Anti-Phishing Working Group APWG

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

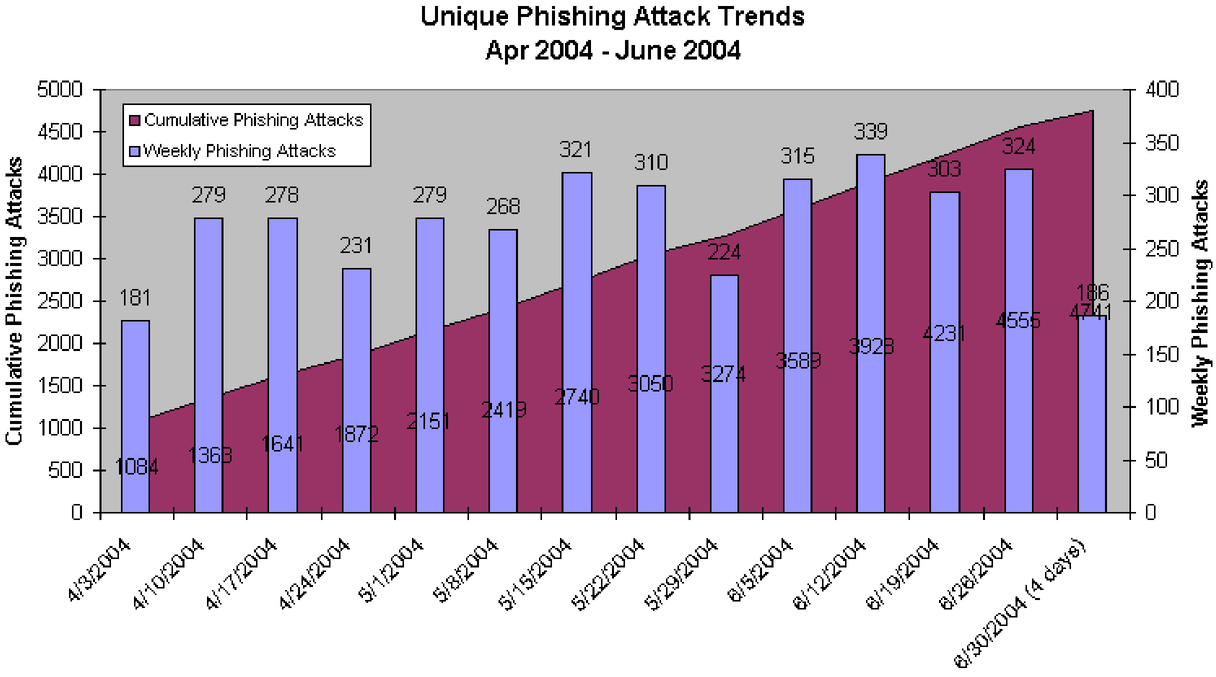
Phishing Attack Trends Report June, 2004

Phishing attacks use spoofed e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, data suggests that phishers are able to convince up to 5% of recipients to respond to them. The result of these scams is that consumers suffer credit card fraud, identity theft, and financial loss.

The Phishing Attack Trends Report analyzes phishing attacks reported to the Anti-Phishing Working Group via the organization's website, http://www.antiphishing.org or email submission via reportphishing@antiphishing.org. The Anti-Phishing Working Group phishing attack repository is the Internet's most comprehensive archive of email fraud and phishing attacks.

Highlights

• Number of unique phishing attacks reported in June:	**1422**
• Average monthly growth rate in phishing attacks through June:	**52%**
• Organization most targeted by phishing attacks in June:	**Citibank (492)**
• Percentage of phishing attacks using spoofed email addresses:	**92%**
• Country hosting the most phishing Web sites in June:	**USA (27%)**
• Average lifespan of a phishing site in June:	**2.25 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 Kendra Boccelli at kboccelli@mac.com or +1 978-499-0844.

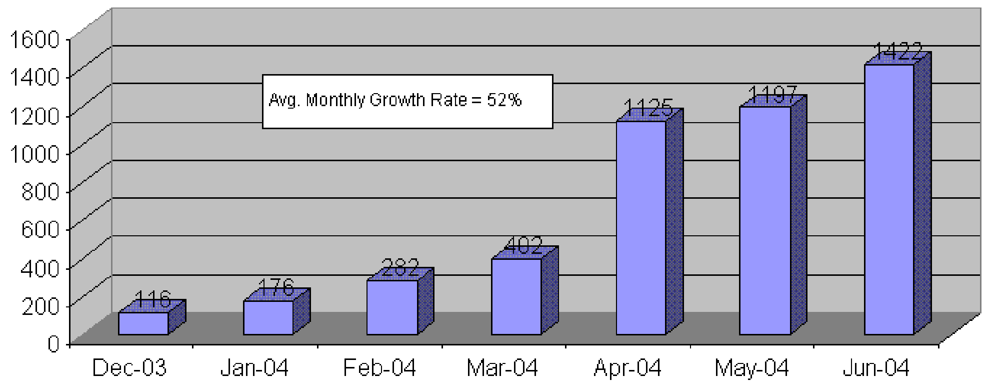
The following companies have donated analysis for the Phishing Attack Trends Report:

TUMBLEWEED COMMUNICATIONS WEBSENSE.

Email Phishing Attack Trends

In June, there were 1422 new, unique phishing attacks reported to the Anti-Phishing Working Group. This was a 19% increase over the number of attacks reported in May (1197). The average number of phishing attacks per day in June was 47.4 (up significantly from the 38.6 per day for May). Analyzing this information on a weekly basis shows every week in June averaged over 300 attacks, with the last 4 days of June on track to continue this trend.

Monthly Unique Phishing Attacks



Who Is Being Targeted By Email Phishing Attacks?

Most-Targeted Companies

In June, Citibank was (once again) the company whose brand was hijacked most often by phishers, followed by eBay and U.S. Bank. Notable growth rates in attacks in the month of June include Citibank (33% growth compared to May), U.S. Bank (50% growth), Fleet (67% growth), and the addition of FirstUSA as a new phishing target, with 10 attacks. Several companies experienced declining attacks, including Visa with a 57% reduction, and AOL with a 17% reduction.

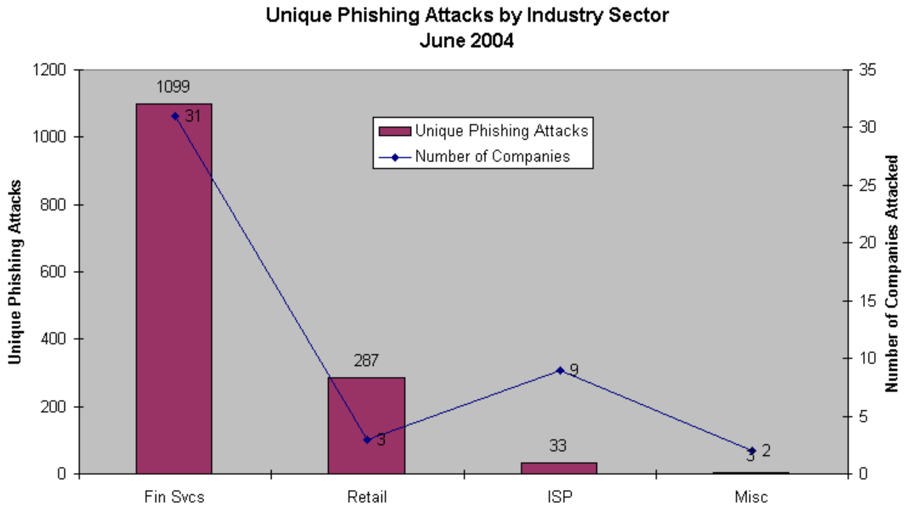
Unique Phishing Attacks by Targeted Company

Phish Target	Jun-04	May-04	Apr-04	Mar-04	Feb-04	Jan-04	Dec-03
Citibank	492	370	475	98	58	34	17
eBay	285	293	221	110	104	51	33
U.S. Bank	251	167	62	4	0	2	0
Paypal	163	149	135	63	42	10	16
Fleet	55	33	28	23	9	2	1
LLoyds	24	17	15	4	0	1	1
Barclays	19	15	31	11	6	1	1
AOL	14	17	9	10	10	35	4
Halifax	11	9	6	1	0	1	0
Westpac	11	12	17	10	0	3	1
FirstUsa	10	0	0	0	0	0	0
VISA	9	21	0	7	8	2	4
Earthlink	7	6	18	5	8	9	6
e-gold	6	3	5	2	2	0	2
Bank One	5	6	4	5	0	0	1
Bendigo	5	1	0	0	0	0	0
HSBC	5	3	3	4	0	1	0
MBNA	4	1	2	0	2	0	0
Suntrust	4	1	5	1	0	0	0
Verizon	4	2	0	0	0	0	0

A “unique phishing attack” in this analysis is defined as a single email blast sent out at one time, targeting one company or organization, and having one unique subject line. Note that phishers are starting to use common spam techniques to get these emails past enterprise spam filters, including using multiple different subject lines for a single attack, so the absolute numbers of phishing attacks may be slightly overestimated for some companies, particularly the top targets.

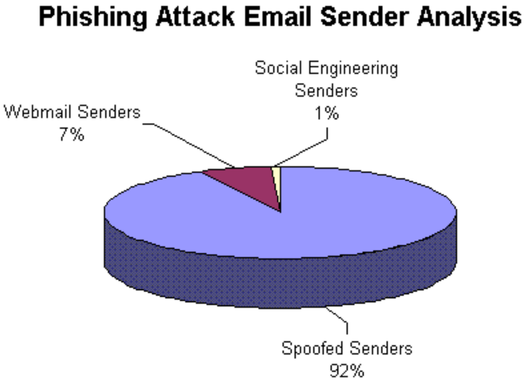
Most-Targeted Industry Sectors

The most targeted industry sector for phishing attacks continues to be Financial Services, from the perspective of total attacks as well as number of companies targeted. The Retail sector (primarily eBay) continues to follow, although there are significantly fewer retailers targeted. The Financial Services sector averaged over 35 reported phishing attacks per company in June.


Unique Phishing Attacks by Industry Sector
June 2004

Email Sender Analysis

In analyzing the "From" address used by phishers for June attacks, we found that at least 92% of them were 'spoofed', or forged. This was down slightly from May, where 95% of attacks used spoofed email addresses. Once again, only a very small percentage of phishing emails actually use "social engineering" email addresses or non-disguised Webmail addresses.


Phishing Attack Email Sender Analysis

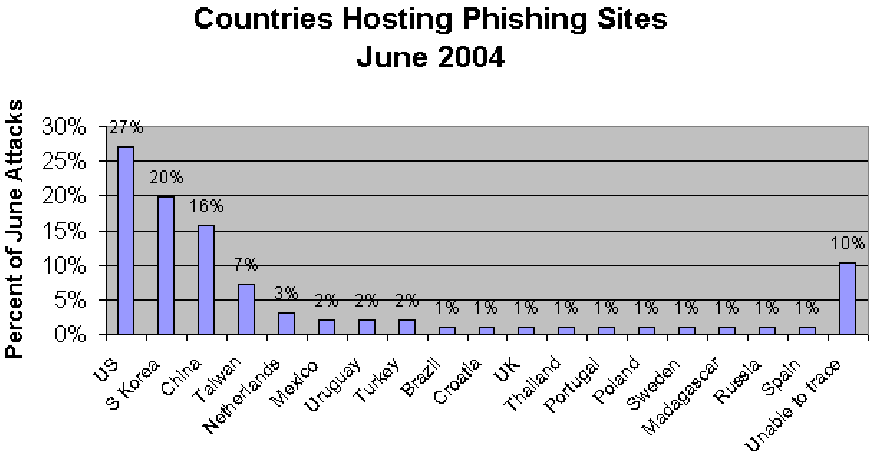
"Social engineering" email addresses use authentic Internet email domains that look similar to email addresses used by the companies they are spoofing. For example, one email address used to spoof Visa was "support@verify-visa.org". Note that this is NOT a valid email address for Visa, but is used to try to fool recipients via 'social engineering' into disclosing their credit card information. It is likely that some percentage of the social engineering and Webmail email addresses may also be forged, so the actual percentage of spoofed phishing emails is likely higher than 92%.

Web Phishing Attack Trends

Note - the following information reflects the analysis of phishing sites during the timeframe of June 15 through June 31.

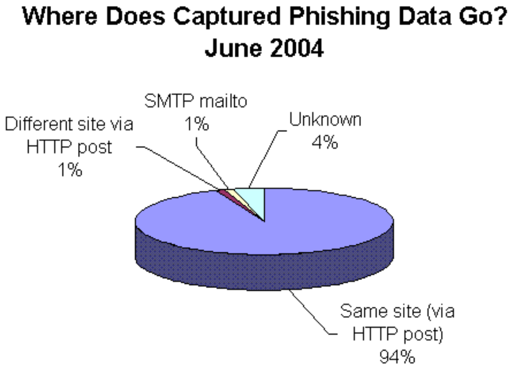
Countries Hosting Phishing Sites

While the United States is clearly the 'leader' in hosting phishing sites, it is interesting that a large number of phishing sites are hosted in Asia/Pacific countries. This may be due in part to a desire by phishers to host their forged sites in places where language and time zone barriers make it more difficult for brand-owning companies to shut the sites down. Analysis indicates that approximately 25% of phishing websites are hosted on hacked Web servers, unbeknownst to their owners.



Follow the Money Trail

By figuring out where captured financial information is sent once it is captured from phishing victims, law enforcement agencies are better able to track down the "money trail" and prosecute these criminals. The vast majority of information captured from phishing victims is saved to the local web server that hosts the phishing site, and is retrieved periodically by the phisher. Only a small percentage of this information is automatically sent to some other site or email address. The next step in following the money trail is therefore to trace from what location phishers are logging into phishing site servers to transfer this data.



Phishing Site Lifecycle

The average “life span” for phishing sites, measured by how long they continue to respond with content, is 2.25 days. The longest-lived phishing site in this limited analysis sample is 15 days. We anticipate getting better site lifecycle data as we accumulate more time series data in the coming months.

Anatomy of a Phish

In the middle of June we started investigating one particular phishing attack. What is interesting from this analysis is that identical attack methods were used to exploit two different Banks, even though the phishing attacks were hosted in different locations over time. We feel this indicates the participation of at least one well-orchestrated, systematic criminal organization in the phishing world.

Date	***Hosting Location***	***Site Information***
June 22	USA, ISP in Plano Texas	http://199.34.XXX.12:4903/target/index.htm
June 25	Uruguay	http://148.244.XXX.93:4903/target/index.htm
June 28	S Korea	http://210.105.XXX.41:4903/target/index.htm
June 29	S Korea	http://210.96.XXX.117:4903/target/index.htm
June 30	S Korea	http://211.232.XXX.227:4901/target/index.htm
June 31	USA, ISP Dial-up	http://64.163.XXX.154:4903/target/index.htm
July 3	S Korea	http://211.114.XXX.74:4903/cfm/index.htm

Common Site Characteristics

- All sites were hosted on machines that appear to have been exploited by the attacker.
- All sites were on hosts that did not have domains registered for them.
- All sites were run on non-port 80. Most were on port 4903, but we saw two on port 4901.
- All sites were used to exploit financial institutions.
- While some “lures” came in via email as an image map other came is as emails with encoded URL’s in the JavaScript.
- All sites used JavaScript to popup a page on top of the original site with the menu items stripped off.

All of the sites in this analysis were answering as the “SHS” web server. This appears to be a web server called the Small HTTP Server (see: http://home.lanck.net/mf/srv/index.htm). One hypothesis about this attack is that it uses zombie machines, with the attacker using Trojan code that hits exploitable machines and installs the Small HTTP Server, running it for X days until the information is gathered.

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.

Lead investigator:
Dan Maier, dmaier@tumbleweed.com

Websense Security Team

Websense Security Team's mission is to discover, research, and investigate advanced Internet threats to protect employee computing environments.

Lead investigator:
Dan Hubbard, dhubbard@websense.com

For press inquiries, please contact Kendra Boccelli at kboccelli@mac.com or +1 978-499-0844.

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 currently over 200 member organizations participating in the APWG. 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 Web site 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 Web site 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.