Anti-Phishing Working Group
APWG

Anti-Phishing Working Group
Committed to wiping out Internet scams and fraud

Phishing Activity Trends Report March, 2006

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, and to corrupt local and remote navigational infrastructures to misdirect consumers to counterfeit websites and to authentic websites through phisher-controlled proxies that can be used to monitor and intercept consumers' keystrokes.

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 March:	**18,480**
• Number of unique phishing sites received in March:	**9666**
• Number of brands hijacked by phishing campaigns in March:	**70**
• Number of brands comprising the top 80% of phishing campaigns in March:	**3**
• Country hosting the most phishing websites in March:	**United States**
• Contain some form of target name in URL:	**48.05 %**
• No hostname just IP address:	**32 %**
• Percentage of sites not using port 80:	**3.9 %**
• Average time online for site:	**5.0 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.

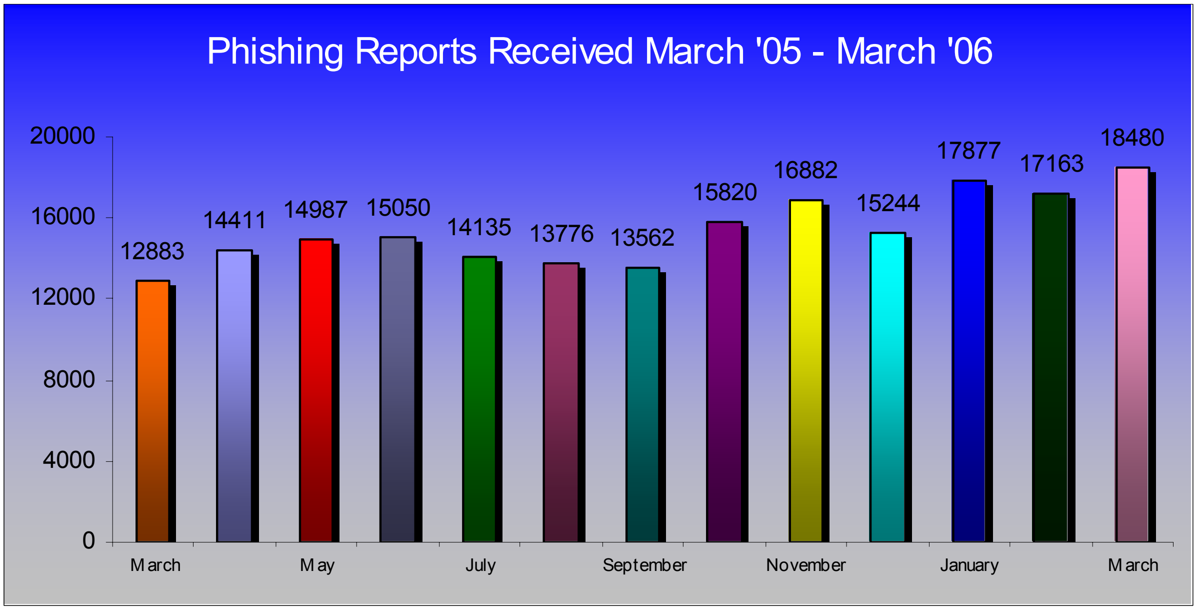
APWG is also tracking crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample) as well as unique sties that are distributing crimeware (typically via browser drive-by exploits).

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:

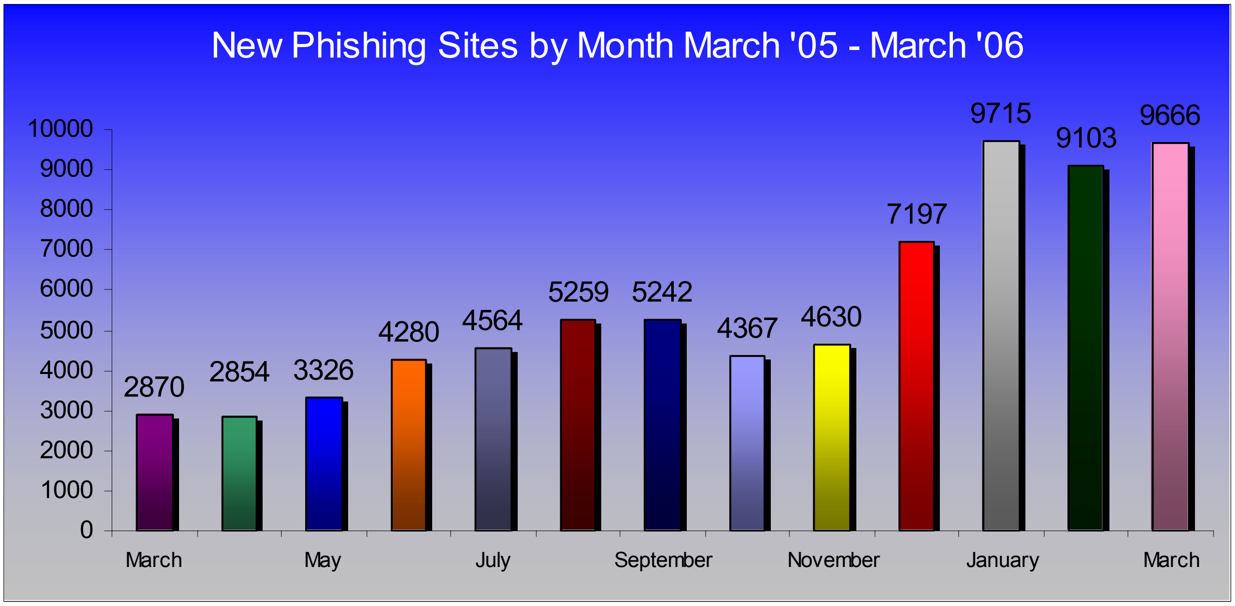
MarkMonitor panda software WEBSENSE.

Phishing Email Reports And Phishing Site Trends

The total number of *unique* phishing reports submitted to **APWG** in March 2006 was **18,480** – the most reports ever recorded. This is a count of ***unique*** phishing email reports. March 2006 continues the trend of more phishing attacks and more phishing sites. The IRS phishing attack doubled in volume in March as compared to February (in the USA, the tax filing deadline was April 17 in 2006, as the usual April 15 deadline fell on a weekend this year.)

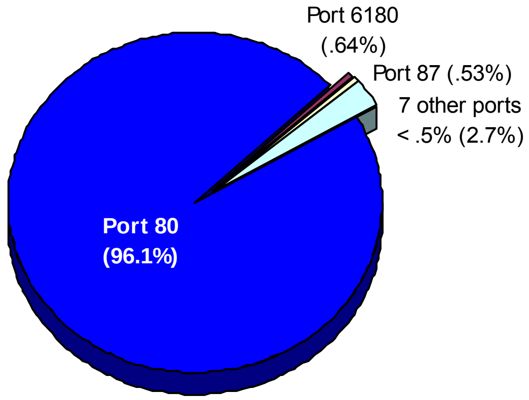


The number of *unique* phishing websites detected by **APWG** was **9666** in March 2006, a continual increase in unique phishing sites during the first three months of 2006.



Top Used Ports Hosting Phishing Data Collection Servers

March saw a continuation of a trend of HTTP port 80 being the most popular port used at 96.1% of all phishing sites reported.

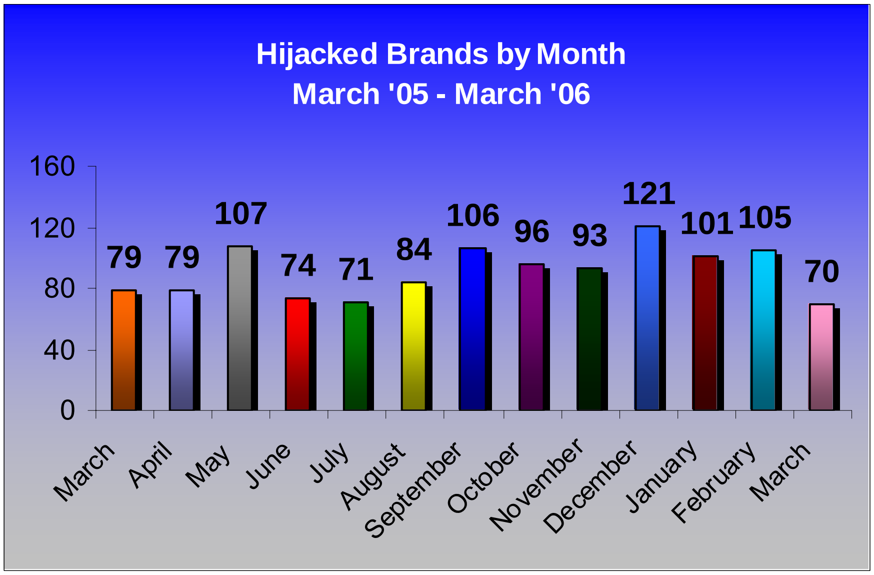


Brands and Legitimate Entities Hijacked By Email Phishing Attacks

Number of Reported Brands

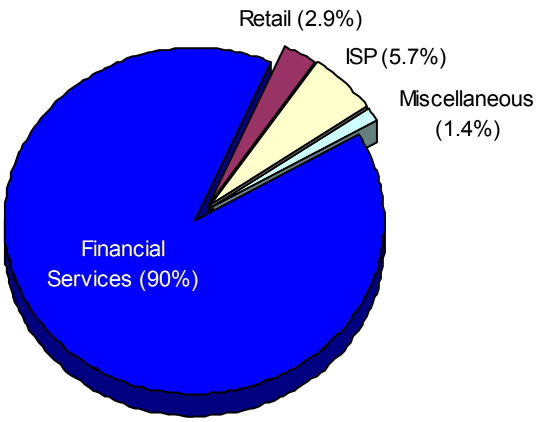
March 2006 showed a major drop off of brands hijacked than February 2006

However, for the first time in many months, a bank was the number one phished company, by a large margin. This would potentially indicate that the phishers have found a way to easily monetize the phished credentials for this particular financial institution. This bank may have a Track 2 issue, allowing the phishers to create counterfeit ATM cards.



Most Targeted Industry Sectors

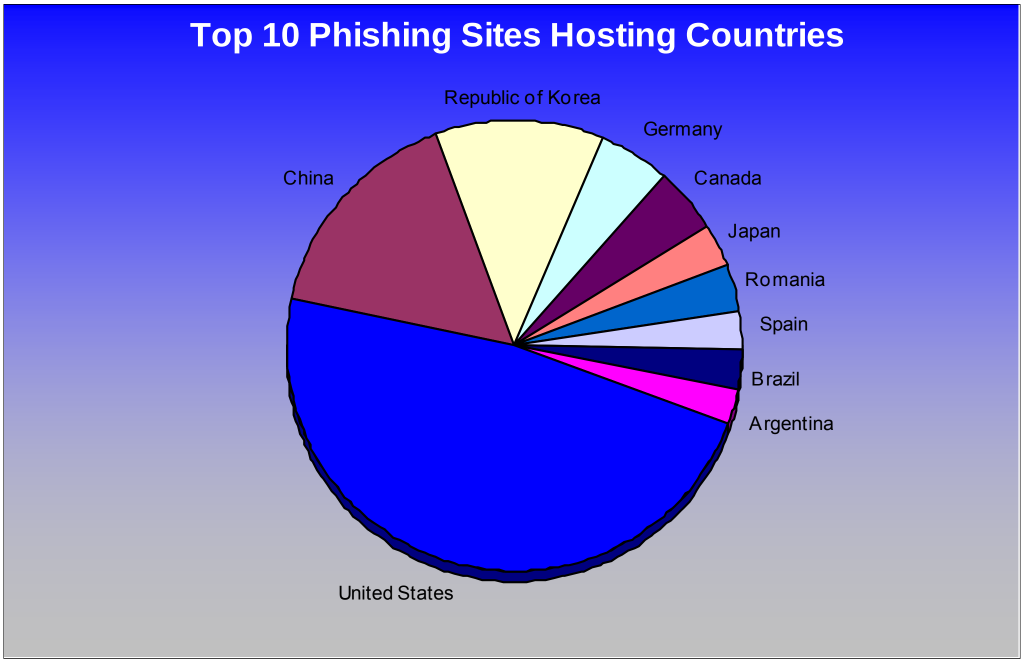
Financial Services continue to be the most targeted industry sector, growing to 90% of all attacks in the month of March.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

In March, 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 35.13%. The rest of the top 10 breakdown is as follows: China 11.93%, Republic of Korea 8.85%, Germany 3.57%, Canada 3.52%, Japan 2.39%, Romania 2.29%, Spain 2.13%, Brazil 1.97%, Argentina 1.92%



PROJECT: Crimeware

Crimeware Taxonomy & Samples According to Classification in March

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

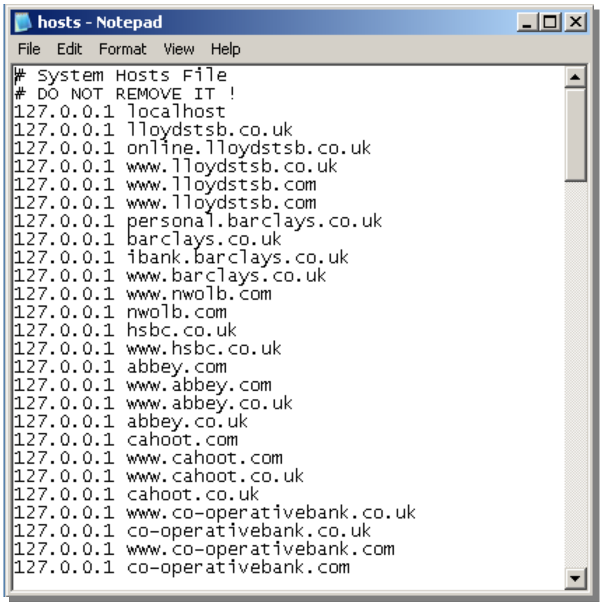
Financial Institution Trojan Attack

During March, Websense Security Labs received reports of a Trojan Horse which targeted users of more than 100 financial institutions in the United States and Europe. Once installed on a user's machine, the malicious code checked to see if there is an active window open (either "my computer" or Internet Explorer). If one of these applications is not open, the malicious code modified the contents of the hosts file on the local machine with a list of sites all pointing to localhost (127.0.0.1).

If either of these applications were open, the behavior was different. In this case, the malicious code performed a DNS lookup to a DNS server hosted in Russia and received an address for a website. The address returned from that DNS server was then populated into the hosts file along with a list of target brands. If the target machine visited one of the sites in the list, the machine was redirected to a fraudulent web site on the hosted machine in Russia. This allowed the attacker to change the destination address through DNS if one of the servers was taken offline.

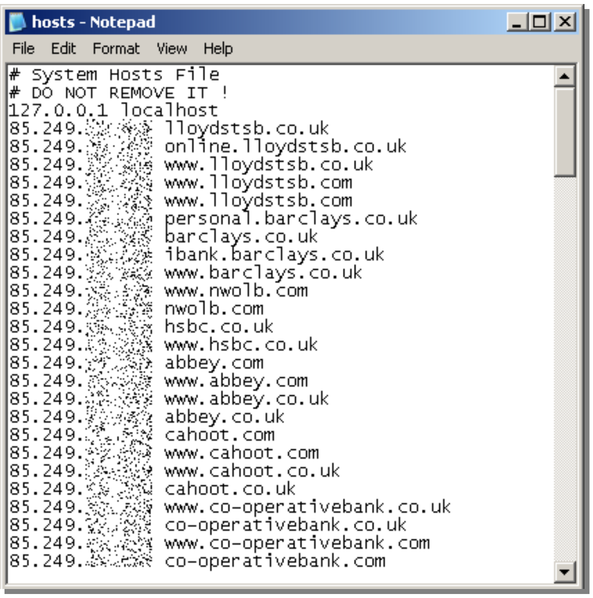
The web server used the hostname received to serve up pages for that particular target. There were more than 100 different phishing brands hosted on this site, all with unique pages for the particular attack.

Screenshot 1: Hosts file when no active window open.



```
# System Hosts File
# DO NOT REMOVE IT !
127.0.0.1 localhost
127.0.0.1 lloydstsb.co.uk
127.0.0.1 online.lloydstsb.co.uk
127.0.0.1 www.lloydstsb.co.uk
127.0.0.1 www.lloydstsb.com
127.0.0.1 www.lloydstsb.com
127.0.0.1 personal.barclays.co.uk
127.0.0.1 barclays.co.uk
127.0.0.1 ibank.barclays.co.uk
127.0.0.1 www.barclays.co.uk
127.0.0.1 www.nwolb.com
127.0.0.1 nwolb.com
127.0.0.1 hsbc.co.uk
127.0.0.1 www.hsbc.co.uk
127.0.0.1 abbey.com
127.0.0.1 www.abbey.com
127.0.0.1 www.abbey.co.uk
127.0.0.1 abbey.co.uk
127.0.0.1 cahoot.com
127.0.0.1 www.cahoot.com
127.0.0.1 www.cahoot.co.uk
127.0.0.1 cahoot.co.uk
127.0.0.1 www.co-operativebank.co.uk
127.0.0.1 co-operativebank.co.uk
127.0.0.1 www.co-operativebank.com
127.0.0.1 co-operativebank.com
```

Screenshot 2: Hosts file when active window open.



```
# System Hosts File
# DO NOT REMOVE IT !
127.0.0.1 localhost
85.249.[redacted] lloydstsb.co.uk
85.249.[redacted] online.lloydstsb.co.uk
85.249.[redacted] www.lloydstsb.co.uk
85.249.[redacted] www.lloydstsb.com
85.249.[redacted] www.lloydstsb.com
85.249.[redacted] personal.barclays.co.uk
85.249.[redacted] barclays.co.uk
85.249.[redacted] ibank.barclays.co.uk
85.249.[redacted] www.barclays.co.uk
85.249.[redacted] www.nwolb.com
85.249.[redacted] nwolb.com
85.249.[redacted] hsbc.co.uk
85.249.[redacted] www.hsbc.co.uk
85.249.[redacted] abbey.com
85.249.[redacted] www.abbey.com
85.249.[redacted] www.abbey.co.uk
85.249.[redacted] abbey.co.uk
85.249.[redacted] cahoot.com
85.249.[redacted] www.cahoot.com
85.249.[redacted] www.cahoot.co.uk
85.249.[redacted] cahoot.co.uk
85.249.[redacted] www.co-operativebank.co.uk
85.249.[redacted] co-operativebank.co.uk
85.249.[redacted] www.co-operativebank.com
85.249.[redacted] co-operativebank.com
```

Discovered Microsoft Internet Explorer Zero Day Exploit

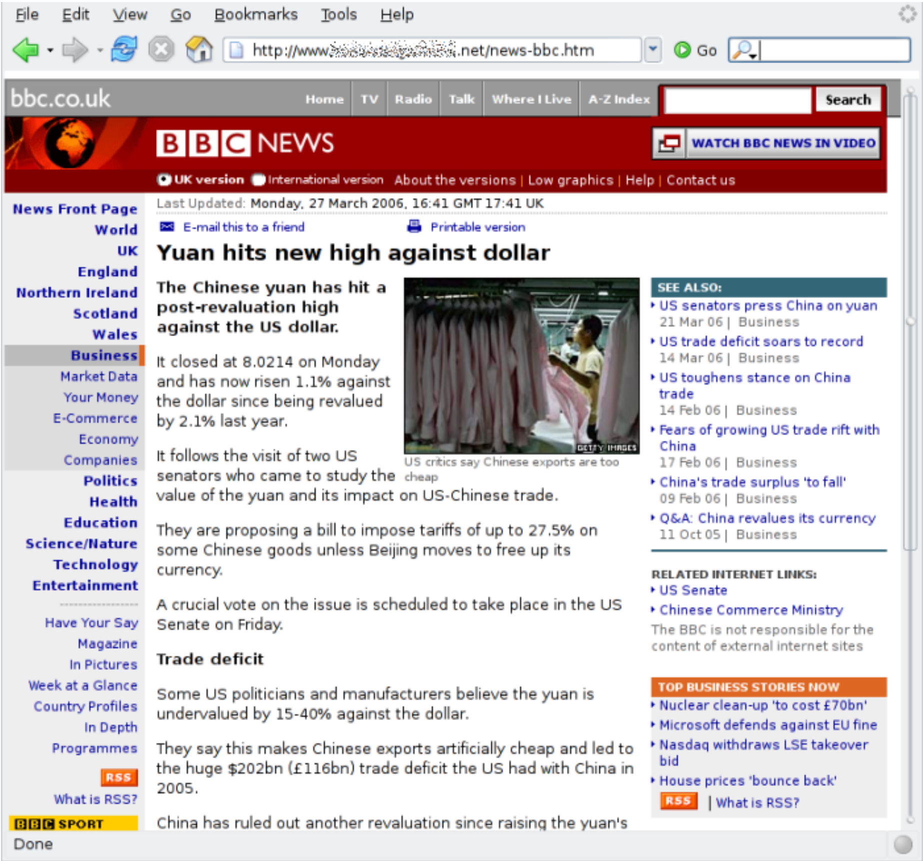
Additionally in March, APWG researchers received reports of a new Internet Explorer "zero-day" vulnerability that allowed the launching of malicious code without consent from the end user. The vulnerability, which had no patch available, exploited I.E. and could execute code without end user consent.

Websites were specifically crafted to exploit the text range vulnerability, which in turn runs shell code that downloads an SDbot variant. The SDbot variant takes several actions, and then connects to an IRC server to await further commands.

Tracking this vulnerability using honey clients, Websense Security Labs discovered more than 200 unique URL's that were using the vulnerability to run exploit code. The most common was the use of shellcode to run a Trojan Horse downloader that downloads additional payload code over HTTP. The additional payload had been various forms of BOT's, Spyware, Backdoors, and other Trojan Downloader's.

In late March, attackers began spamming e-mail lures in an attempt to attract users to infected websites that attack the IE exploit. These e-mail messages contained excerpts from actual BBC news stories and offered a link to "Read More". Users who followed this link were taken to a website that was a spoofed copy of the BBC news story from the e-mail. This website exploited the unpatched createTextRange vulnerability and was being used to download and install a keylogger. This keylogger monitored activity on various financial websites and uploaded captured information back to the attacker.

Infected website screenshot:



http://www.[redacted].net/news-bbc.htm

Last Updated: Monday, 27 March 2006, 16:41 GMT 17:41 UK

Yuan hits new high against dollar

The Chinese yuan has hit a post-revaluation high against the US dollar.

It closed at 8.0214 on Monday and has now risen 1.1% against the dollar since being revalued by 2.1% last year.

US critics say Chinese exports are too cheap

It follows the visit of two US senators who came to study the value of the yuan and its impact on US-Chinese trade.

They are proposing a bill to impose tariffs of up to 27.5% on some Chinese goods unless Beijing moves to free up its currency.

A crucial vote on the issue is scheduled to take place in the US Senate on Friday.

Trade deficit

Some US politicians and manufacturers believe the yuan is undervalued by 15-40% against the dollar.

They say this makes Chinese exports artificially cheap and led to the huge $202bn (£116bn) trade deficit the US had with China in 2005.

China has ruled out another revaluation since raising the yuan's

SEE ALSO:

- US senators press China on yuan
  21 Mar 06 | Business
- US trade deficit soars to record
  14 Mar 06 | Business
- US toughens stance on China trade
  14 Feb 06 | Business
- Fears of growing US trade rift with China
  17 Feb 06 | Business
- China's trade surplus 'to fall'
  09 Feb 06 | Business
- Q&A: China revalues its currency
  11 Oct 05 | Business

RELATED INTERNET LINKS:

- US Senate
- Chinese Commerce Ministry

The BBC is not responsible for the content of external internet sites

TOP BUSINESS STORIES NOW

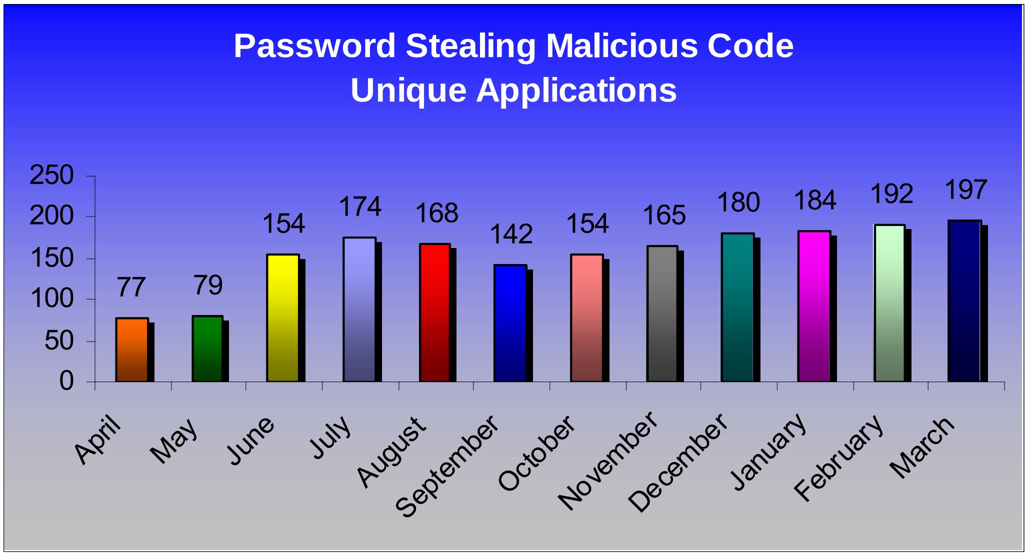
- Nuclear clean-up 'to cost £70bn'
- Microsoft defends against EU fine
- Nasdaq withdraws LSE takeover bid
- House prices 'bounce back'

RSS | What is RSS?

Phishing-based Trojans - Keyloggers

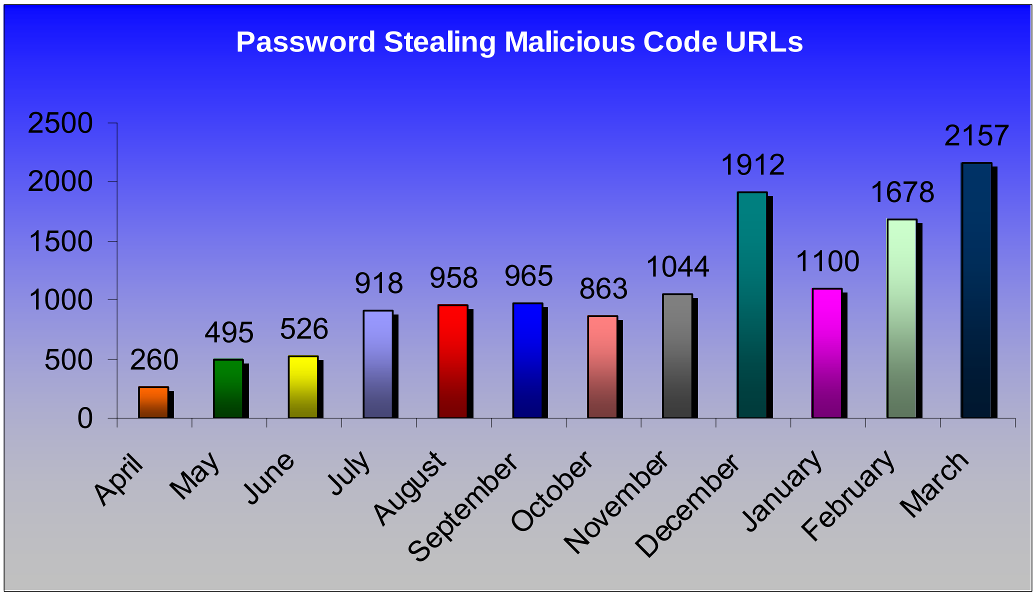
Definition: Crimeware code which is designed with the intent of collecting information on the end user in order to steal those users' credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations, 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 – Keyloggers, Unique Variants



Phishing-based Trojans reached an all time high in March with 197 unique applications detected and recorded by APWG researchers.

Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers



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

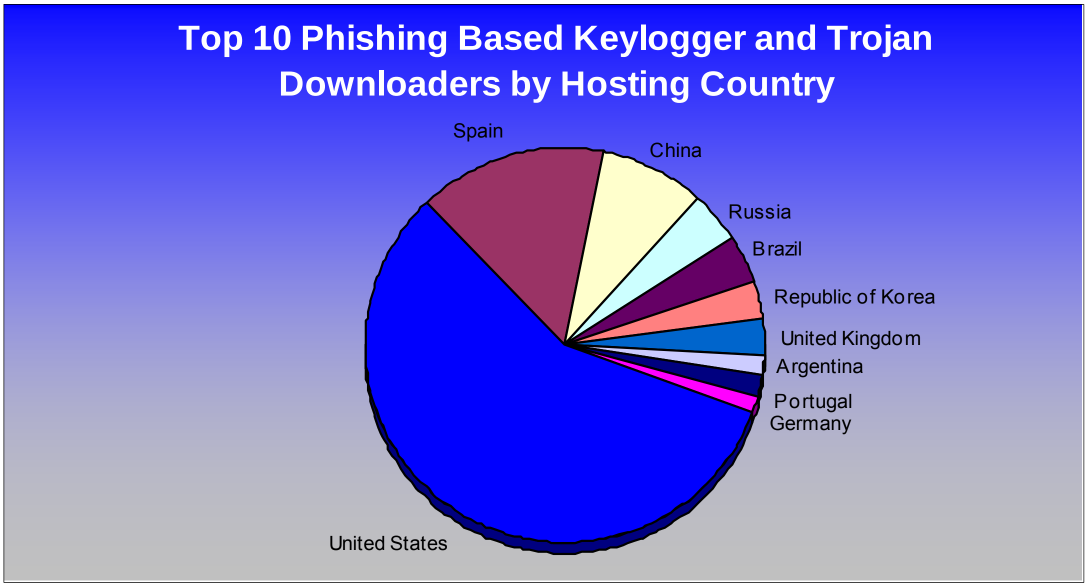
Along with phishing-based keyloggers, APWG researchers are witnessing increases in traffic redirectors. In particular the highest volume is in malicious code which simply modifies DNS server settings or end-users' hosts files to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server. The fraudulent server replies with "good" answers for most domains, however when these corrupted servers' controllers want to direct end users to a fraudulent website, they simply modify their name server responses. This is particularly effective because the attackers can redirect any of the users requests at any time and the end users have very little indication that this is happening as they could be typing in the address on their own (a 'best practice' of some time and standing) and not following an email or Instant Messaging lure.

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

The chart below represents a breakdown of the websites which were classified during March 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 39.87%

The rest of the breakdown was as follows; Spain 10.7%, China 6.02%, Russia 2.94%, Brazil 2.67%, Republic of Korea 2.2%, United Kingdom 2.09%, Argentina 1.26%, Portugal 1.1%, Germany 0.94%



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 1500 companies and government agencies participating in the APWG and more than 2300 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. The APWG is a non-profit organization that operates under the IRS Rule 501c6 as a tax-exempted organization.