Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

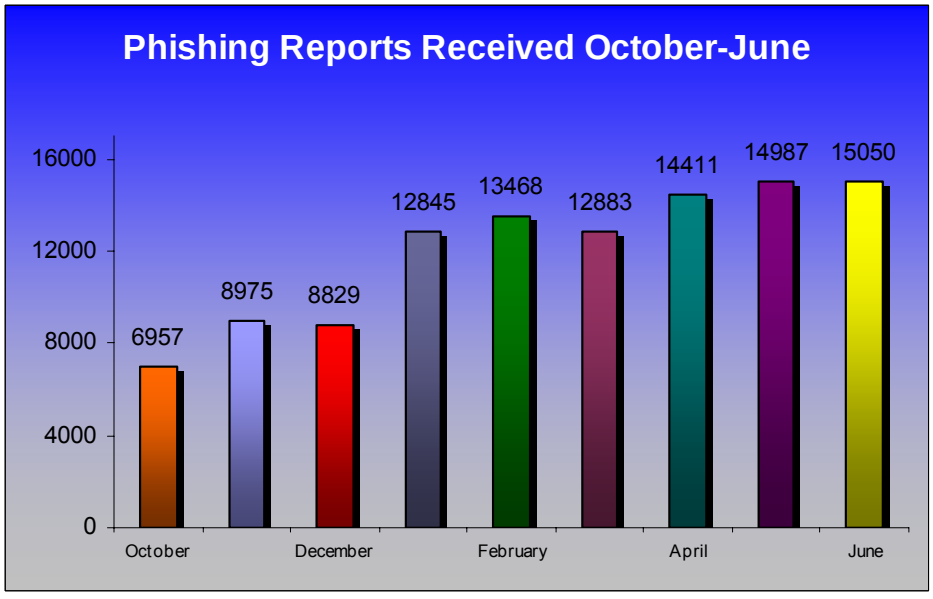
Phishing Activity Trends Report June, 2005

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 keylogger systems to intercept consumers online account user names and passwords.

The 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. Starting with this month's report, the APWG additionally measures the evolution, proliferation and propagation of crimeware drawing from the independent research of our member companies.

Highlights

- Number of phishing reports received in June: **15,050**
- Number of brands hijacked by phishing campaigns in June: **74**
- Number of brands comprising the top 80% of phishing campaigns in June: **5**
- Country hosting the most phishing websites in June: **United States**
- Contain some form of target name in URL: **46 %**
- No hostname just IP address: **41 %**
- Percentage of sites not using port 80: **8 %**
- Average time online for site: **5.9 days**
- Longest time online for site: **30 days**



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:

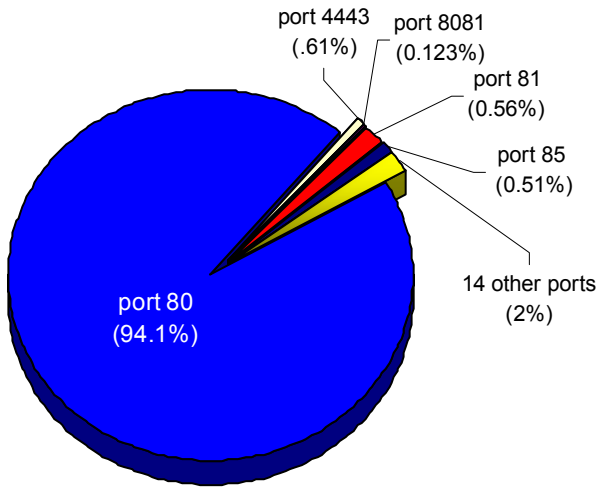
TUMBLEWEED COMMUNICATIONS

panda software

WEBSENSE.

Top Used Ports Hosting Phishing Data Collection Servers

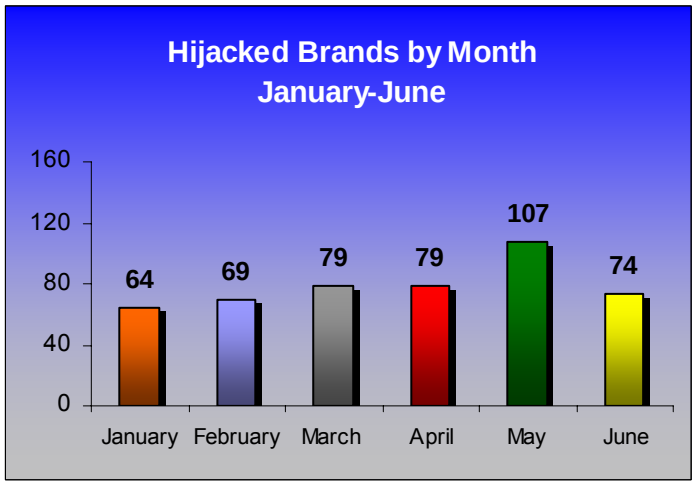
June saw a continuation of a trend of using look-alike cousin domain names to host phishing sites. Consequently, the use of alternate ports has decreased and the standard HTTP port 80 is in use at 94.1% of all phishing sites reported.



Brands and Legitimate Entities Hijacked By Email Phishing Attacks

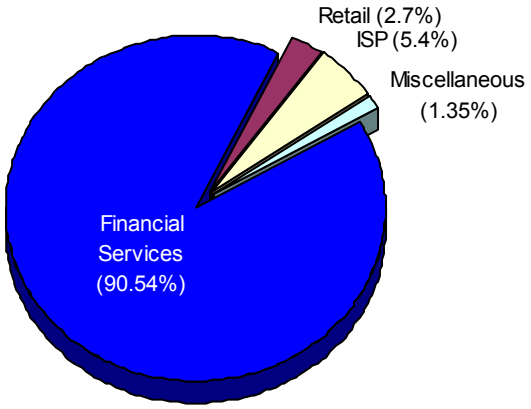
Number of Reported Brands

In June, the number of reportedly phished brands dropped when compared with April, reflecting numbers similar to previous months.



Most Targeted Industry Sectors

Financial Services continue to be the most targeted industry sector growing to nearly 91% of all attacks.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

In June, Websense Security Labs saw a large decrease in the number of phishing sites that are hosted in China. The United States remains the on the top of the list with 35.5%, with the top 10 breakdown as follows; China 11.2%, Korea 10.1%, France 5.6%, Germany 3.2%, Canada 2.8%, Japan 2.4%, Italy 1.76%, Romania 1.72%, Netherlands 1.65%.

Attack Method Update

PROJECT: Crimeware

Since early 2004, the APWG has been observing technical advances worldwide in the way that criminals are attacking unsuspecting users in order to steal consumer information. Although phishing with social engineering lure emails and counterfeit websites is the most prominent phishing technique, there is a rise in alternative methods to co-opt consumers' online credentials or gain control of their accounts without using direct deception. (The APWG notes that in Brazil, the archetypical phishing approach is actually a blended social engineering and technical subterfuge attack, driving a general population to generic entertainment sites in order to plant key loggers, techniques manifestly more potent than pure social engineering schemes when you examine the alleged phishers' takings reported during police arrests there over the past year – upwards of tens of millions each time.)

Automated systems based on trojaning schemes and session hikacking systems have reported worldwide over the past 18 months in a trend of development that has surged markedly over the past 3 months, supporting the APWG's view that automated phishing systems are the way of the future worldwide for this criminal enterprise.

Furthermore, PandaLabs detected a Trojan-type phishing system which exploited to the full one of the main advantages that this type of crimeware possesses compared to traditional phishing: Trj/Bancos.NL includes a list of thousands of brandholders' domains, demonstrating the advance of phishing technology toward wide-scope consumer-credential capture techniques. The PandaLabs finding indicates a drive by phishers to effect a generic keylogger potent against all credible potential targets.

It is the APWG's belief that phishers will, over time, adopt more automated attack systems based on technical subterfuge to supplement social engineering schemes - or replace them. To remain relevant in its data reporting, the APWG initiated **PROJECT: Crimeware,** a program of collaborative research designed to capture, record and characterize incidents that are new and emerging in order for the APWG to include them in the monthly report and, possibly, other reports that specifically address the threats posed by crimeware.

What is crimeware? The APWG defines it as a genus of technology distinguished from adware, spyware and malware by the fact that it is, by design, developed for the single purpose of animating a financial or business crime.

Crimeware Taxonomy & Classification Details

PROJECT: Crimeware proposes types of crimeware attacks which will be classified and reported upon monthly:

Phishing-based Trojans - Keyloggers

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 and online retailers and ecommerce merchants) in order to target specific information, the most common are; access to financial based websites, ecommerce sites, and web-based mail sites.

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 information to fraudulent sites, and crimeware that may install a network level driver or filter to redirect 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.

Man-in-the-middle Phishing (Pharming)

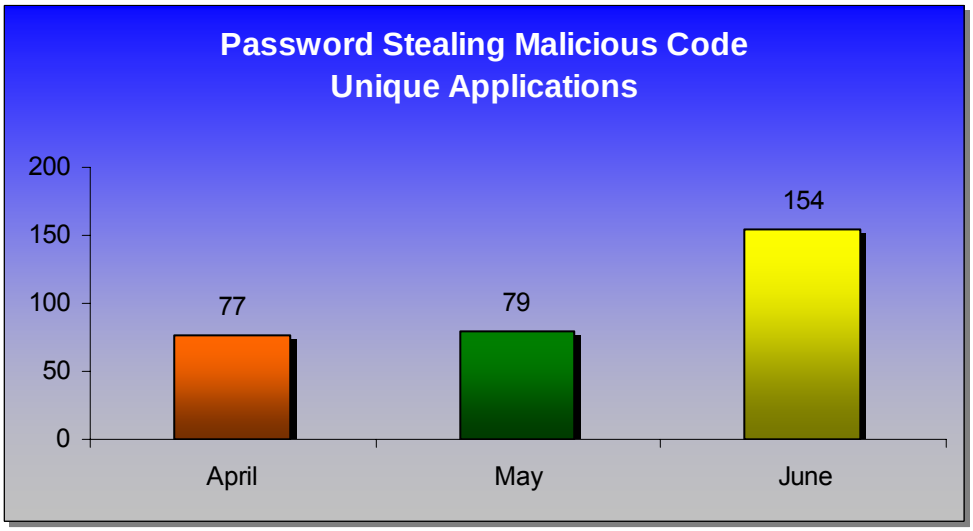
Definition: An attack that intercepts information in between two parties' communications in order to redirect users to a fraudulent location. The most popular attack is DNS cache poisoning.

Other

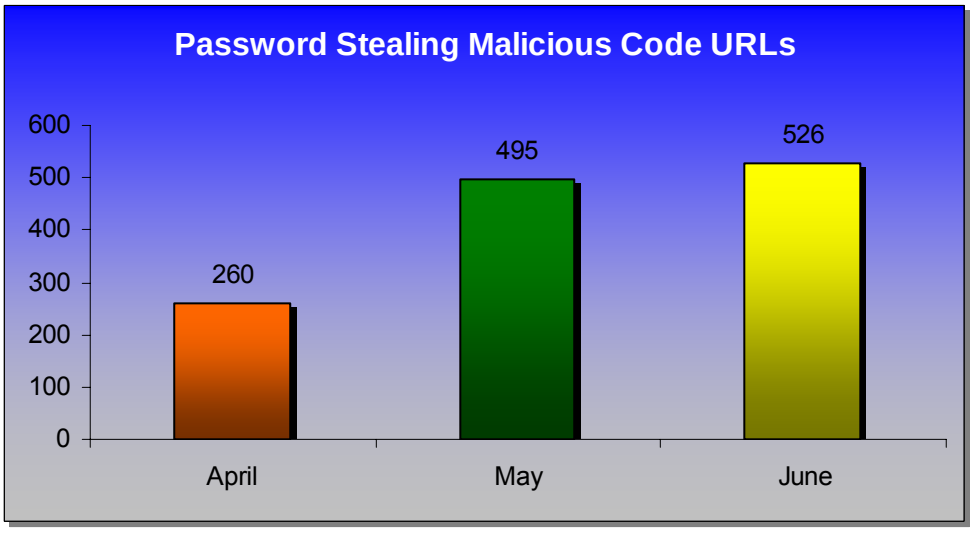
This is reserved for anything that does not fit into the other attack classes. If a new attack class becomes frequent enough we can create its own class. Some recent examples that belong in there are:

- Typo-attacks: mistyping a popular domain and being infected with crimeware.
- Search-engine poisoning: being directed to a fraudulent website which downloads crimeware onto your machine simply by searching on a search engine.

Phishing-based Trojans – Keyloggers, Unique Variants



Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers

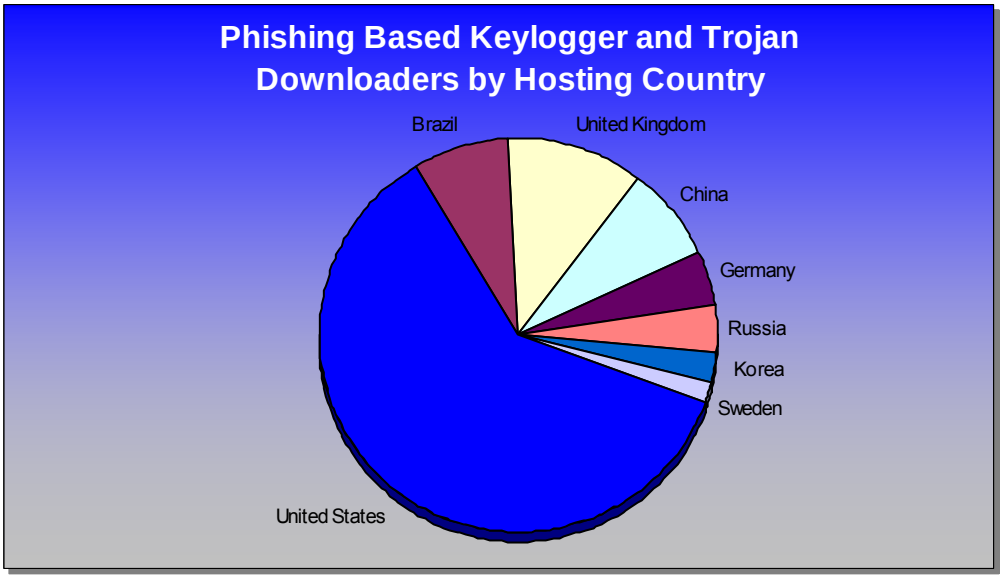


Phishing-based Trojans & Downloader's Hosting Countries (by IP address)

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

Of interest is that the United States is still the top geographic location with more than 55%, Brazil is third with almost 7%. To date, Brazil still has the highest concentration of phishing-based keyloggers that target Brazilian financial institutions and use deception techniques written in Portuguese. Also, unlike regular phishing websites, it is not as common for the websites to be hosted on compromised machines. It is more likely that they are on a free hosting ISP, blog, or personal storage.

The rest of the breakdown was as follows; United Kingdom 10%, China 7%, Germany 4.2%, Russia 3.5%, Korea 2.2%, Sweden 1.5%.



Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Phishing Research Contributors

Tumbleweed Message Protection Lab

The mission of the Tumbleweed Message Protection Lab is to analyze current and emerging enterprise email threats, and design new email protection technologies.

PandaLabs

PandaLabs is an international network of research and technical support centers devoted to protecting users against malware. Present in over 50 countries, it offers services around the clock, 365 days a year.

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 nearly 900 companies and government agencies participating in the APWG and nearly 1400 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.