Phishing Activity Trends Report

3rd Quarter 2009

APWG

Committed to Wiping Out Internet Scams and Fraud

July – September 2009

Phishing Activity Trends Report, 3rd Quarter / 2009

Phishing Report Scope

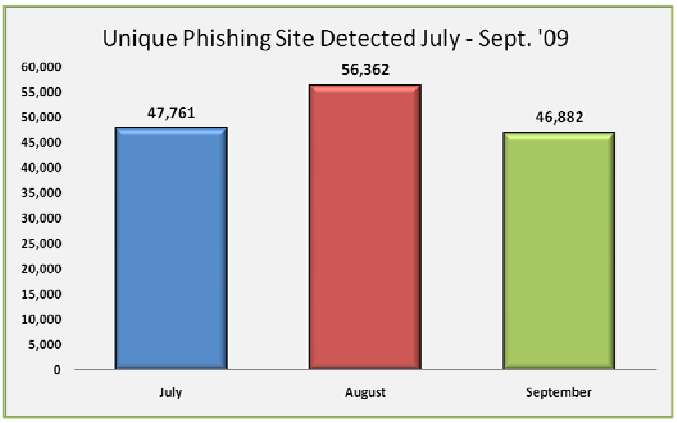
The quarterly *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.antiphishing.org and by email submissions to reportphishing@antiphishing.org. APWG also measures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

Unchecked eCrime Growth in Q3, With Record Highs in Phishing & Targeted Brands



August's 56,362 unique phishing websites is the highest number ever detected by the APWG, displacing the previous all-time high for this data set of 55,643 in April, 2007. [See page 4 for details.]

3rd Quarter '09 Phishing Activity Trends Summary

- Unique phishing reports submitted to APWG Q3, 2009 reached a record 40,621 in August, 5.5 percent more than the previous record in September, 2007. [p. 4]
- Unique phishing websites reported to APWG reached a record 56,362 in August, displacing the previous record of 55,643 by 1.3 percent in April, 2007. [p. 4]
- The number of unique brand-domain pairs rose to a record 24,438 in August, increasing more than 8 percent from the previous high of 21,085 in June 2009. [p. 5]
- The number of hijacked brands rose to a record 341 in August, up more than 10 percent from the previous record of 310 in March 2009. [p. 6]
- Financial Services rose back to the top of most targeted industry sectors in Q3 after a brief displacement by Payment Services in Q1 & Q2 of 2009. [p. 7]
- Over the quarter, the proportion of crimeware-specific (malicious code designed specifically against financial institutions' customers) malware remained consistent, while data-stealing malware rose. [p. 8]
- The number of rogueware variants fell as gangs turned to ransomware to extort money from users. [p. 9]
- The total number of infected computers dropped to 11,001,646 in Q3, representing more than 48.35 percent of the total sample of scanned computers. [p. 10]

Methodology

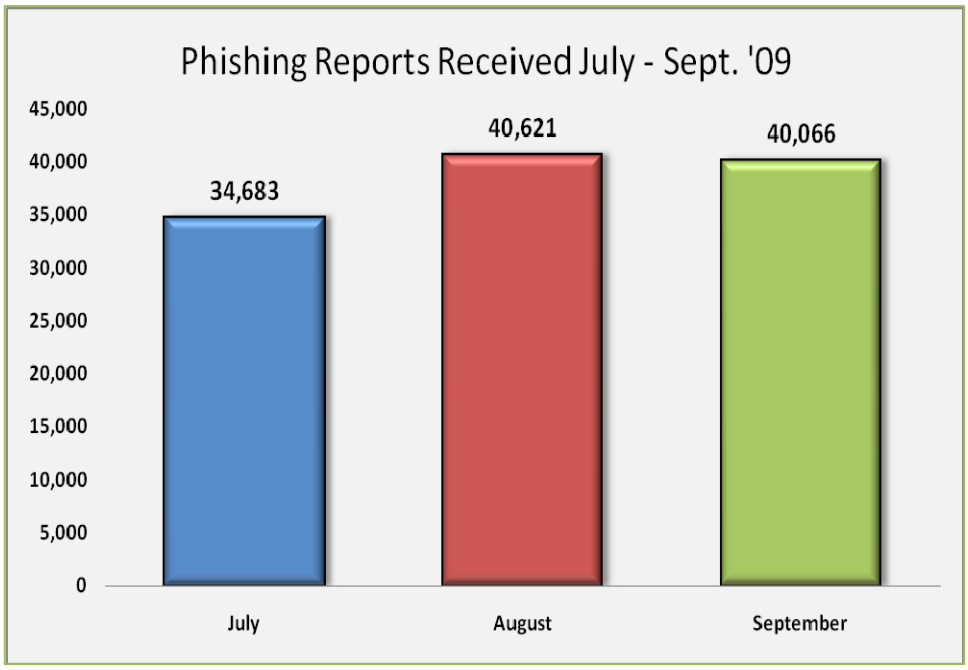
APWG continues to refine and develop its tracking and reporting methodology and to incorporate new data sources into our reports. APWG has re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent 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: 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 3rd Quarter, 2009

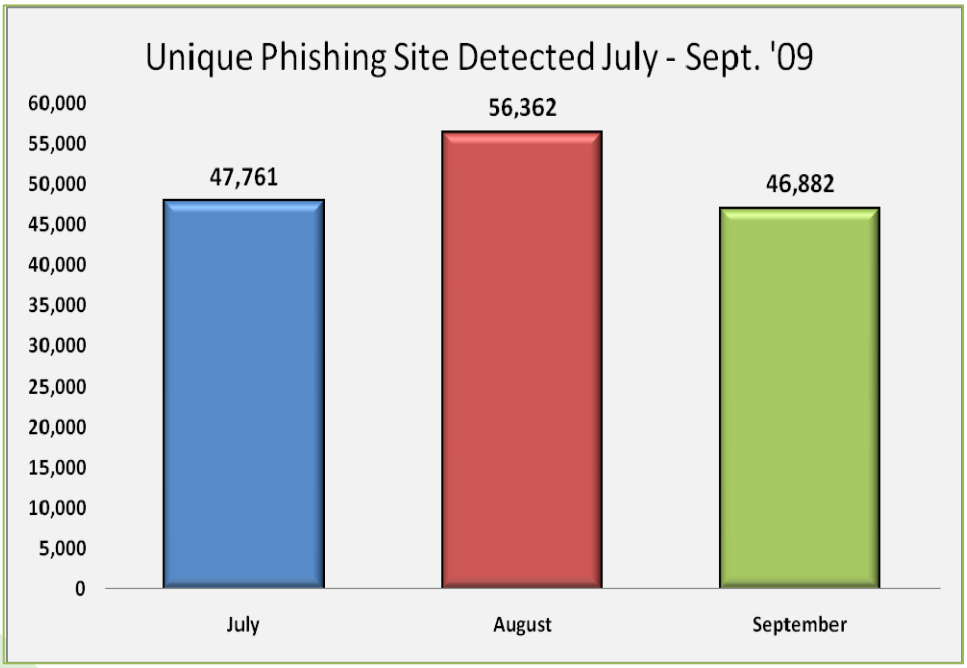
	July	August	September
Number of unique phishing email reports received by APWG from consumers	34,683	40,621	40,066
Number of unique phishing web sites detected	47,761	56,362	46,882
Number of brands hijacked by phishing campaigns	261	341	333
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	36.95%	59.37%	63.02%
No hostname; just IP address	1.17%	2.83%	1.30%
Percentage of sites not using port 80	0.05%	0.17%	0.06%

Phishing Email Reports and Phishing Site Trends – 3rd Quarter 2009



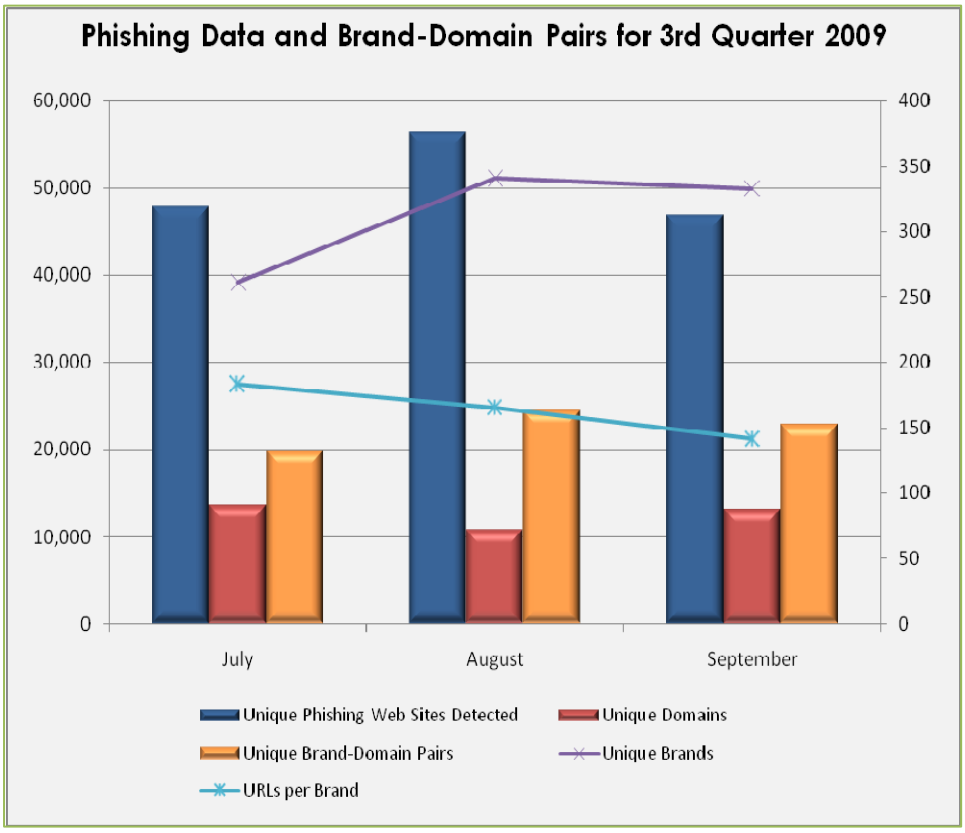
The number of unique phishing reports submitted to APWG in the third quarter of 2009 reached an all-time high of 40,621 in August, a number nearly 5.5 percent higher than the previous record high of 38,514 reported in September 2007.

The number of unique phishing websites detected by the APWG during the third quarter of 2009 reached a new record in August with 56,362, an increase of nearly 1.3 percent more than the former record high of 55,643 that was reported in April 2007.



Brand-Domain Pairs Measurement – 3rd 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 rose to an all time high of 24,438 in August, increasing more than 8 percent from the previous high of 21,085 in June 2009.

"Q3, 2009 continues the trend for record-high numbers of brand-domain pairs and near-record numbers of unique phish URLs," said Ihab Shraim, chief security officer and vice president, network and system engineering, at MarkMonitor.

"In addition, when comparing Q3 2009 to Q3 2008, we observed a 19 percent increase in unique brands being targeted and an 85 percent increase of domain names used in phish attacks."

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	August	September
Number of Unique Phishing Web Sites Detected	47,761	56,362	46,882
Unique Domains	13,494	10,806	13,087
Unique Brand-Domain Pairs	19,790	24,438	22,831
Unique Brands	261	341	333
URLs Per Brand	182.99	165.28	141.78

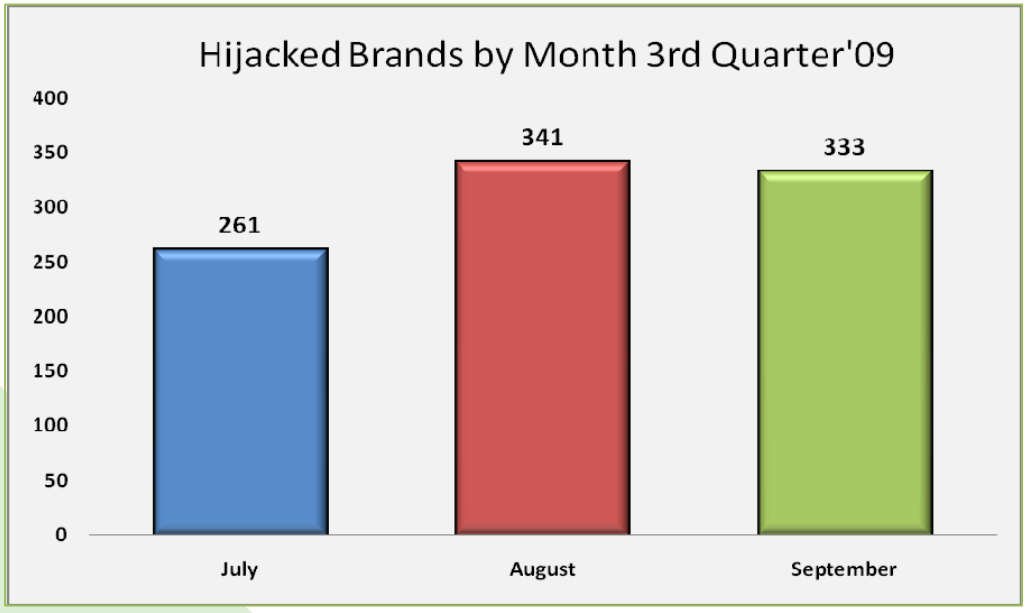
Most Used Ports Hosting Phishing Data Collection Servers – 3rd Quarter 2009

The third 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.

July		August		September	
Port 80	99.94%	Port 80	99.83%	Port 80	99.94%
Port 443	.02%	Port 443	.09%	Port 443	.02%
Port 8095	.01%	Port 88	.02%	Port 81	.01%
Port 8091	.01%	Port 5000	.02%	Port 84	.01%
Port 8017	.01%	Port 82	.01%	Port 8011	.01%
Port 84	.01%	Port 8081	.01%	Port 88	.01%
		Port 8011	.01%		
		Port 84	.01%		

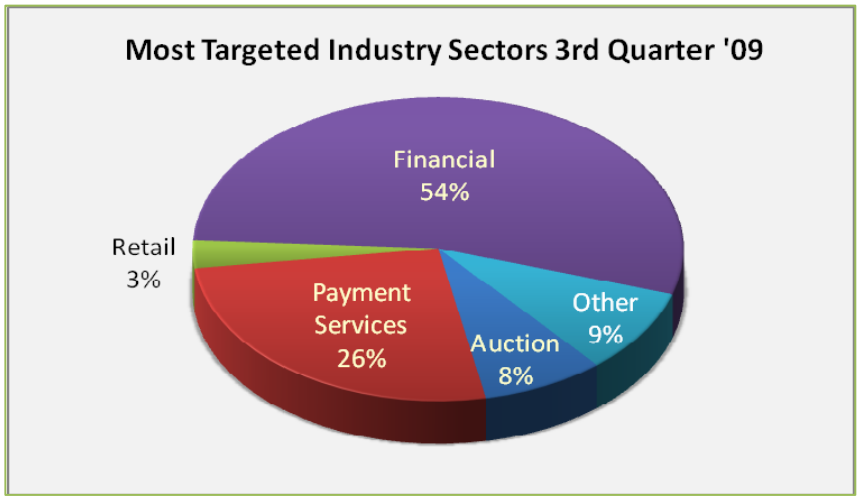
Brands and Legitimate Entities Hijacked by Email Phishing Attacks – 3rd Quarter 2009

The third quarter of 2009 saw a rise in the number of hijacked brands to a record 341 in August, up 10 percent from the previous record of 310 in March 2009. It should be noted that September's number of 333 is also beats the previous high. Phishers continue to expand their target base to attack new brands. [See MarkMonitor commentary on page 5 of this report for additional information, regarding the use of domain names in phishing attacks against brand holders' customers.]



Most Targeted Industry Sectors – 3rd Quarter 2009

Financial Services returned to the top of most targeted industry sectors in Q3, after being eclipsed by the proportion of attacks directed at the Payment Services sector in Q1 and Q2 of 2009. (In the first quarter of 2009, the Payment Services sector jumped into the top position of the most targeted industry sectors for the first time since APWG began tracking the proportions of phishing attacks directed at discrete industry sectors.



Countries Hosting Phishing Sites – 3rd Quarter 2009

The United States continued its position as the top country hosting phishing sites during the third quarter of 2009. In the previous APWG first-half 2009 report, Sweden took the top spot in June and descended to second place in July. Sweden completely dropped from the top 10 in this category in both August and September, removing the country from the listing as a top hosting country.

July		August		September	
USA	38.89%	USA	62.58%	USA	75.76%
Sweden	33.44%	China	8.33%	Hong Kong	6.49%
Romania	6.74%	Germany	3.90%	China	3.44%
Poland	2.99%	Hong Kong	2.73%	Germany	1.99%
Spain	2.10%	Rep. Korea	2.20%	UK	1.34%
China	1.95%	Poland	2.15%	Rep. Korea	1.30%
Canada	1.81%	France	1.82%	France	1.09%
Hungary	1.71%	UK	1.47%	Canada	1.07%
UK	1.33%	Canada	1.47%	Russia	0.84%
France	1.17%	Netherlands	1.45%	Poland	0.82%

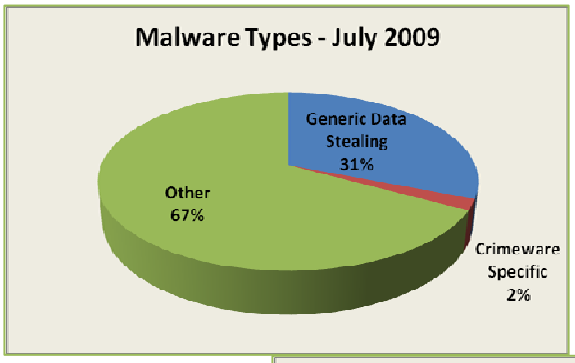
Crimeware Taxonomy and Samples According to Classification

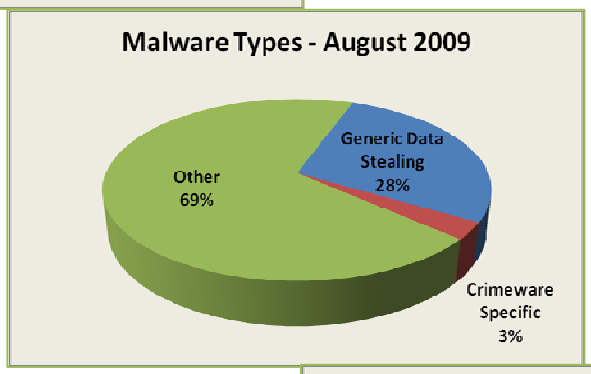
The APWG's Crimeware statistics categorize crimeware attacks as follows, though the taxonomy will grow as variations in attack code are spawned:

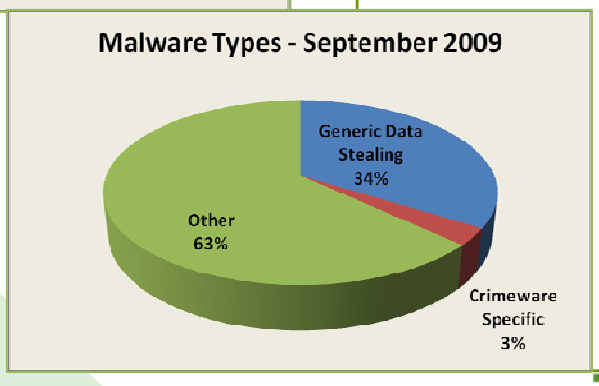
Definition: Crimeware code which is designed with the intent of collecting information on the end-user in order to steal those users' credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations, 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 – 3rd 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 to be used in attacks against financial institutions' customers) malware was consistent, while data-stealing malware grew.







Malevolent Software Definitions

Crimeware (data-stealing malicious code designed specifically to be used to victimize financial institutions' customers and to co-opt those institutions' identities); ***Data Stealing/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.)

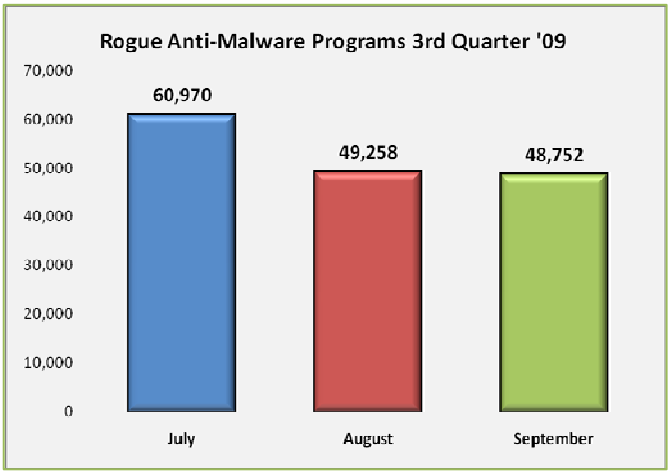
Rogue Anti-Malware Programs – 3rd Quarter 2009

Luis Corrons, PandaLabs Technical Director and APWG *Trends Report* analyst, points out that rogue antivirus is one of the most efficient – and increasingly preferred - ways to victimize consumers. Unlike banking Trojans, where cybercriminals have to infect a PC, steal data, etc. a *rogueware* attack simply fools a users into paying for worthless software – or forcing them to make a ransom payment. The user is the one willing to pay in order to "disinfect" their PC - or free it from a cybercriminal's control.

The cybercriminals that use rogueware realize two main improvements in efficiency:

1. Avoiding detection of their "programs" by users' antivirus software. Cybercriminals use server-side polymorphism techniques: in many cases they create a discrete binary for each infection. This is the reason for the huge increase in new rogueware samples in the last 2 years.

2. Increasing the user conversion rate. Cybercriminals profit faster by increasing the proportion of users who pay after downloading rogueware. These techniques have rocketed in the last quarter, with new cybercriminals using *ransomware* – which don't let you use your PC until you buy a 'license'.



In Q3, we've seen that cybercriminals have focused mainly on this 2nd aspect regarding the conversion rate. The rogueware family TotalSecurity is the one with most new variants in Q3 (around 25 percent of all the new samples belong to this family) that is using the ransomware technique. The efficiency of user conversion has allowed the cybercriminals to enjoy apparently satisfying profitability without having to exert heroic effort for maximal dispersion and propagation of their rogueware, Corrons points out.

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

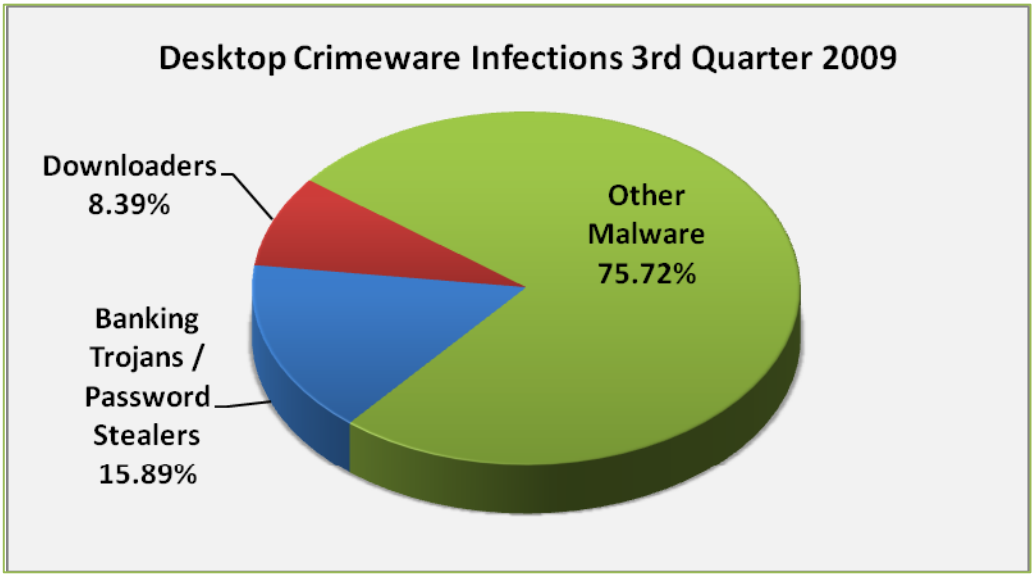
This chart represents a breakdown of the websites which were classified during the third quarter 2009 as hosting malevolent software in the form of either a phishing-based keylogger - or a Trojan downloader which downloads a keylogger. China eclipsed the United States, long-standing leader in this category, in August and September, 2009.

July		August		September	
USA	34.69%	China	34.98%	China	26.90%
China	34.25%	USA	28.95%	USA	25.96%
Russia	4.99%	Russia	6.21%	Russia	17.88%
Brazil	4.91%	Brazil	4.40%	Germany	4.43%
Germany	4.18%	Netherlands	4.30%	Brazil	3.28%
Canada	2.51%	Germany	3.34%	Ukraine	3.12%
Netherlands	1.51%	Canada	2.02%	Rep. Korea	2.56%
France	1.24%	Rep. Korea	2.00%	Netherlands	2.23%
Spain	1.22%	Spain	1.71%	Canada	1.60%
Rep. Korea	1.23%	UK	1.42%	Spain	1.56%

Desktop Crimeware Infections – 3rd 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.

The proportion of infected computers detected has decreased for the first time in 2009. In the same way, the proportion of banking Trojans has decreased from a 16.94 percent in Q2 to 15.89 percent in Q3. The proportion of Downloaders has dropped to 8.39 percent from 11.44 percent in Q2 - but it is still higher than in Q1 (4.22%).



Q3: Scanned Computers	22,754,837	
Infected Computers	11,001,646	48.35%
Non Infected Computers	11,753,191	51.65%
Banking Trojans / Password	1,748,161	15.89%
Downloaders	923,038	8.39%

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, 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 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 3,300 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.