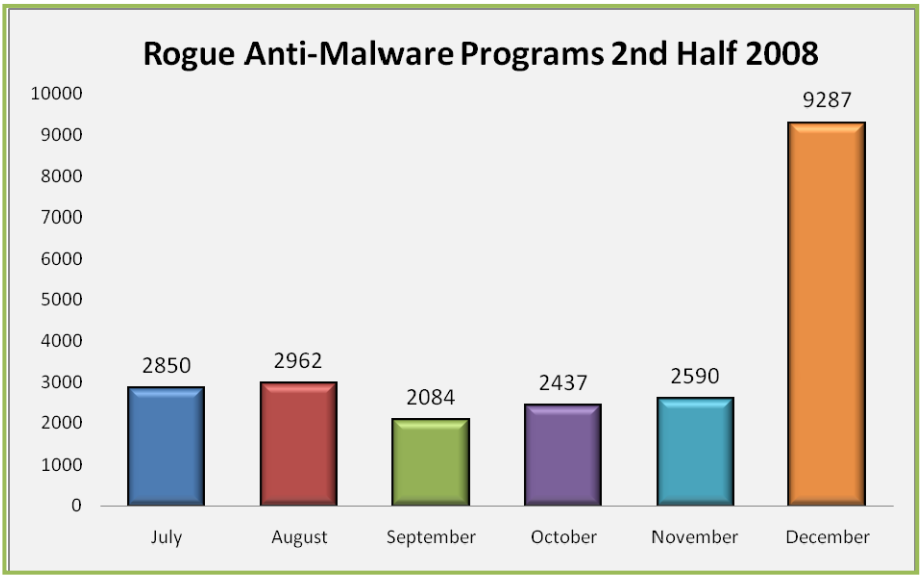
The numbers of rogue anti-malware programs rose some 225 percent from 2,850 in July to 9,287 in December, more than tripling the number of detected rogue anti-malware programs from its July level.

Two new statistical sets have been added to the *Phishing Activity Trends Report*, using data contributed from APWG member Panda Labs. Those statistics measure trends in Rogue Anti-Malware Programs (fake anti-malware products that can be used for automated phishing, extortion or, most commonly up until recently, the fraudulent sale of a worthless purported anti-virus product), [See page 9] and the levels of desktop malware infection and protection as determined through Panda Labs' Scanning Vulnerability Testing program [See charts and analyses on page 10].

According to Luis Corrons, Panda Labs' Technical Director and *APWG Phishing Activity Trends Report* contributing analyst, "Rogue anti-malware applications are not something new. They have been around for a few years. But it was not until mid-2008 when cybercriminals realized that this form of attack was a great way to obtain fresh money from users."

In order to avoid being detected and removed, cybercriminals use the same techniques they have been using for years with Trojans: in one hand they implement different techniques, such as killing AV processes and rootkits; on the other hand, they create as many variations (samples) as possible.

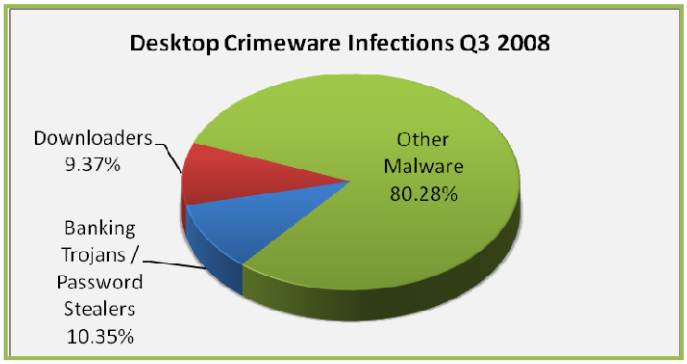
"It's war: cybercriminals vs. anti-malware companies. We've been fighting malware for 20 years, so we know what we have to do. The next step from their side is clear by taking a look at the data from December – they are trying to 'DDoS' the anti-malware labs," said Corrons.



Desktop Crimeware Infections 2nd Half 2008

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.

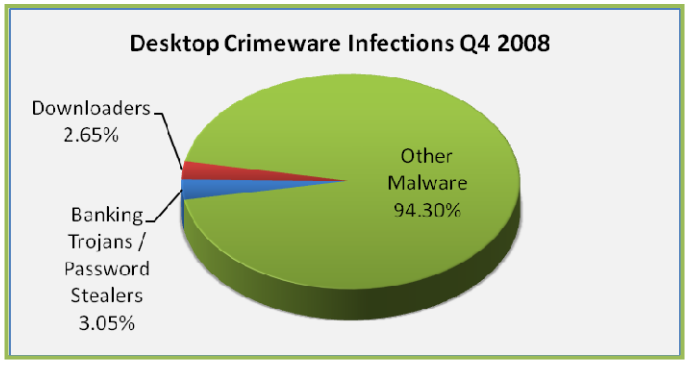
The number of infected computers detected increased from 22 percent in Q3 to 35 percent in Q4. Even though there are more computers infected as the half progressed, the percentage infected with Banking Trojans and Downloaders has decreased. The main reason for this, Panda Labs believes, is the huge increase in infections by rogue anti-malware programs in Q4.



Q3: Scanned Computers	4,141,097	
Infected Computers	917,919	22.17%
Non Infected Computers	3,223,178	77.83%
Banking Trojans / Password	94,997	10.35%
Downloaders	86,016	9.37%

One theory Panda Labs extends to explain this is that due to the financial crisis, malware authors are diversifying the ways they are obtaining income from the users. Recently, Panda Labs has observed some Wadelac and Conficker samples infecting users with these rogue anti-malware programs.

Q4: Scanned Computers	20,472,201	
Infected Computers	7,159,633	34.97%
Non Infected Computers	13,312,568	65.03%
Banking Trojans / Password	218,297	3.05%
Downloaders	189,949	2.65%



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

The chart below represents a breakdown of the websites which were classified during 2nd Half 2008 as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger.

July		August		September		October		November		December	
USA	33.92%	USA	37.42%	USA	41.03%	Brazil	31.48%	USA	33.77%	USA	32.43%
Brazil	22.26%	Russia	15.95%	Brazil	15.38%	USA	29.26%	Brazil	25.00%	China	24.77%
China	16.61%	China	15.34%	China	14.53%	China	10.37%	China	10.96%	Brazil	16.22%
Russia	9.54%	Brazil	15.34%	Portugal	7.69%	Portugal	10.37%	Portugal	6.58%	Russia	6.31%
Portugal	4.95%	France	3.68%	Russia	4.27%	Russia	8.15%	Russia	5.26%	Latvia	4.95%
France	3.89%	Portugal	3.68%	France	4.27%	Italy	2.59%	Latvia	5.26%	Rep. Korea	4.05%
Rep. Korea	2.83%	Italy	3.07%	Italy	3.42%	France	2.59%	Ukraine	4.39%	Portugal	3.60%
Germany	2.47%	Germany	1.84%	Rep. Korea	3.42%	Czech Rep.	2.22%	Italy	3.95%	Germany	2.72%
UK	2.12%	UK	1.84%	Ukraine	3.42%	Ukraine	1.85%	Netherlands	3.07%	Ukraine	2.70%
Italy	1.41%	Rep. Korea	1.84%	UK	2.56%	Rep. Korea	1.11%	Canada	1.76%	Netherlands	2.25%

APWG Phishing Activity Trends Report Contributors

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

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 Cas Purdy at 858.320.9493 or cpurdy@websense.com or Te Smith at 831.818.1267 or Te.Smith@markmonitor.com or Luis Carrons at lcorrons@pandasoftware.es. 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 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.

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