Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Phishing Activity Trends Report September, 2005

Phishing is a form of online identity theft that employs both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as account usernames and passwords. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant **crimeware** onto PCs to steal credentials directly, often using key logging systems to intercept consumers online account user names and passwords.

The monthly *Phishing Activity Trends Report* analyzes phishing attacks reported to the Anti-Phishing Working Group (APWG) via the organization's website at http://www.antiphishing.org or email submission to reportphishing@antiphishing.org. The APWG phishing attack repository is the Internet's most comprehensive archive of email fraud and phishing activity. The APWG additionally measures the evolution, proliferation and propagation of **crimeware** drawing from the independent research of our member companies. In the second half of this report are tabulations of crimeware statistics and reportage on specific criminal software detected by our member researchers.

Highlights

- Number of unique phishing reports received in September: **13562**
- Number of unique phishing sites received in September: **5259**
- Number of brands hijacked by phishing campaigns in September: **106**
- Number of brands comprising the top 80% of phishing campaigns in September: **6**
- Country hosting the most phishing websites in September: **United States**
- Contain some form of target name in URL: **50 %**
- No hostname just IP address: **34 %**
- Percentage of sites not using port 80: **8 %**
- Average time online for site: **5.5 days**
- Longest time online for site: **31 days**

Methodology

APWG is continuing to refine and develop our tracking and reporting methodology. We have recently 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 unique base URLs of the phishing sites.

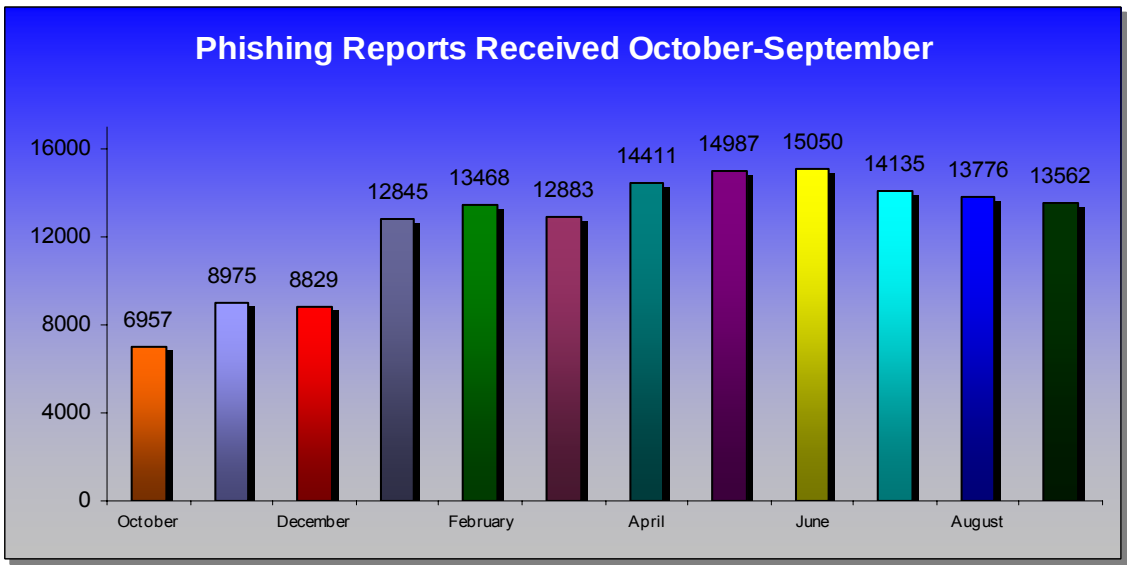
APWG is also tracking crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample) as well as unique sties that are distributing crimeware (typically via browser drive-by exploits).

The **Phishing Attack Trends Report** is published monthly by the Anti-Phishing Working Group, an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. For further information, please contact Ronnie Manning at rmanning@websense.com or 858.320.9274 or APWG Secretary General Peter Cassidy at 617.669.1123. Analysis for the **Phishing Attack Trends Report** has been donated by the following companies:

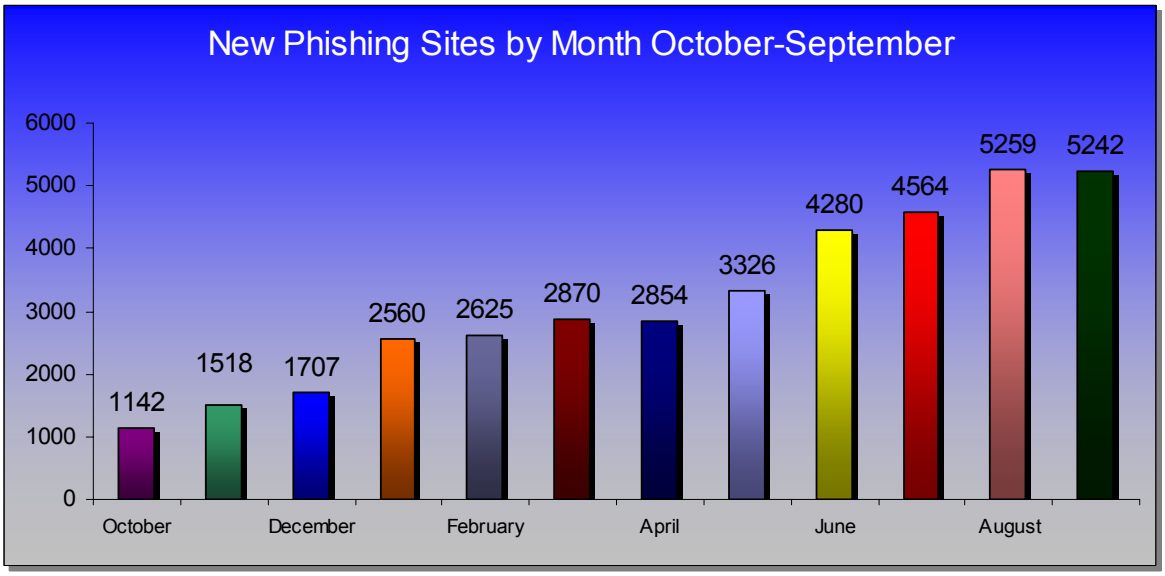
MarkMonitor panda software WEBSENSE.

Phishing Email Reports And Phishing Site Trends

The total number of unique phishing reports submitted to **APWG** in September 2005 was 13,562. This is a slight reduction from the 13,776 reported in August. Keep in mind; this is a count of ***unique*** phishing email reports.

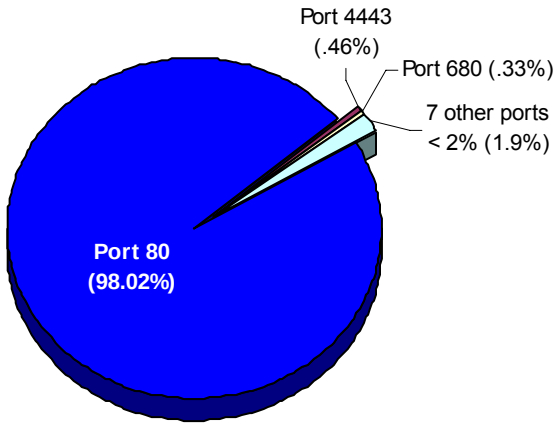


The number of unique phishing websites detected by **APWG** was **5242** in September 2005, the second highest number ever.



Top Used Ports Hosting Phishing Data Collection Servers

September saw a continuation of a trend of HTTP port 80 being the most popular port used, growing to 98.02% of all phishing sites reported.



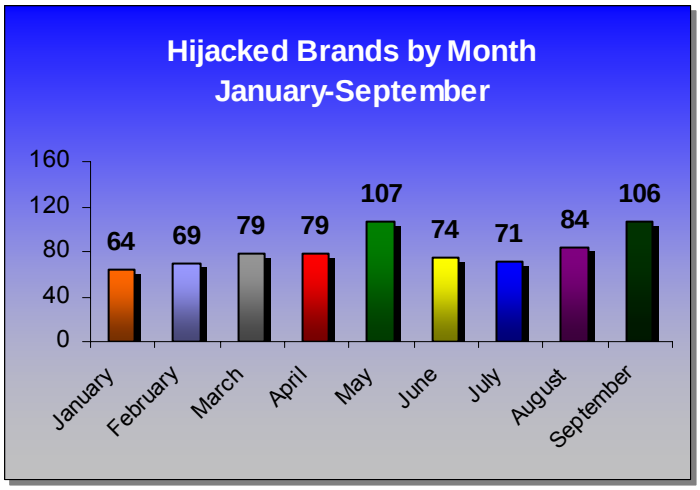
Brands and Legitimate Entities Hijacked By Email Phishing Attacks

Number of Reported Brands

In September, the number of reportedly phished brands rose to 106. In September, there was a large jump in the number of brands being phished.

Of particular note are a large number of credit unions, continuing a trend that we have seen for several months now. There was an unexpected resurgence of several larger banks appearing higher in the statistics.

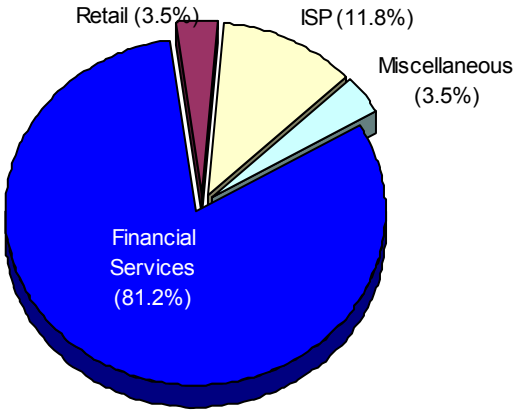
A lot more European and Canadian financial institutions were reported in September.



Most Targeted Industry Sectors

Financial Services continue to be the most targeted industry sector staying steady at 81.2% of all attacks.

There was a dramatic increase in the number of ISPs being phished in September 2005. There was also a rash of phishing scams using the brand of disaster relief agencies, including the Red Cross.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

In September, Websense® Security Labs™ saw a continuation of the top three countries hosing phishing websites. The United States remains the on the top of the list with 31.22%, with the top 10 breakdown as follows; China: 12.13%, Republic of Korea: 10.91%, Germany: 3.16%, Canada: 2.97%, Japan: 2.44%, France: 2.31%, Poland: 2.24%, Brazil: 1.98%, Romania: 1.98%

September Anecdotes and New Targets – Relief Fund and Photo Phishing Attacks

During the month of September, the APWG witnessed several new phishing attacks which utilized people's willingness to assist during times of desperation. This unfortunate attacks prey on the goodness of donators who send relief funds for natural disasters. There were several attacks against a variety of targets and subject matters including; The Red Cross, The Salvation Army, Hurricane Katrina Donations, and Hurricane Rita Donations.

The largest volume was on Hurricane Katrina that was often combined with Red Cross fraud. The attackers started registering domain names that reflected relief and donation sites as soon as the hurricane was named and started blasting out lures shortly after the hurricane hit.

Hurricane Katrina Fraudulent Activity Examples

Websense Security Labs received multiple reports of a new email scam, which attempts to lure users into visiting a malicious website. The message gives a brief news update on Hurricane Katrina and provides a link to the full news story. This website contains encoded JavaScript, which attempts to exploit two HTML Help vulnerabilities. Microsoft has addressed these vulnerabilities with http://www.microsoft.com/technet/security/bulletin/MS05-001.mspx.In the event that either of the exploits are successful, a Trojan downloader is placed on the workstation. The Trojan begins downloading a second malicious file, which is also a Trojan. The second Trojan has backdoor functionality that gives the attacker complete control of the workstation.

The technique, exploit, and Trojan used in this attack are nearly identical to the Iraqi News Email Scam that began circulating in early August.

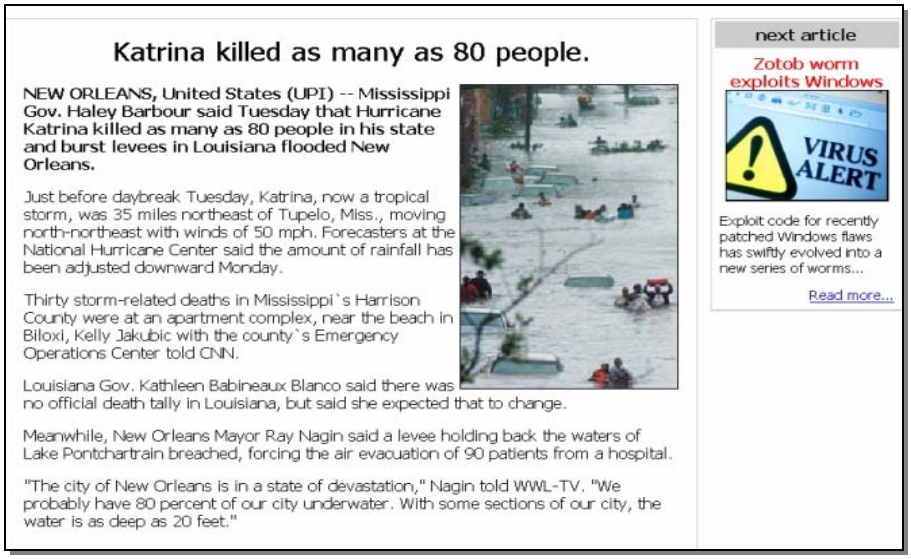
The first website involved in the attack is hosted in Mexico; the second is in the United States.

Websense Security Labs has also observed several hundred new websites, which are requesting donations for Hurricane Katrina relief. Many of these sites are believed to be fraudulent.

Sample email text:

Just before daybreak Tuesday, Katrina, now a tropical storm, was 35 miles northeast of Tupelo, Miss., moving north-northeast with winds of 50 mph.

Forecasters at the National Hurricane Center said the amount of rainfall has been adjusted downward Monday. Mississippi Gov. Haley Barbour said Tuesday that Hurricane Katrina killed as many as 80 people in his state and burst levees in Louisiana flooded New Orleans.



Katrina killed as many as 80 people.

NEW ORLEANS, United States (UPI) -- Mississippi Gov. Haley Barbour said Tuesday that Hurricane Katrina killed as many as 80 people in his state and burst levees in Louisiana flooded New Orleans.

Just before daybreak Tuesday, Katrina, now a tropical storm, was 35 miles northeast of Tupelo, Miss., moving north-northeast with winds of 50 mph. Forecasters at the National Hurricane Center said the amount of rainfall has been adjusted downward Monday.

Thirty storm-related deaths in Mississippi`s Harrison County were at an apartment complex, near the beach in Biloxi, Kelly Jakubic with the county`s Emergency Operations Center told CNN.

Louisiana Gov. Kathleen Babineaux Blanco said there was no official death tally in Louisiana, but said she expected that to change.

Meanwhile, New Orleans Mayor Ray Nagin said a levee holding back the waters of Lake Pontchartrain breached, forcing the air evacuation of 90 patients from a hospital.

"The city of New Orleans is in a state of devastation," Nagin told WWL-TV. "We probably have 80 percent of our city underwater. With some sections of our city, the water is as deep as 20 feet."

2nd Example

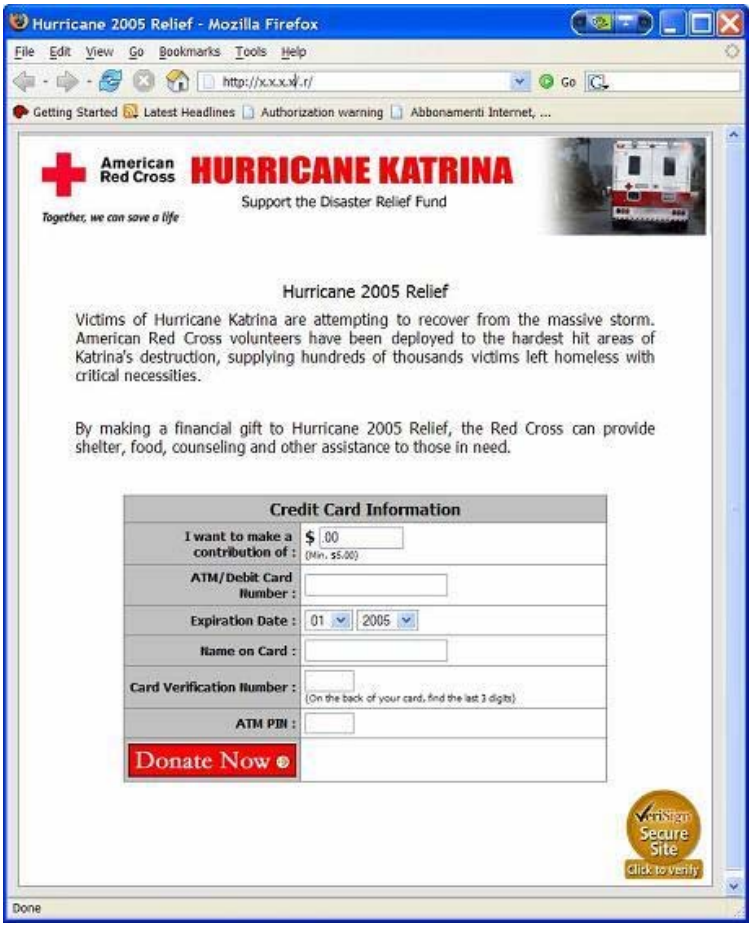
Websense Security Labs received reports of a new phishing attack that targets people to donate money in order to support the relief efforts for Hurricane Katrina. The spoofed email is written in HTML and poses as if it was coming from the Red Cross. The email also has the Verisign "Secure Site" Logo on it to attempt to dupe the end-user into believing that it is legitimate. Upon connecting to the link provided within the email, the user is directed to a fraudulent website which is hosted in Brazil and was up at the time of this alert. The site is also hosting other content and appears to have been compromised. The user's credit card, expiry date, and PIN are requested through a online form and, once entered, the user is then redirected to the real Red Cross website.

Phishing email body:

Victims of Hurricane Katrina are attempting to recover from the massive storm. American Red Cross volunteers have been deployed to the hardest hit areas of Katrina's destruction, supplying hundreds of thousands victims left homeless with critical necessities.

By making a financial gift to Hurricane 2005 Relief, the Red Cross can provide shelter, food, counseling and other assistance to those in need.

Phishing website screenshot



In addition APWG researchers are seeing more phishing attacks that are targeting popular online services and online games. In most cases the purpose is to capture the end-user credentials in order to connect to other services that are connected to that account, to install keyloggers to capture logon credentials, and to capture logon credentials for online game tokens.

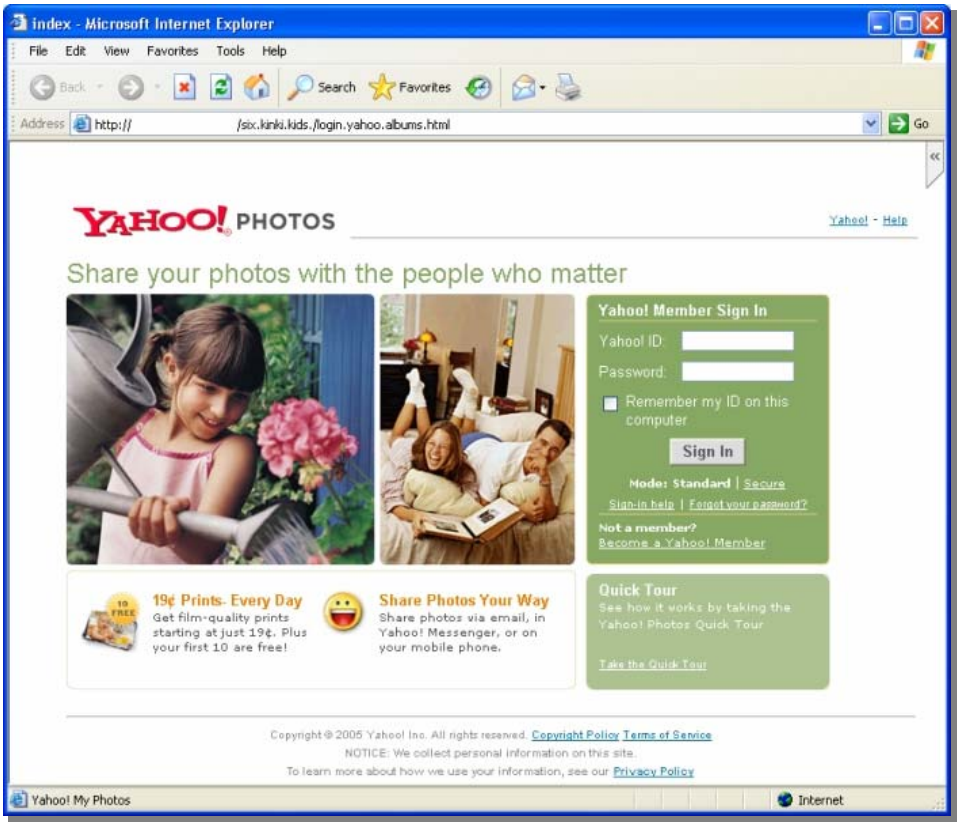
Yahoo! Photos Example Alert

Websense Security Labs has observed a change in the technique used in phishing attacks, which target users of Yahoo!. Phishing attacks attempt to capture a user's Yahoo! ID and password by displaying a fake Yahoo! Sign In page, and have been around for some time. Recently, though, these phishing sites have begun using alternative Yahoo! Sign In pages, such as Yahoo! Photos.

In the Yahoo! Photos example, users receive an email or instant message that claims to be from a friend wanting to show off photos of a recent event, such as a vacation or a birthday party. The message contains a link to a phishing site, which records the user's Yahoo! ID and password, and then forwards the Yahoo! ID and password on to the real Yahoo! Photos site.

The majority of these phishing sites are hosted in the United States on the free web space provided by the Yahoo! Geocities service.

Phishing website screenshot sample



PROJECT: Crimeware

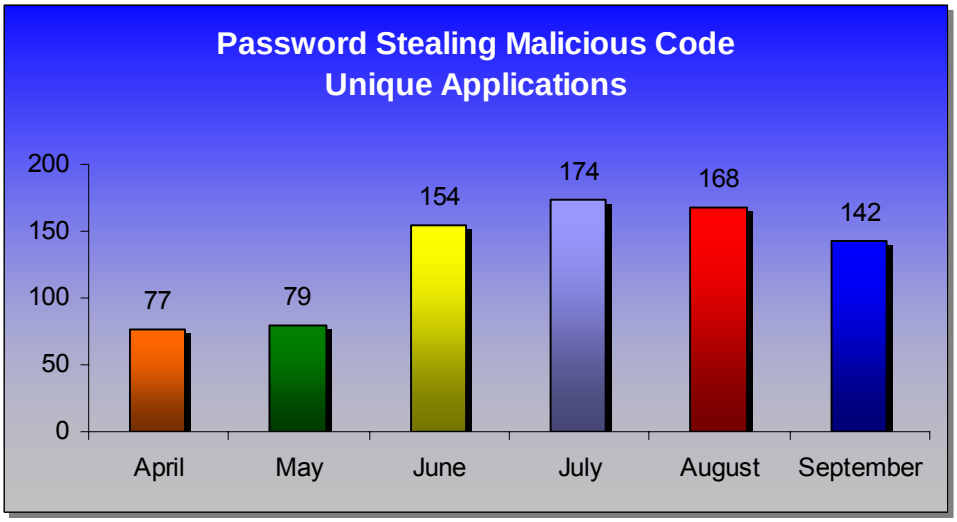
Crimeware Taxonomy & Classification Details

PROJECT: Crimeware categorizes crimeware attacks as follows, though the taxonomy will grow as variations in attack code are spawned:

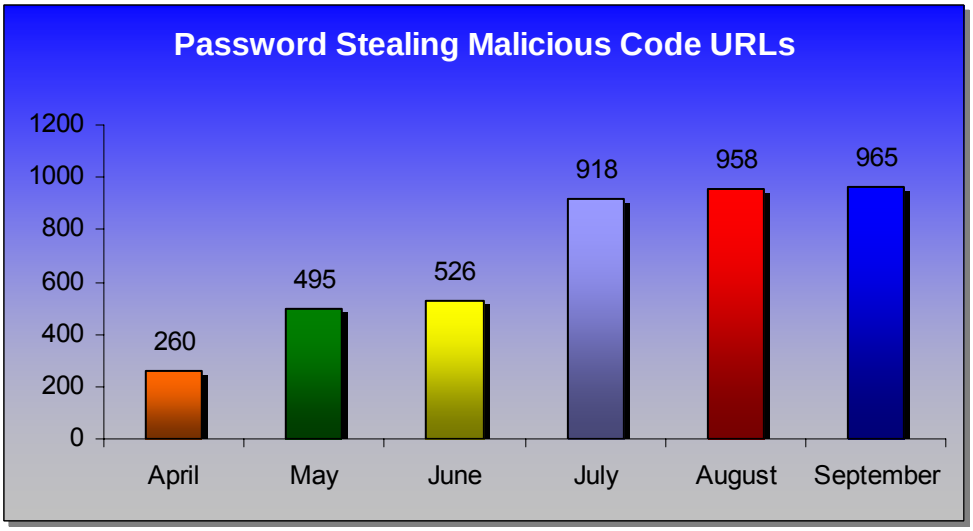
Phishing-based Trojans - Keyloggers

During the month of September, Websense Security Labs have witnessed a slight decrease in the number of variants of keyloggers, but a steady increase of password stealing malicious code URLs.

Phishing-based Trojans – Keyloggers, Unique Variants



Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers

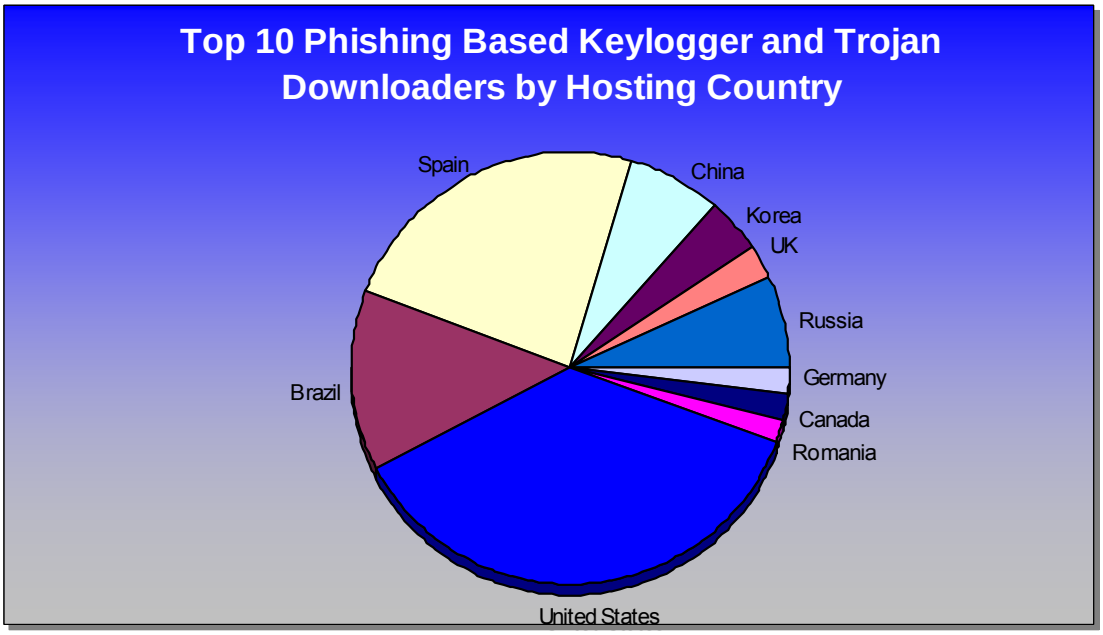


Phishing-based Trojans & Downloader's Hosting Countries (by IP address)

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

The United States is still the top geographic location with 33%, Spain continues to grow rapidly to 21.4%, passing Brazil (12.5%) to become second highest.

The rest of the breakdown was as follows; China 6.5%, Korea 3.62%, United Kingdom 2.37%, Russia 6.25%, Germany 1.75%, Romania 1.75%, Canada 1.75%



More Sophisticated Trojans and Infection Methods

In September, Websense Security Labs witnessed samples of phishing-based keyloggers that were complete applications that had GUI's, step-through wizards, and complex error checking. Unlike malicious applications in the past which usually run in the background, are covert, and very small in size, these are larger Visual Basic written applications that lead the user into entering information into a GUI.

The following is an example alert that was issues by Websense Security Labs on September 21, 2005:

Websense Security Labs has received reports of a new attack that targets AOL customers. Users receive a spoofed email from the security department at AOL. The email claims that AOL had a security breach over the weekend and that confidential information may have been compromised. The email also requests that users connect to a website to download and install a new security patch, which will protect their information.

When users click on the link, they are redirected to a fraudulent website which is hosted in Scotland. This site hosts a piece of malicious code, named patch.scr, which is written in Visual Basic and uses Yoda Crypt. When the file is run, a wizard opens to guide users through the disclosure of their confidential account and billing information, including their account limit.

Once this information is obtained, it is sent in a text file via FTP to an account at a hosting facility.

Email Body:

mandatoryupdate@aol. com

Valued AOL Member:

Over this past weekend America Online fell victim to attacks from hackers. Thousands of people were affected as personal and private information was illegally stolen from them off of our servers. We are still unable to identify everyone who was affected by these attacks.

To prevent this from happening to you or to correct the problem if you have fallen victim to such an attack, we have created a new _Security Patch_ <URL removed> - a new, required update for members of all versions of America Online Software.

Failure to _download_ <URL Removed> this _Security Patch_ <URL Removed> the next 48 hours will result in the temporary suspension of your America Online account. At this point we will send you a Security Patch CD in the mail. Upon installing it, your account will be reactivated. Instead of that, you can _download our Security Patch right here_ <URL Removed>, or by visiting the following URL:

After logging in you will be prompted to 'Run' the above Security Patch.
We thank you for your cooperation and look forward to continue to serve you.

----- America Online of an attack that is targeting AOL users.

Screenshot 1

Screenshot 2

Screenshot 3

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Phishing Research Contributors

MarkMonitor

MarkMonitor is the global leader in delivering comprehensive online corporate identity protection services, with a focus on making the Internet safe for online transactions.

PandaLabs

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

Websense® Security Labs™

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

For media inquiries please contact Ronnie Manning at rmanning@websense.com or 858.320.9274 or Peter Cassidy, APWG Secretary General at 617.669.1123.

About the Anti-Phishing Working Group

The Anti-Phishing Working Group (APWG) 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 share information and best practices for eliminating the problem. Where appropriate, the APWG will also look to share this information with law enforcement.

Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, and solutions providers. There are more than 1300 companies and government agencies participating in the APWG and more than 2000 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 Anti-Phishing Working Group is http://www.antiphishing.org. It serves as a public and industry resource for information about the problem of phishing and email fraud, including identification and promotion of pragmatic technical solutions that can provide immediate protection and benefits against phishing attacks. The analysis, forensics, and archival of phishing attacks to the website are currently powered by Tumbleweed Communications' Message Protection Lab.

The APWG was founded by Tumbleweed Communications and a number of member banks, financial services institutions, and e-commerce providers. It held its first meeting in November 2003 in San Francisco and in June 2004 was incorporated as an independent corporation controlled by its steering committee, its board and its executives.