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

Phishing Activity Trends

Report for the Month of January, 2007

Summarization of January Report Findings

► The number of phishing spoof sites reached an all time high of 29,930 unique phishing URLs reported in January, an increase of more than 25 percent from December and nearly 5 percent from the previous high in June, 2006. ► APWG saw a total of 135 brands being hijacked in January with numerous non-traditional websites spoofed such as social network portals and gambling sites. ► APWG notes that more brokerage company websites and many more International banks' brands were spoofed and hijacked in January. ► The number of crimeware variants reached an all time high in January of 345, up from 340 in December, 2006, rising 1.5% from that month, which was the previous highpoint for keylogging crimeware variants detected in a single month.

Phishing Defined and Report Scope

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 its member companies, Global Research Partners, the organization's website at http://www.antiphishing.org and 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.

Statistical Highlights for January 2007

• Number of unique phishing reports received in January:	**29930**
• Number of unique phishing sites received in January:	**27221**
• Number of brands hijacked by phishing campaigns in January:	**135**
• Number of brands comprising the top 80% of phishing campaigns in January:	**10**
• Country hosting the most phishing websites in January:	**United States**
• Contain some form of target name in URL:	**24.5 %**
• No hostname just IP address:	**18 %**
• Percentage of sites not using port 80:	**3.0 %**
• Average time online for site:	**4 days**
• Longest time online for site:	**30 days**

Methodology

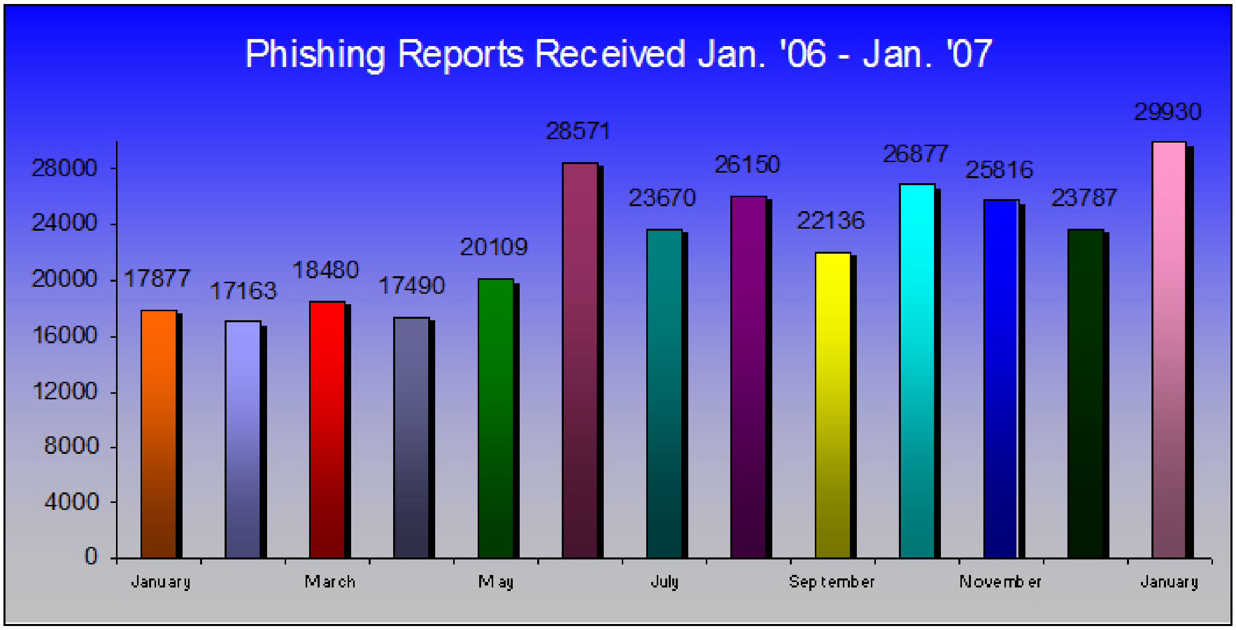
APWG is continuing to refine and develop our tracking and reporting methodology. We have recently re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent out to multiple users, directing them to 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).

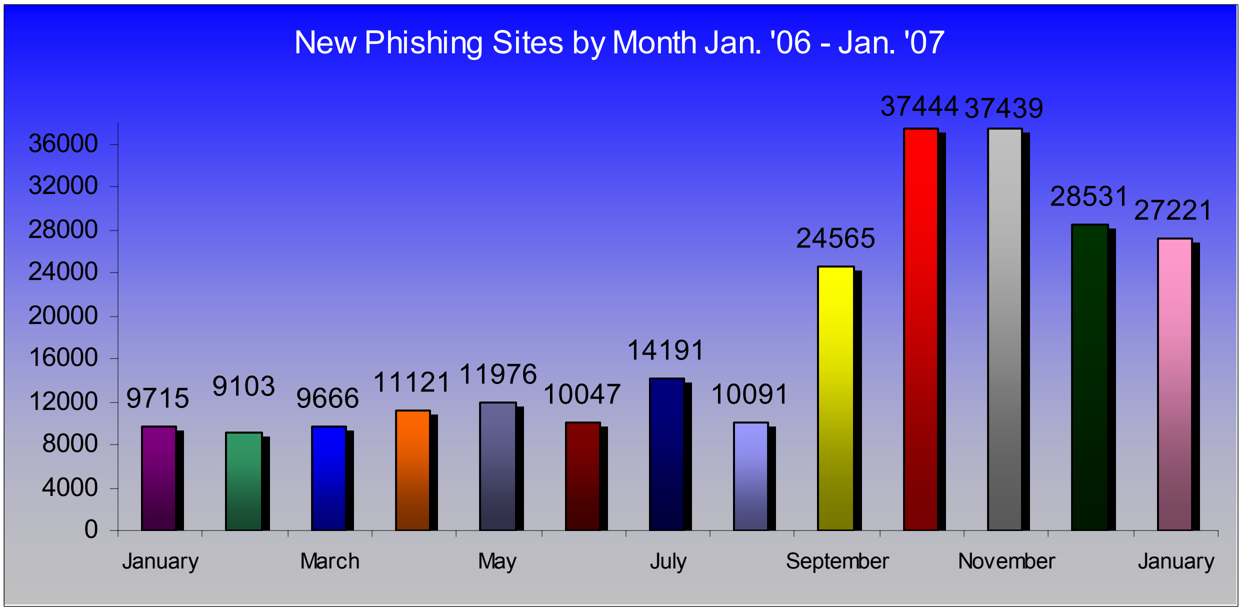
Phishing Email Reports and Phishing Site Trends for January 2007

The total number of *unique* phishing reports submitted to **APWG** in January 2007 was **29,930** – the highest recorded number by the APWG. This is a count of ***unique*** phishing email reports received by the APWG from the public, its member organizations and its research partners.



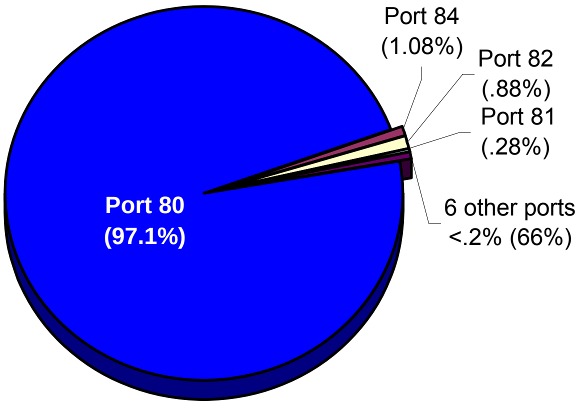
The **Phishing Attack Trends Report** is published monthly by the Anti-Phishing Working Group, an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. For further information, contact APWG Secretary General Peter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

The number of *unique* phishing websites detected by **APWG** was **27,221** in January 2007.



Top Used Ports Hosting Phishing Data Collection Servers in January 2007

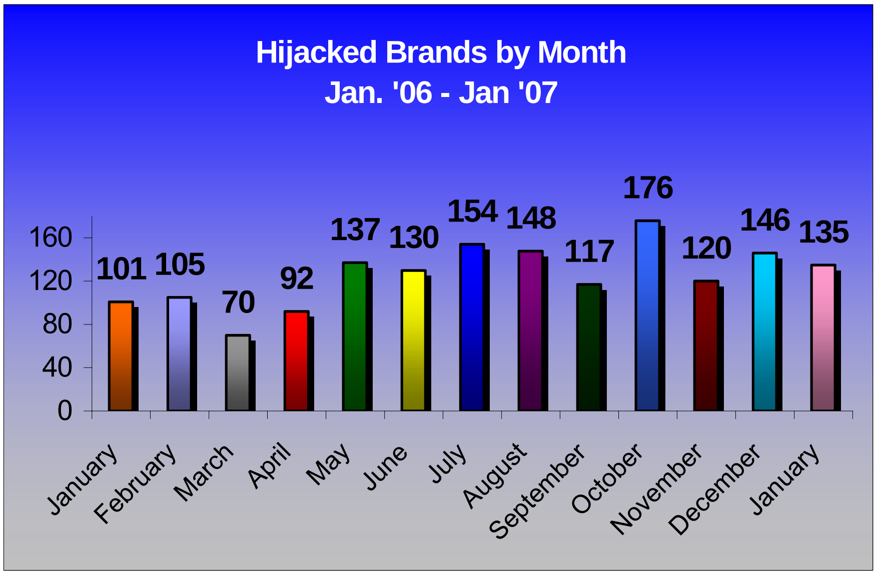
January saw a continuation of a trend of HTTP port 80 being the most popular port used at 97.1% of all phishing sites reported.



Brands & Legitimate Entities Hijacked By Email Phishing Attacks in January 2007

Number of Reported Brands

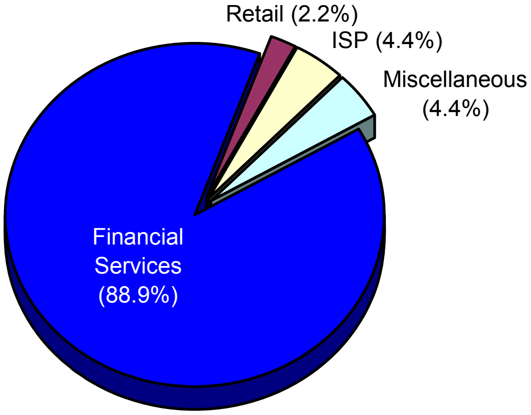
January 2007 showed the number of brands hijacked remaining steady to previous months. Of note, numerous non-traditional websites spoofed such as social networking portals and gambling sites were hijacked.



Most Targeted Industry Sectors in January 2007

Financial Services continue to be the most targeted industry sector at 88.9% of all attacks in the month of January.

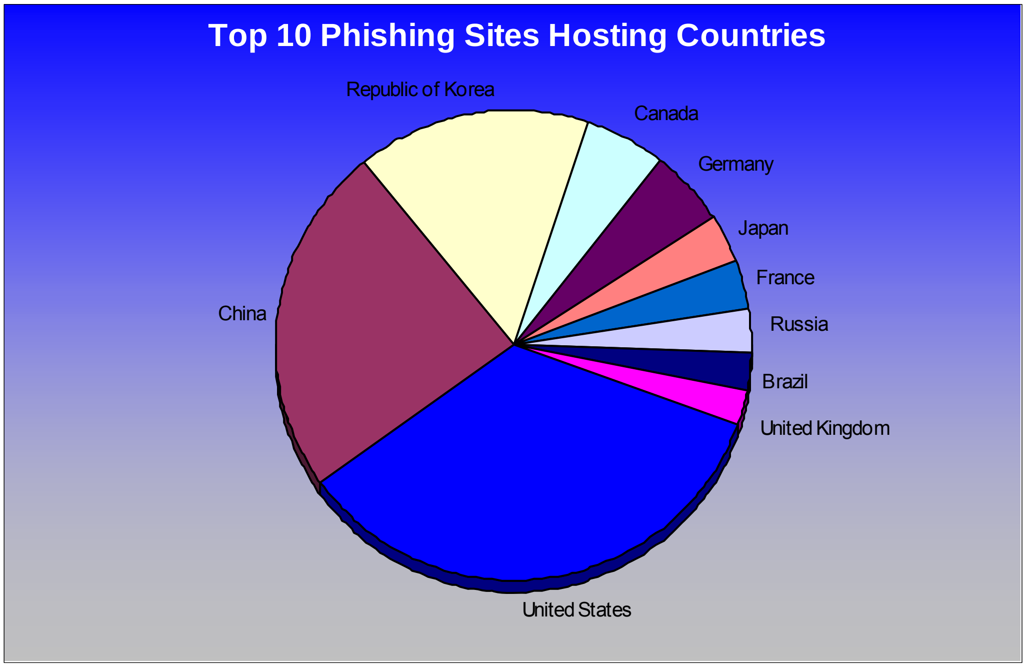
In addition, more brokerages websites and many more International banks and brands were spoofed and hijacked.



Web Phishing Attack Trends in January 2007

Countries Hosting Phishing Sites

In January, 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 24.27%. The rest of the top 10 breakdown is as follows:
China 17.23%, Republic of Korea 11%, Canada 4.05%, Germany 3.64% Japan 2.41%, France 2.33% Russia 2.15%, Brazil 1.9%, United Kingdom 1.67%.



PROJECT: Crimeware

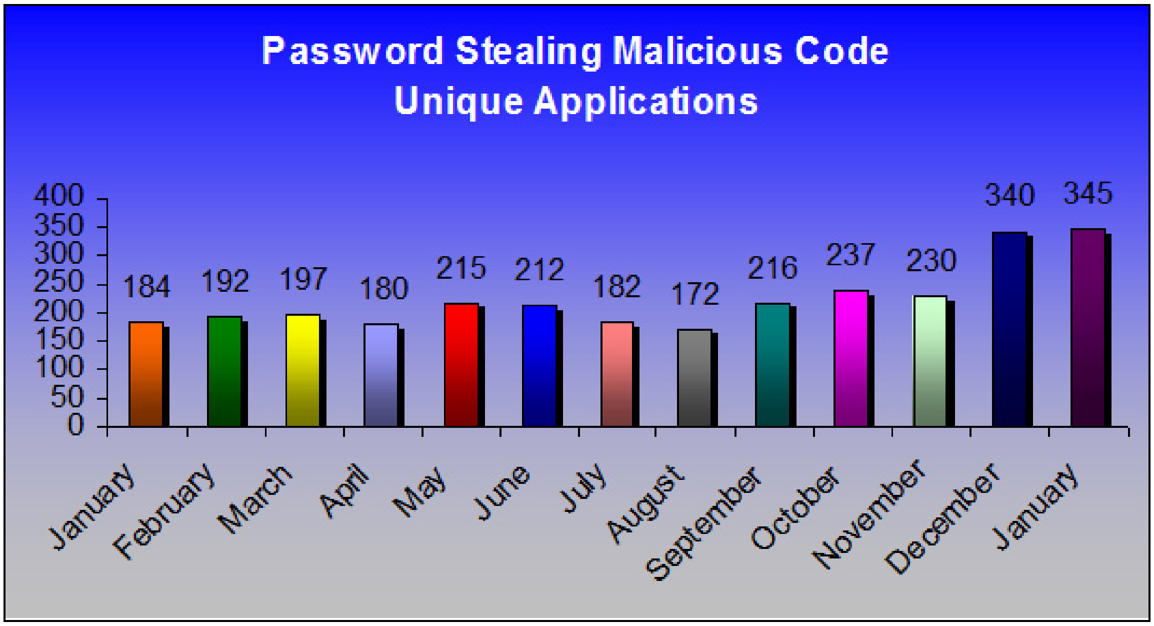
Crimeware Taxonomy & Samples According to Classification in January 2007

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

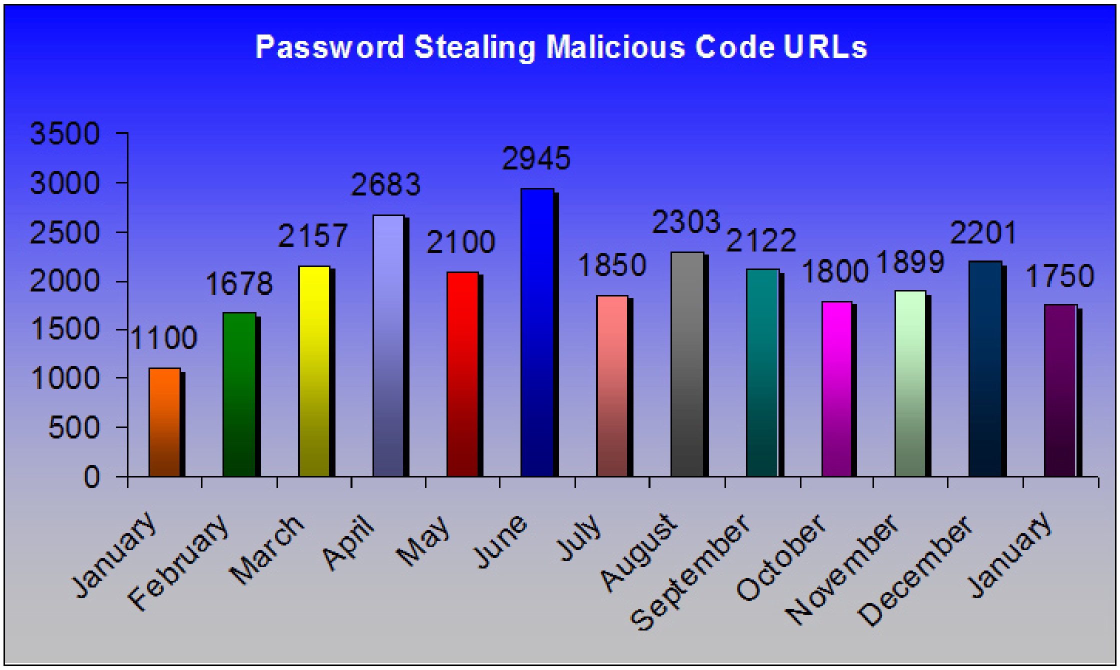
Phishing-based Trojans - Keyloggers

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 in January



Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers in January



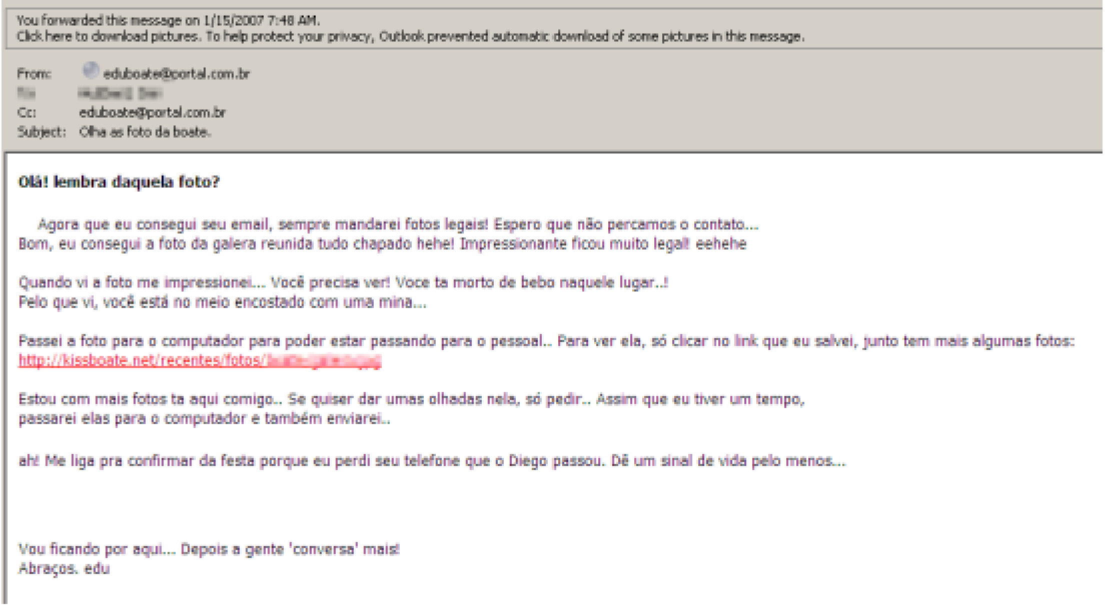
PROJECT Crimeware Field Sighting: Brazilian and Russian eGangs Collaborating

In January, Websense Security Labs discovered that Brazilian-based malicious code authors were utilizing a popular web exploit kit, which originated in Russia. This combination of the groups working together is relevant because previously we have not seen such collaboration. The Web Attacker toolkit allowed attackers to place code on their website to infect users when the site is visited. This toolkit is the most popular exploit kit on the web today.

Previously, Brazilian attacks mostly used deception as a means to dupe users into running their code. These attacks provide the largest volume of unique samples that we see on daily basis.

Of the sample attacks that we received, one is a fake news story about a robbery that claims to have a large reward for the capture of the criminal. Another attack is contained in an email asking you to view some photos.
In both examples, the attackers used email as the lure to attract visitors to their sites. Both sites contained live code that installed and downloaded information stealing malicious code, if the visitor's PC was not fully patched.

Attack example screenshot 1



You forwarded this message on 1/15/2007 7:48 AM.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: eduboate@portal.com.br
[redacted]
Cc: eduboate@portal.com.br
Subject: Olha as foto da boate.

Olá! lembra daquela foto?

Agora que eu consegui seu email, sempre mandarei fotos legais! Espero que não percamos o contato...
Bom, eu consegui a foto da galera reunida tudo chapado hehe! Impressionante ficou muito legal! eehehe

Quando vi a foto me impressionei... Você precisa ver! Voce ta morto de bebo naquele lugar..!
Pelo que vi, você está no meio encostado com uma mina...

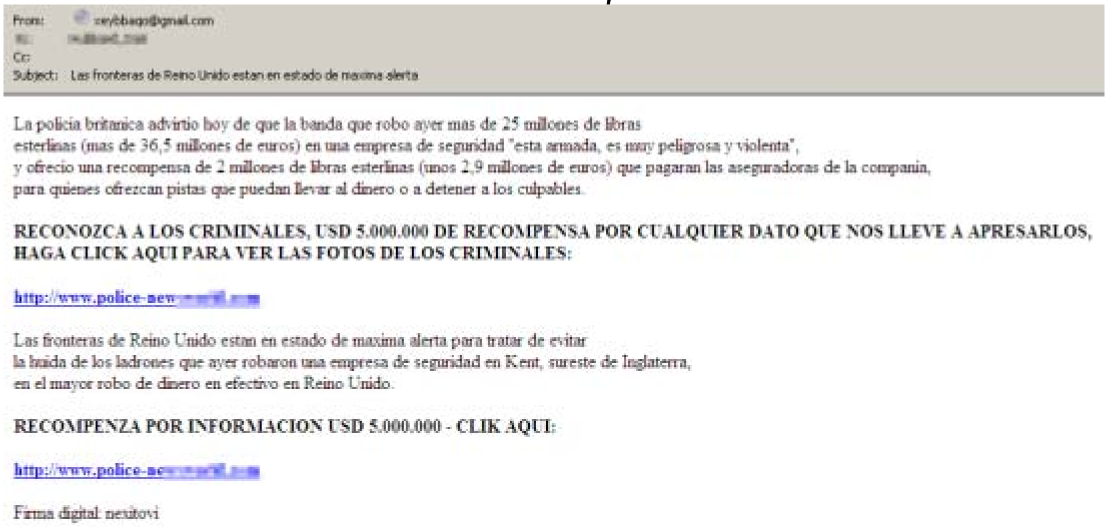
Passei a foto para o computador para poder estar passando para o pessoal.. Para ver ela, só clicar no link que eu salvei, junto tem mais algumas fotos:
http://kissboate.net/recentes/fotos/[redacted]

Estou com mais fotos ta aqui comigo.. Se quiser dar umas olhadas nela, só pedir.. Assim que eu tiver um tempo,
passarei elas para o computador e também enviarei..

ah! Me liga pra confirmar da festa porque eu perdi seu telefone que o Diego passou. Dê um sinal de vida pelo menos...

Vou ficando por aqui... Depois a gente 'conversa' mais!
Abraços. edu

Attack example screenshot 2



From: ceybbaqo@gmail.com
[redacted]
Cc:
Subject: Las fronteras de Reino Unido estan en estado de maxima alerta

La policia britanica advirtio hoy de que la banda que robo ayer mas de 25 millones de libras
esterlinas (mas de 36,5 millones de euros) en una empresa de seguridad "esta armada, es muy peligrosa y violenta",
y ofrecio una recompensa de 2 millones de libras esterlinas (unos 2,9 millones de euros) que pagaran las aseguradoras de la compania,
para quienes ofrezcan pistas que puedan llevar al dinero o a detener a los culpables.

RECONOZCA A LOS CRIMINALES, USD 5.000.000 DE RECOMPENSA POR CUALQUIER DATO QUE NOS LLEVE A APRESARLOS, HAGA CLICK AQUI PARA VER LAS FOTOS DE LOS CRIMINALES:

http://www.police-new[redacted]

Las fronteras de Reino Unido estan en estado de maxima alerta para tratar de evitar
la huida de los ladrones que ayer robaron una empresa de seguridad en Kent, sureste de Inglaterra,
en el mayor robo de dinero en efectivo en Reino Unido.

RECOMPENZA POR INFORMACION USD 5.000.000 - CLIK AQUI:

http://www.police-ne[redacted]

Firma digital: nesitovi

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.

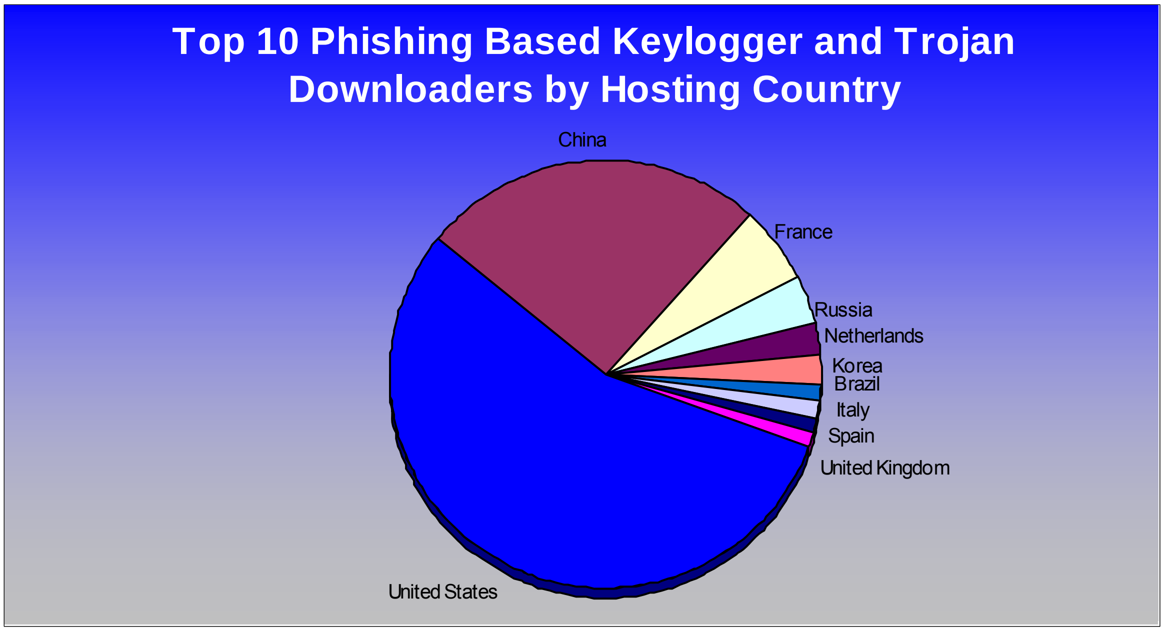
Along with phishing-based keyloggers we are seeing high increases in traffic redirectors. In particular the highest volume is in malicious code which simply modifies your DNS server settings or your hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server. The fraudulent server replies with "good" answers for most domains, however when they want to direct you to a fraudulent one, 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 and not following an email or Instant Messaging lure.

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

The chart below represents a breakdown of the websites which were classified during January 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 the top geographic location with 47%.

The rest of the breakdown was as follows; China 22%, France 5%, Russia 3%, Netherlands 2%, Korea 2%, Brazil 1%, Italy 1%, Spain 1%, United Kingdom 1%.



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 Peter Cassidy, APWG Secretary General at 617.669.1123 or pcassidy@antiphishing.org and Cas Purdy at 858.320.9493 or <cpurdy@websense.com>.

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 1600 companies and government agencies participating in the APWG and more than 2600 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, a 501c6 tax-exempted corporation, 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.