Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

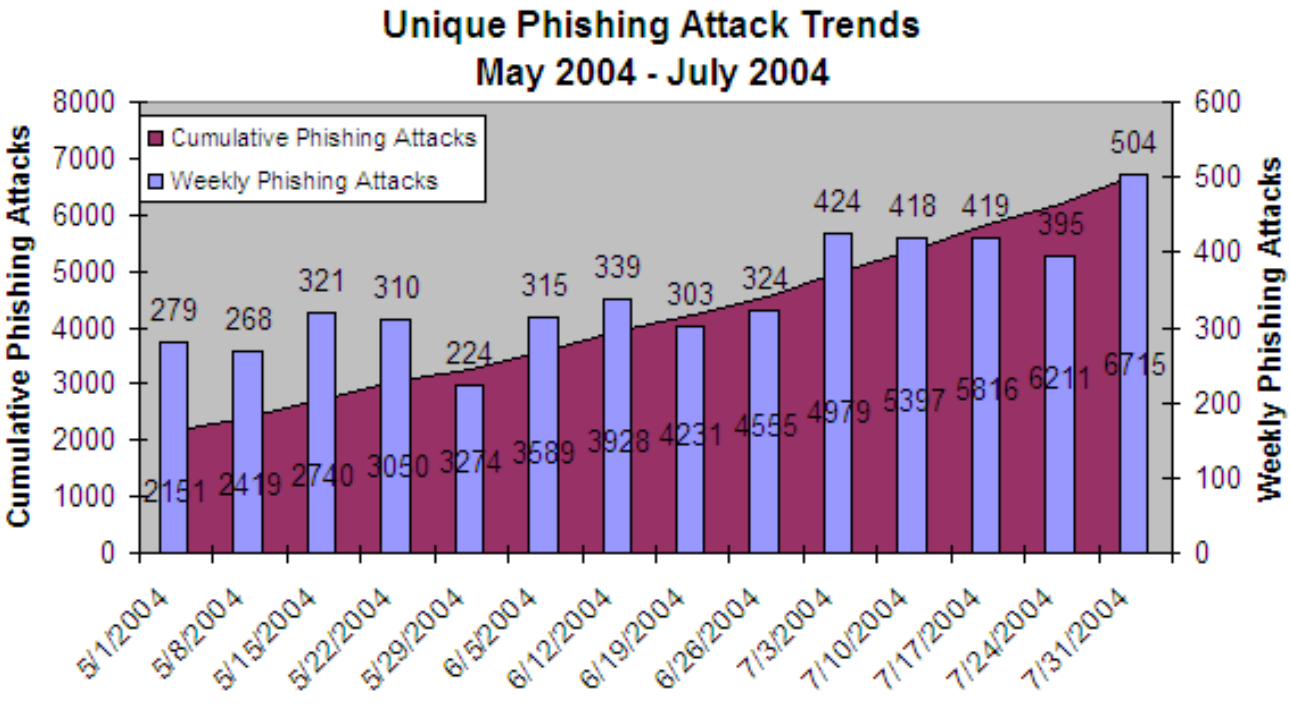
Phishing Attack Trends Report July, 2004

Phishing attacks use spoofed emails 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. As a result of these scams, an increasing number of consumers are suffering credit card fraud, identity theft, and financial loss.

The Phishing Attack 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 via reportphishing@antiphishing.org. The APWG phishing attack repository is the Internet's most comprehensive archive of email fraud and phishing attacks.

Highlights

- Number of unique phishing attacks reported in July: **1974**
- Average monthly growth rate in phishing attacks through July: **50%**
- Organization most targeted by phishing attacks in July: **Citibank (682)**
- Country hosting the most phishing Web sites in July: **USA (35%)**



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.

Analysis for the **Phishing Attack Trends Report** has been donated by the following companies:

TUMBLEWEED COMMUNICATIONS WEBSENSE.

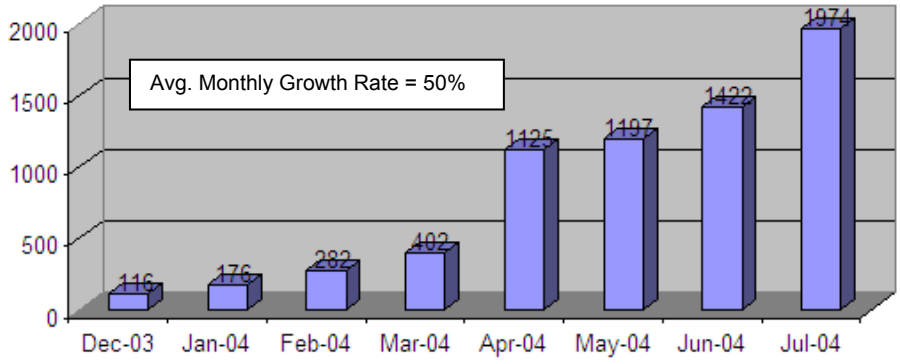
Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Email Phishing Attack Trends

In July, there were 1974 new, unique phishing attacks reported to the APWG. This was a 39% increase over the number of attacks reported in June (1422). The average number of phishing attacks per day in July was 63.7 (up significantly from the 47.4 per day for June). Analyzing this information on a weekly basis shows every week in July averaged over 395 attacks, with the last week of July breaking the 500 attack level.

Monthly Unique Phishing Attacks



Who Is Being Targeted By Email Phishing Attacks?

Most-Targeted Companies

In July, Citibank was - once again - the company whose brand was hijacked most often by phishers. U.S. Bank saw a dramatic 148% increase, which vaults them into second place by a significant margin over eBay, which saw a slight decrease in phishing attacks over the month. Other companies experiencing increases in phishing attacks include AOL, Suntrust, Earthlink, Wells Fargo and MBNA. Organizations experiencing decreases in phishing attacks include eBay, Paypal, and Fleet.

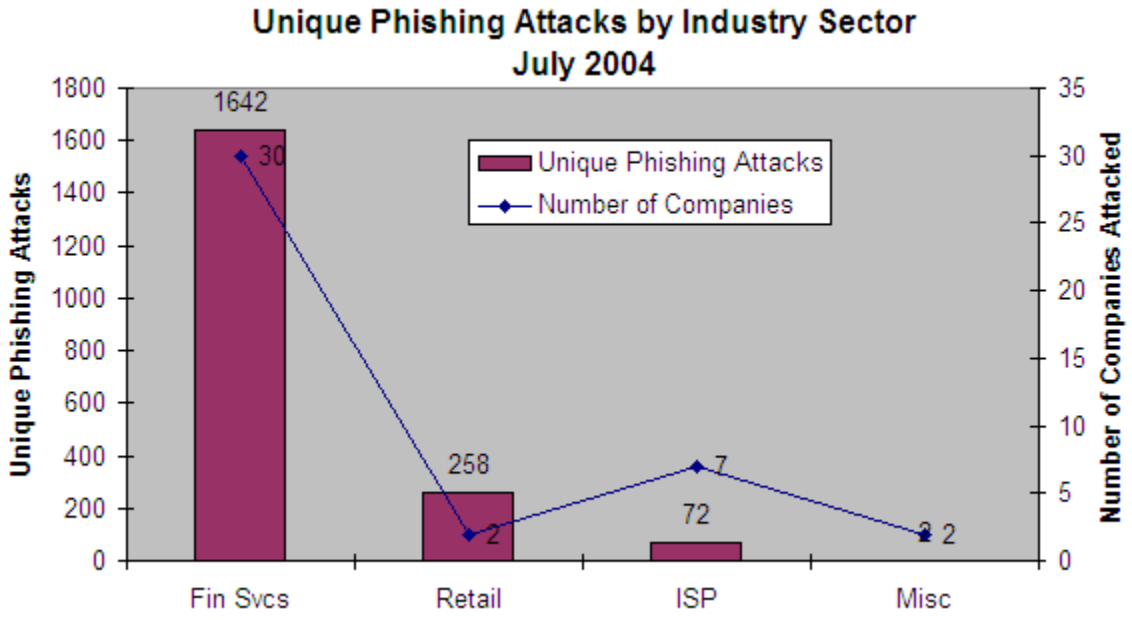
Unique Phishing Attacks by Targeted Company

Phish Target	Jun-04	Jun-04	May-04	Apr-04	Mar-04	Feb-04	Jan-04
Citibank	682	492	370	475	98	58	34
U.S. Bank	622	251	167	62	4	0	2
eBay	255	285	293	221	110	104	51
Paypal	147	163	149	135	63	42	10
AOL	41	14	17	9	10	10	35
Suntrust	25	4	1	5	1	0	0
LLoyds	23	24	17	15	4	0	1
Fleet	20	55	33	28	23	9	2
Barclays	17	19	15	31	11	6	1
Earthlink	15	7	6	18	5	8	9
Wells Fargo	12	1	0	0	12	0	0
Westpac	11	11	12	17	10	0	3
Halifax	10	11	9	6	1	0	1
MBNA	9	4	1	2	0	2	0
Postbank	9	0	0	0	0	0	0
VISA	9	9	21	0	7	8	2
Nationwide inter	8	2	10	0	0	0	0
HSBC	6	5	3	3	4	0	1
Verizon	6	4	2	0	0	0	0
Woolwich	6	3	3	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. Therefore, the absolute numbers of phishing attacks may be slightly overestimated for some companies, particularly the top targets.

Most-Targeted Industry Sectors

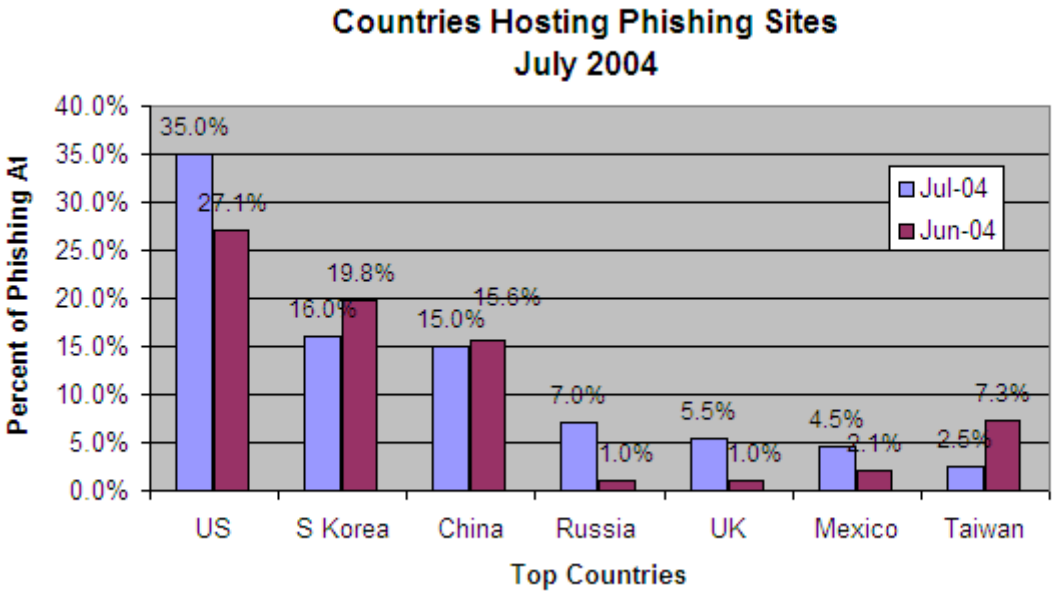
The most targeted industry sector for phishing attacks continues to be Financial Services, from the perspective of total attacks as well as number of companies targeted. This sector averaged almost 53 reported phishing attacks per day in July. The Retail sector (primarily eBay) continues to follow, although there are significantly fewer retailers targeted.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

The United States is once again the 'leader' in number of hosted phishing sites, with a growing percentage of the total. Other countries, including Russia, the UK and Mexico have shown significant increases in phishing sites hosted as well. Analysis indicates that approximately 35% of phishing websites are hosted on exploited machines, unbeknownst to their owners.



Fraud-Based Sites on the Rise

Over the month of July our research indicates a rise in fraud-based websites. Unlike phishing attacks that hijack the brand of established e-commerce or financial institutions, these sites are posing as generic e-commerce sites. The user believes they are ordering legitimate products or applying for a legitimate mortgage. The most common fraud-based sites seen during July were fake loan scams, mortgage frauds, online pharmacy frauds, and fake online banking institutions.

Phishing Site Lifecycle

The average "life span" for fraud sites, measured by how long they continue to respond with content, is 6.1 days. Note that this lifecycle combines identified phishing sites along with the "fraud" sites discussed above.

The longest-lived phishing site in this analysis sample is 31 days (in other words, the site was live during the entire month).

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 Labs

Websense Security Labs mission is to discover, investigate, and report on advanced Internet threats to protect employee computing environments.

Lead investigator:
Dan Hubbard, dhubbard@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 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.