Anti-Phishing Working Group

Phishing Attack Trends Report March, 2004

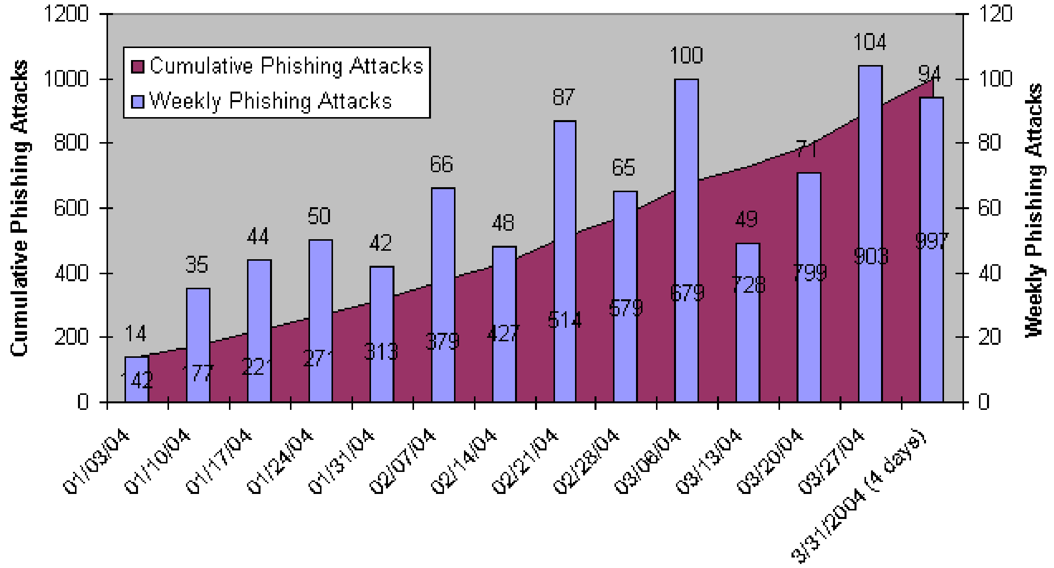
Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, 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 March:	**402**
• Average number of unique phishing attacks per day reported in March:	**13.0**
• Organization most targeted by phishing attacks in March:	**eBay**
• Business sector most targeted by phishing attacks in March:	**Financial Services**

Unique Phishing Attack Trends
Jan 2004 - Mar 2004



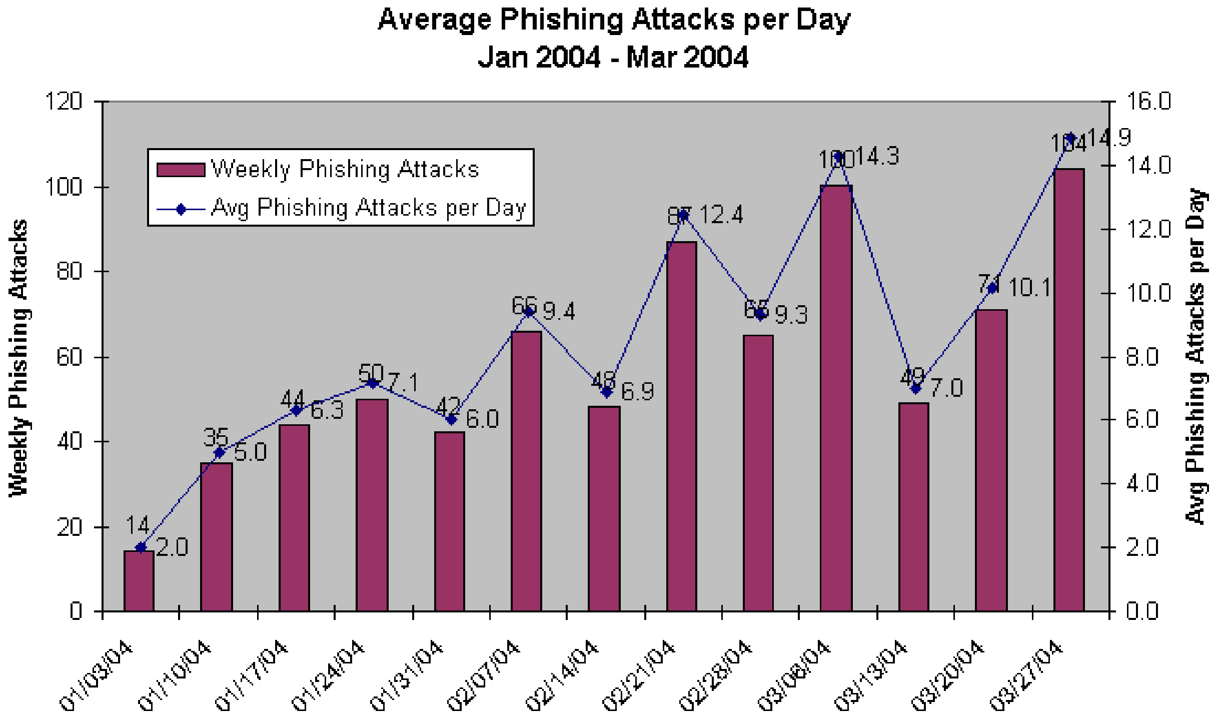
The **Phishing Attack Trends Report** is published monthly by the Anti-Phishing Working Group, an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. For further information, please contact Dan Maier at dmaier@antiphishing.org or +1 650-216-2078.

Analysis for the **Phishing Attack Trends Report** has been donated by the Tumbleweed Communications Message Protection Lab. The mission of the Tumbleweed Message Protection Lab is to analyze enterprise email threats (e.g. spam, email fraud, viruses, etc) and design new email protection technologies.

TUMBLEWEED
COMMUNICATIONS

Email Phishing Attack Trends

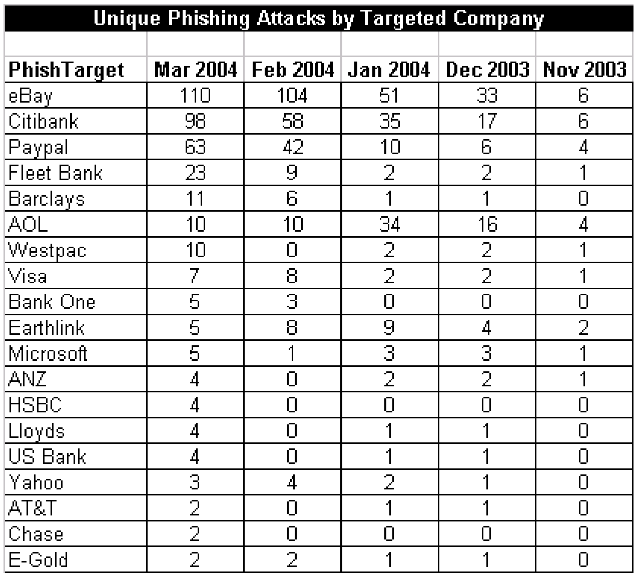
In March, there were 402 new, unique phishing attacks reported to the Anti-Phishing Working Group. This was a 43% increase over the number of attacks reported in February (282). The average number of phishing attacks per day grew significantly in March to 13.0. Analyzing this information on a weekly basis shows an increasing trend, with a new peak of 14.9 attacks per day in the third week of March. This marks the first time that we've seen more than 100 unique attacks in a week, and it happened twice in March (with the last four days of the month totaling 94 attacks, as well).



Who Is Being Targeted?

Most-Targeted Companies

The most targeted companies in March were largely similar to those targeted in previous months. eBay once again was the most targeted company, with 110 unique attacks that hijacked the company's brand. This represents minimal growth in attacks from the number seen in February (104). Citibank was once again the second most attacked company in March with 98 unique attacks hijacking its brand, a 69% growth in attacks. And once again, Paypal was the third most-phished company, with 63 unique attacks targeting it. Other notable attacks include a significant jump in the volume of attacks against Fleet Bank, Barclays, and Westpac.

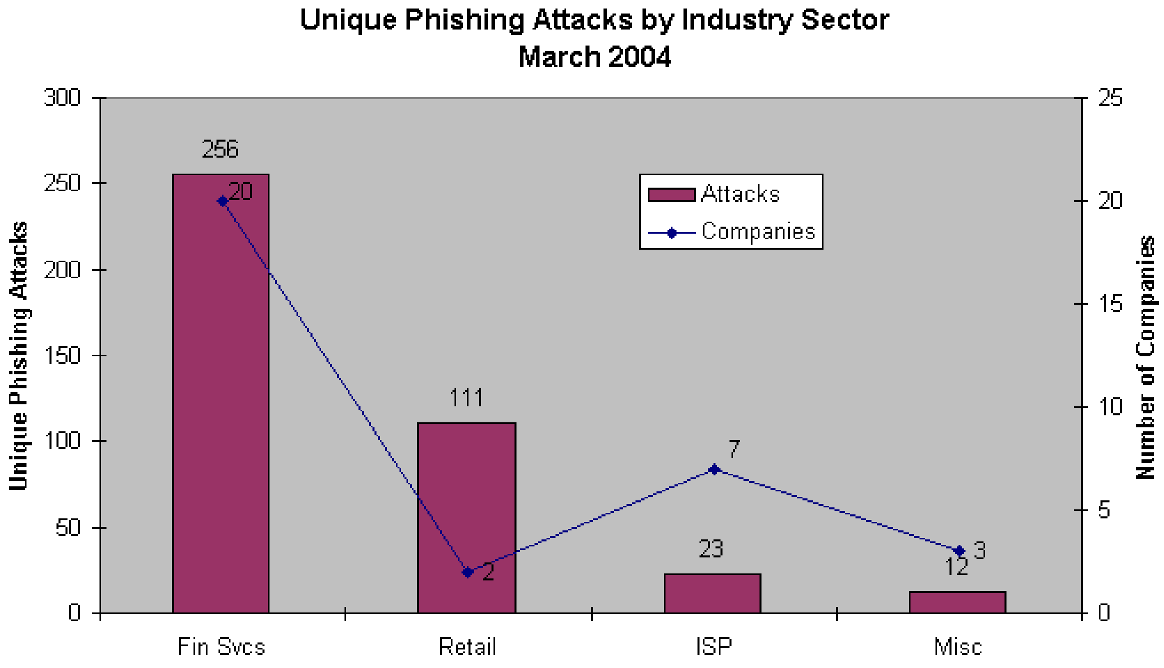


Unique Phishing Attacks by Targeted Company

PhishTarget	Mar 2004	Feb 2004	Jan 2004	Dec 2003	Nov 2003
eBay	110	104	51	33	6
Citibank	98	58	35	17	6
Paypal	63	42	10	6	4
Fleet Bank	23	9	2	2	1
Barclays	11	6	1	1	0
AOL	10	10	34	16	4
Westpac	10	0	2	2	1
Visa	7	8	2	2	1
Bank One	5	3	0	0	0
Earthlink	5	8	9	4	2
Microsoft	5	1	3	3	1
ANZ	4	0	2	2	1
HSBC	4	0	0	0	0
Lloyds	4	0	1	1	0
US Bank	4	0	1	1	0
Yahoo	3	4	2	1	0
AT&T	2	0	1	1	0
Chase	2	0	0	0	0
E-Gold	2	2	1	1	0

Most-Targeted Industry Sectors

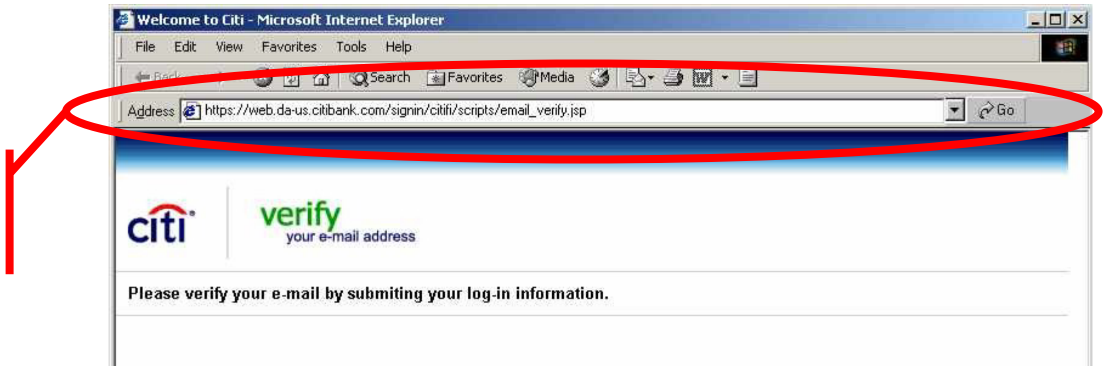
The most targeted industry sector for phishing attacks continues to be Financial Services, from the perspective of total attacks as well as number of companies targeted. The Retail sector (primarily eBay) continues to follow, although there are significantly fewer retailers targeted. The Financial Services sector averaged 8.3 phishing attacks reported per company in March.



APWG THREAT ADVISORY ALERT

Phishing Technique Replaces Web Browser Address Bar with Malicious JavaScript

A dangerous new type of phishing attack has been detected that replaces the "Address" bar at the top of a Web browser with a working fake, using JavaScript. This technique allows the phisher to display a completely fraudulent Web address URL, while taking the consumer to the phisher's spoofed site.



Address https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

Please verify your e-mail by submiting your log-in information.

Fake Address bar allows phisher to disguise the fact that the user is on a fraudulent Web site

This sophisticated new attack type does not make use of the MS Internet Explorer bug published last November, but extends the same visual effect to multiple browser platforms. It does so by automatically detecting the consumer's browser, and applying a custom JavaScript that replaces the look and feel of the Web address bar with an appropriately designed working fake.

How It Works

A consumer receives a forged email that pretends to be from a bank. The email claims that the recipient must verify their email address, and includes a web link. When clicked, the user's browser is opened, and they are taken to a Web page with an email verification form. The web link is HTML and the displayed text appears to link to the real bank's site.

However, the URL does not take the user to the bank's website. Instead, it takes him to a fraudster's site. The fraudulent site instantly detects the user's browser, and runs custom JavaScript code that removes the real address bar and replaces it with a fake address bar at the top of the browser window. The copy is exact. It has the "Address" field, it displays a URL web address that appears to be a secure link to the real bank (e.g. "https://"), and it has the "Go" button on the right hand side. In almost all respects, the web address and web page appear to be real. You can even type in the bank's web address directly into the fake Address bar. This is a live piece of JavaScript code, not a static fake Address bar image.

Implications

This is one of the most sophisticated phishing attacks that we have yet detected, and has serious security implications for consumers. Because the fake Address bar remains installed even after you leave the phisher's site, there is a possibility that a phisher could use this technique to secretly track every web site that you visit. Or even worse, a phisher could potentially employ a "man-in-the-middle" attack to see everything that you send or receive through your Web browser until you close it.

For More Information

APWG THREAT ADVISORY ALERT:
http://www.antiphishing.org/news/03-31-04_Alert-FakeAddressBar.html

Phishing Archive: Citibank - "Verify your E-mail with Citibank" (31-Mar-2004)
http://www.antiphishing.org/phishing_archive/Citibank_3-31-04.htm

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.