Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

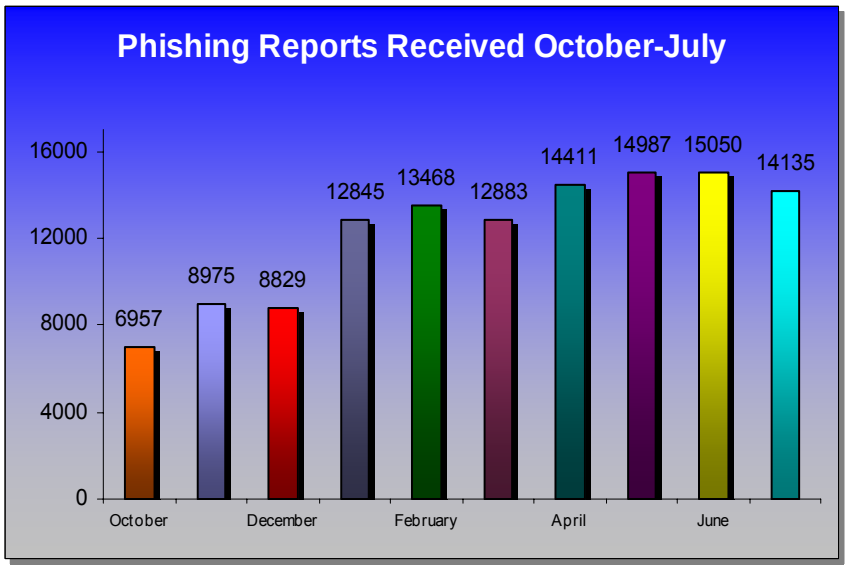
Phishing Activity Trends Report July, 2005

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 phishing reports received in July:	**14,135**
• Number of brands hijacked by phishing campaigns in July:	**71**
• Number of brands comprising the top 80% of phishing campaigns in July:	**6**
• Country hosting the most phishing websites in July:	**United States**
• Contain some form of target name in URL:	**46 %**
• No hostname just IP address:	**41 %**
• Percentage of sites not using port 80:	**9 %**
• 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:

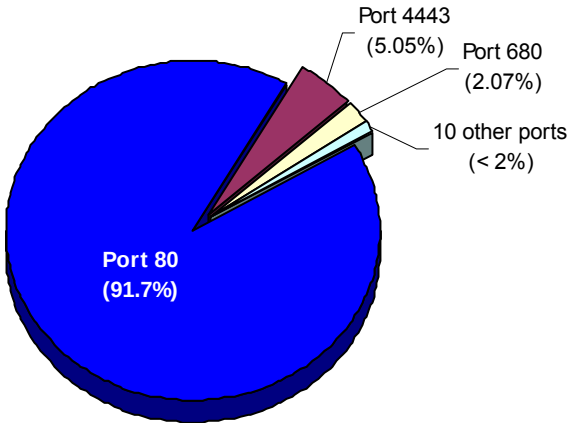
panda software

WEBSENSE.

APWG - Anti-Phishing Working Group

Top Used Ports Hosting Phishing Data Collection Servers

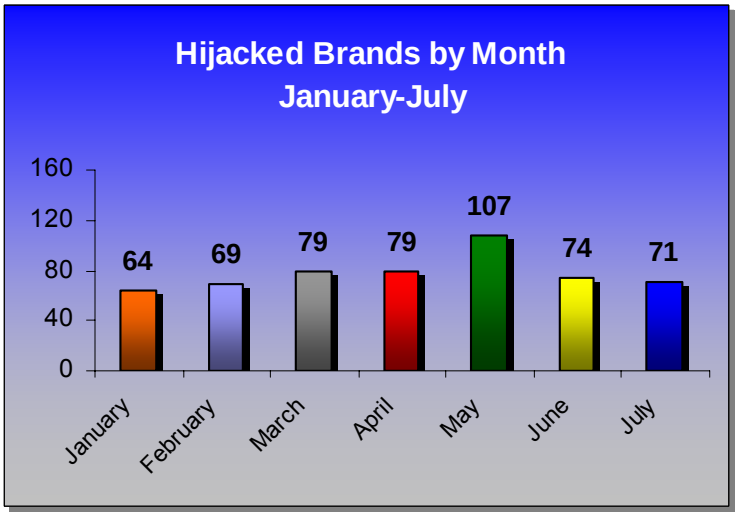
July saw a continuation of a trend of using look-alike cousin domain names to host phishing sites. Consequently, the use of alternate ports has decreased and the standard HTTP port 80 is in use at 91.7% of all phishing sites reported.



Brands and Legitimate Entities Hijacked By Email Phishing Attacks

Number of Reported Brands

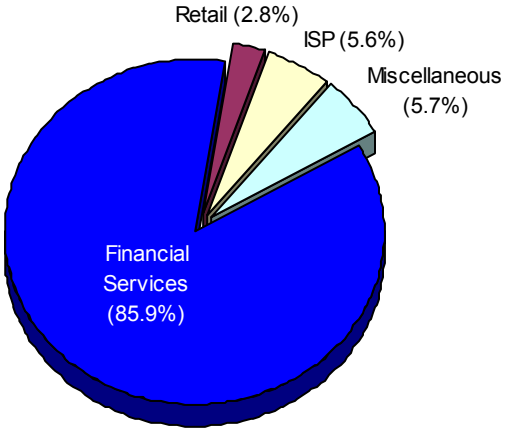
In July, the number of reportedly phished brands dropped once again to 71. However, phishers are spreading their nets, and are moving away from some traditional larger targets, and hitting a wider base of smaller financial institutions.



Most Targeted Industry Sectors

Financial Services continue to be the most targeted industry sector growing to nearly 86% of all attacks. APWG sees a number of new targets in financial services including insurance, credit unions, payment services and an ATM network.

We are seeing an increase in the number of reported attacks against European financial institutions and ISPs. In addition, more attacks against the customers of Canadian institutions being reported as well.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

In July, Websense® Security Labs™ saw a large increase in the number of phishing sites that are hosted in Australia. The United States remains the on the top of the list with 30%, with the top 10 breakdown as follows; Korea: 14%, China: 10%, France: 6%, Australia: 5%, Germany: 3.5%, Japan: 3%, Canada: 1.7%, Thailand: 1.5%, Italy: 1.5%

Phishing attacks are becoming more and more frequent on brands that are not based in the UK and United States. Although the US and UK are still the most common, Websense Security Labs have seen increases in attacks that are written in languages other than English attempting to gain credentials from users in a number of countries including; Italy, Spain, Japan, Korea, and Germany.

PROJECT: Crimeware

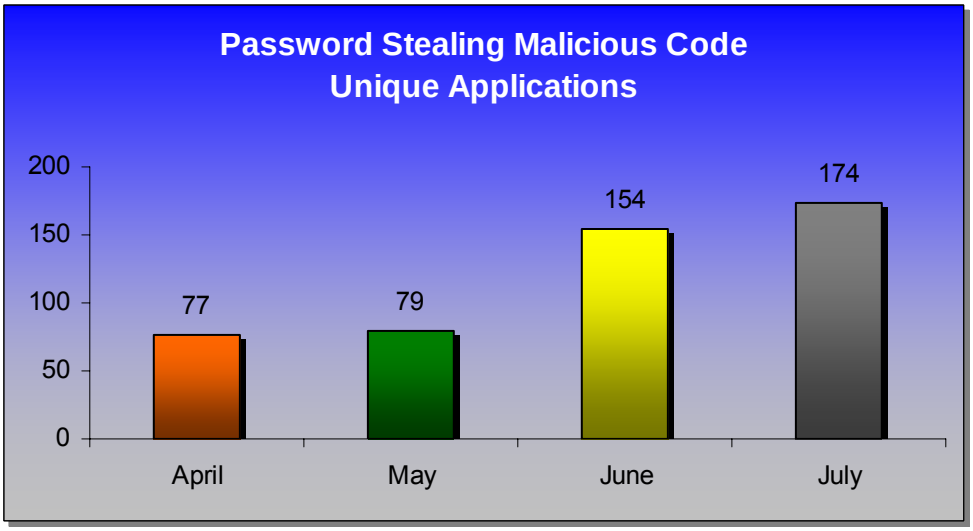
Crimeware Taxonomy & Classification Details

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

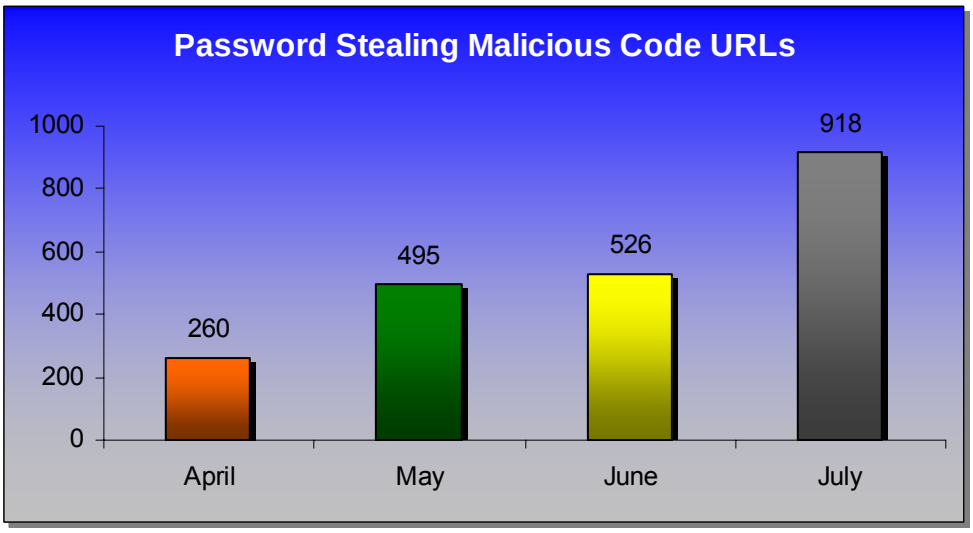
Phishing-based Trojans - Keyloggers

During the month of July, Websense Security Labs have again witnessed increased numbers of variants and new banking keyloggers. The numbers of websites which were hosting these keyloggers rose even more dramatically as we saw close to a 100% increase. The United States and Brazil compromise almost 70% of all the sites that were hosting Trojan keyloggers and used personal hosting websites that are mostly used for online journals, blogs, and personal storage.

Phishing-based Trojans – Keyloggers, Unique Variants



Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers

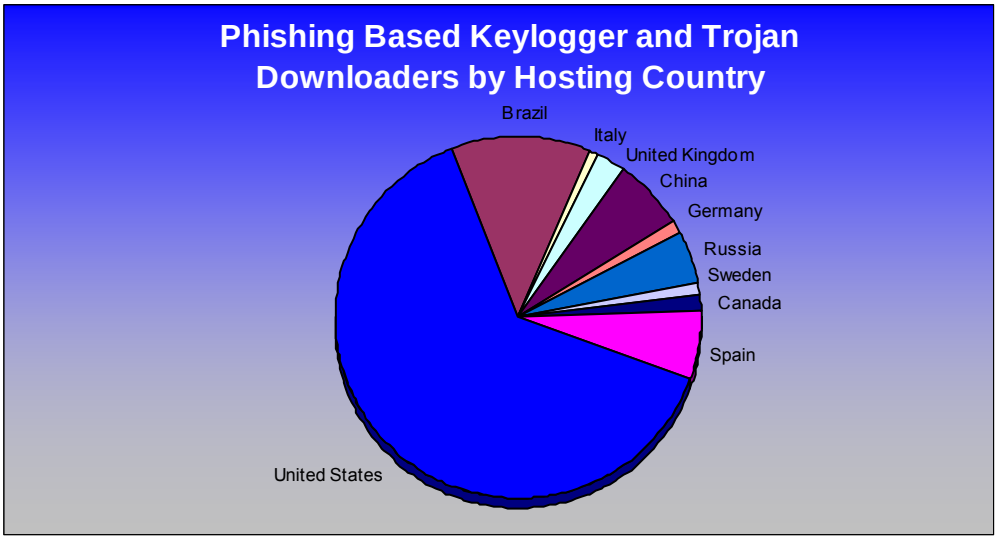


Phishing-based Trojans & Downloader's Hosting Countries (by IP address)

The chart below represents a breakdown of the websites which were classified during July 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 more than 57%, Brazil is second with 11%. Continued from last months report, Brazil still has the highest concentration of phishing-based keyloggers that target Brazilian financial institutions and use deception techniques written in Portuguese.

The rest of the breakdown was as follows; China 5.7%, Spain 5.4%, Russia 4.4%, United Kingdom 2.4%, Canada 1.2%, Germany 1%, Sweden 1%, Italy 1%



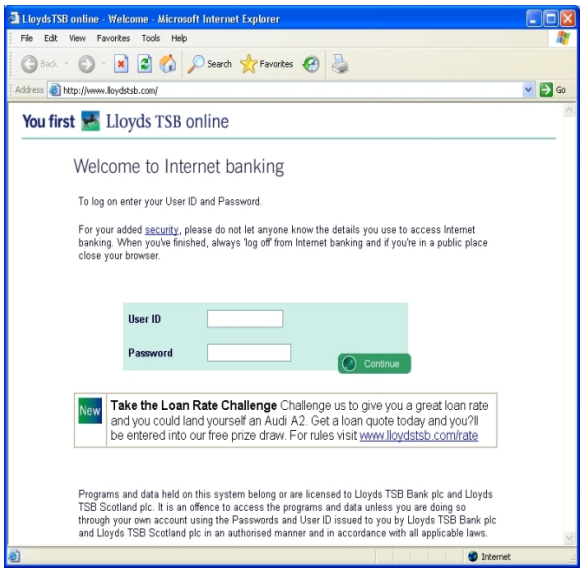
Phishing-based Trojans – Redirectors

During the month of July, we saw increases in the number of Trojan Horses which are designed to modify your system in order to redirect you to a fraudulent site upon typing in the URL of the real site. The most common being the modification of the hosts file on personal computers.

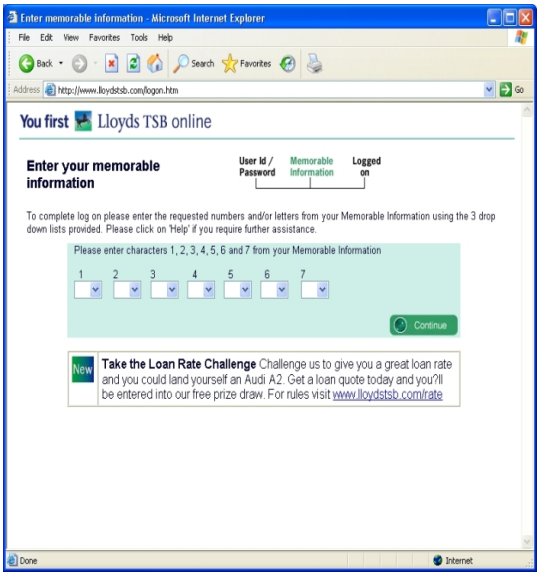
Websense Security Labs detected a new trojan variant that performed a phishing attack against users. The trojan modified the hosts file on the infected machine, and then maps the real address of a bank to the IP address of a phishing site. This mapping causes users to be redirected to a phishing site when they attempt to access their bank account.

In the example screenshots shown below, the browser displays the correct web address, but has actually loaded a phishing site. After users enter their logon information into the fake website, they are redirected to the real website of the bank. This trojan also functions as a keylogger. The trojan starts capturing keystrokes once it detects an online banking site is being accessed. The trojan then uploads the captured keystrokes to the attacker.

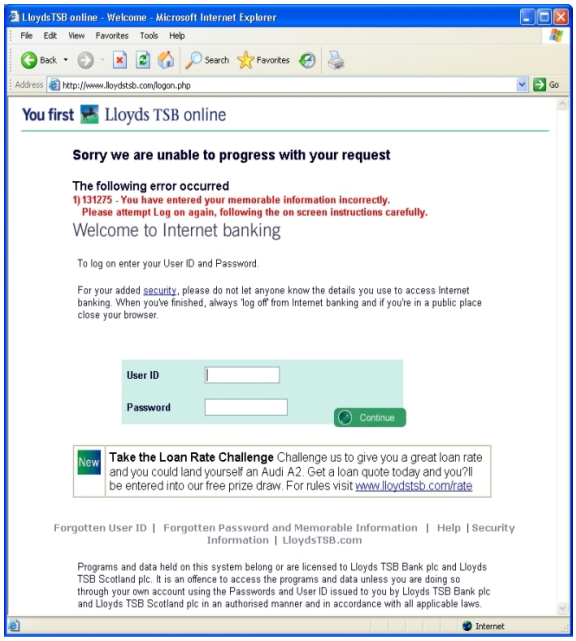
Fake site screenshot 1:



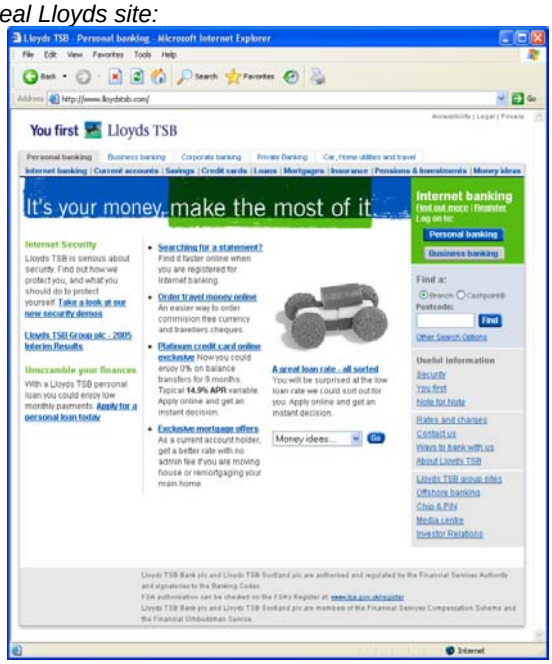
Fake site screenshot 2:



Fake site screenshot 3:



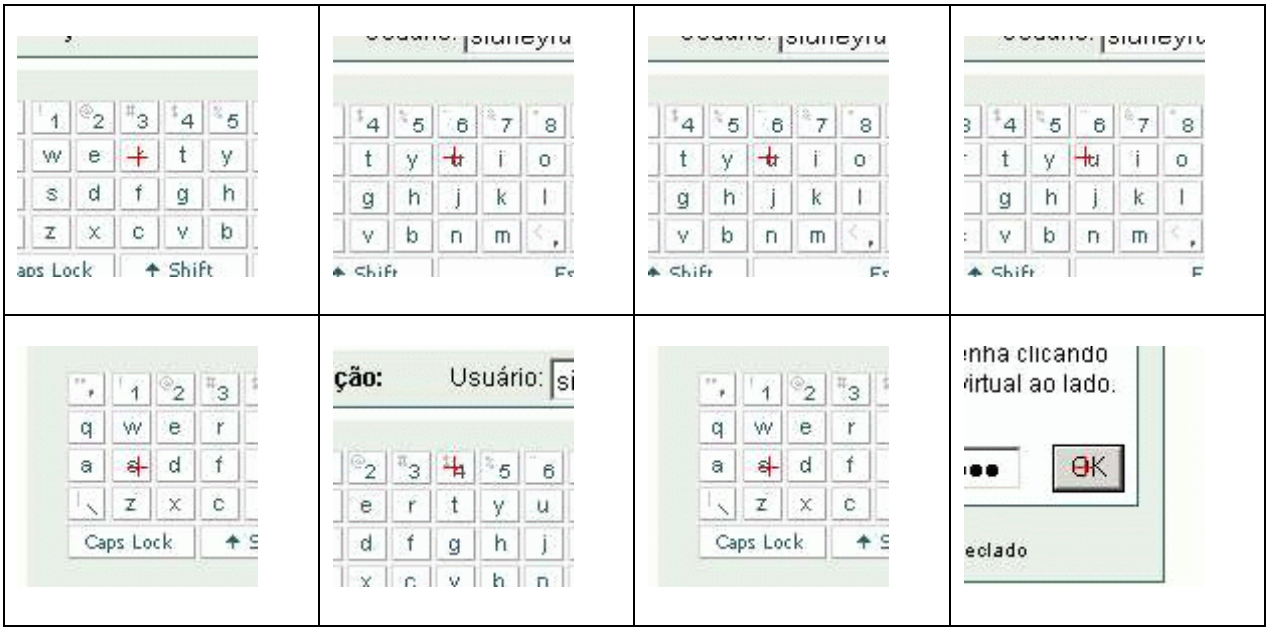
Real Lloyds site:



Screen Scraper

In late July we started to see some additional techniques being deployed more frequently than previously. These are Trojan Horses which are designed to capture screenshots of the target machine in order to capture credentials from the end-user. Due to the increase in phishing-based keyloggers several banks have changed the method to how they authenticate users within their website. In this case they are using a browser popup window which requests the user clicks on numeric keypad in order to logon.

The malicious code waits for the active window to equal one of the sites that they want to monitor information for. Once accessed the program then "scrapes" the screen based on the mouse clicks and uploads that information to a website in order to compromise the credentials. The below example is from a website that was hosting images from a screen scraper.



Phishing Research Contributors

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 more than 1200 companies and government agencies participating in the APWG and more than 1800 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.