Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

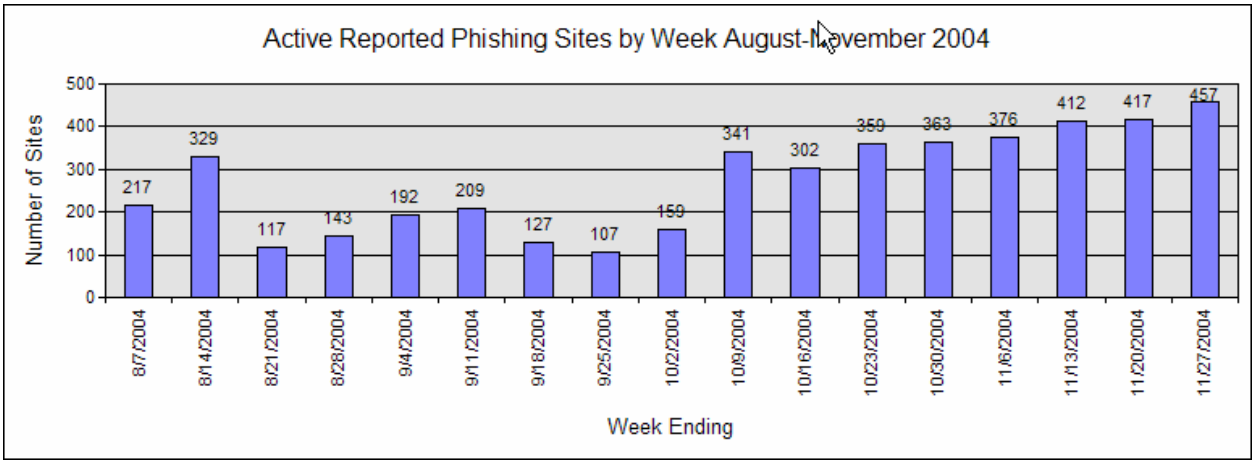
Phishing Activity Trends Report November, 2004

Phishing is a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them 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 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.

Highlights

- Number of active phishing sites reported in November: **1518**
- Average monthly growth rate in phishing sites July through November: **28%**
- Number of brands hijacked by phishing campaigns in November: **51**
- Number of brands comprising the top 80% of phishing campaigns in November: **6**
- Country hosting the most phishing websites in November: **United States**
- Contain some form of target name in URL **22.1 %**
- No hostname just IP address **67 %**
- Percentage of sites not using port 80 **19.2 %**
- Average time online for site **6.2 days**
- Longest time online for site **31 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 the APWG at press@antiphishing.org or Ronnie Manning at rmanning@websense.com or 858.320.9274.

Data and analysis for this **Phishing Attack Trends Report** has been donated by the following companies:

TUMBLEWEED COMMUNICATIONS

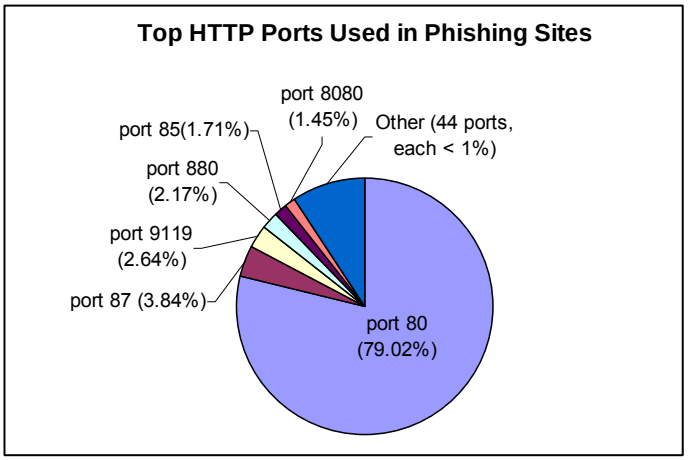
WEBSENSE.

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

APWG Trend Alert

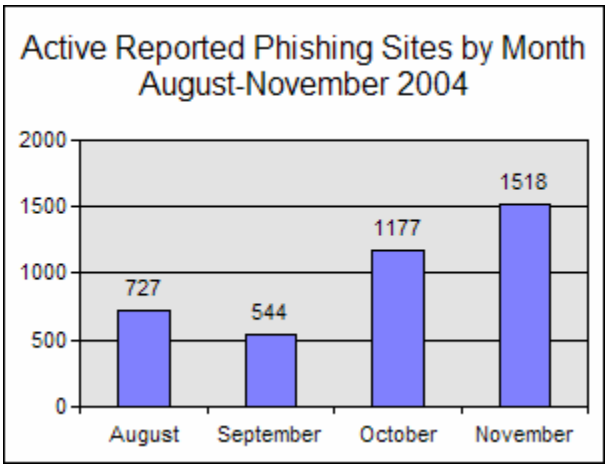
The rise in non-port 80 hosted sites and the number of sites which are hosting phishing attacks lead us to believe that the number of machines that are compromised and are being used to host these attacks is growing.



Email Phishing Attack Trends

In November, there were 8,459 new, unique phishing email messages reported to the APWG. This was nearly four times the number of unique reports received in August (2,158) and represents an average monthly growth rate of 34% since July (2,625).

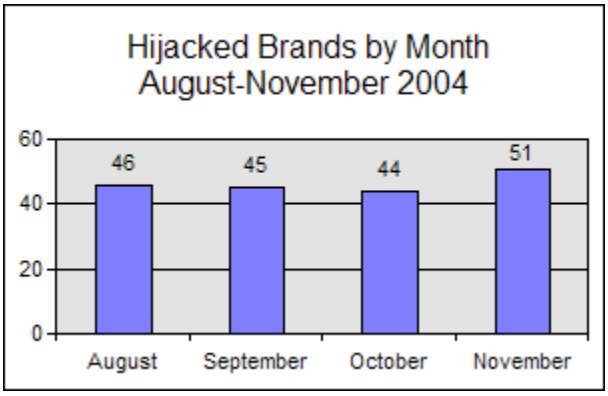
An analysis of the reported email messages reveals a similar trend in the number of unique baiting sites disguised within the messages. In November, there were 1,518 unique sites reported, a jump of 29% over October (1177) and a month-to-month growth rate of 28% since August (727).



What Brands Are Being Hijacked By Email Phishing Attacks?

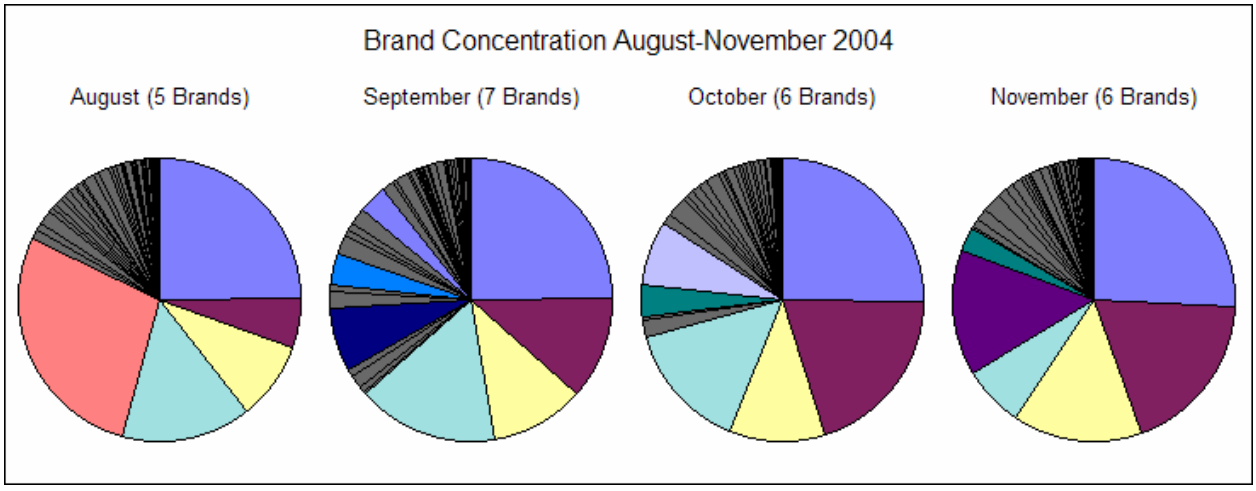
Number of Reported Brands

In November, all measures of phishing activity are increasing including the number of reported hijacked brands which rose to 51, including five brands first reported this month. This brings to 122 the total number of brands that have reportedly been hijacked since the APWG began examining phishing trends and reporting their findings in November of 2003.



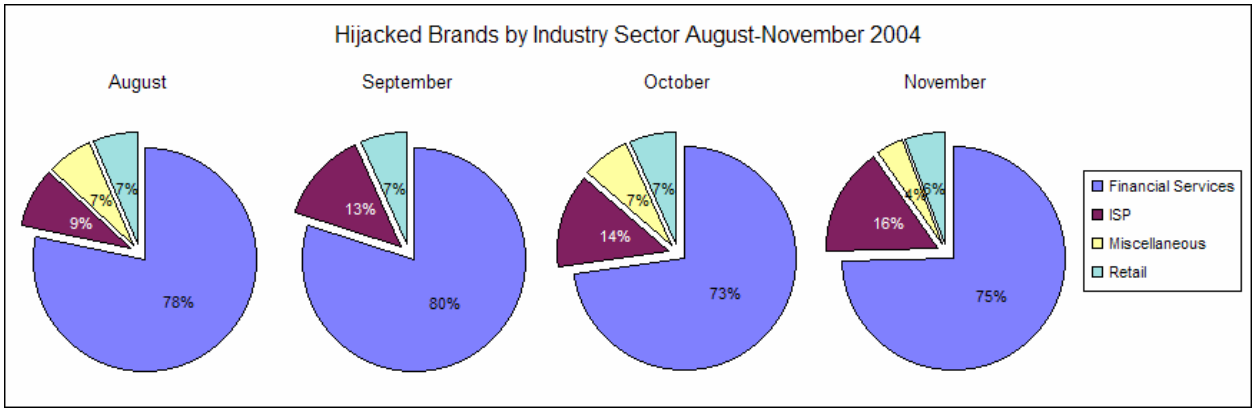
Brand Concentration

The figures below illustrate the concentration of phishing activity as reported against hijacked brands. The number of reported brands comprising the top 80% of all phishing activity has remained roughly stable in recent months, with six brands accounting for the bulk of phishing activity in November. Of the top six in November, however, only four appeared in the top six in October, so the breadth and specifics of attacks continues to shift from month to month. As always, consumers should maintain a sense of reasonable awareness while conducting business online.



Most-Targeted Industry Sectors

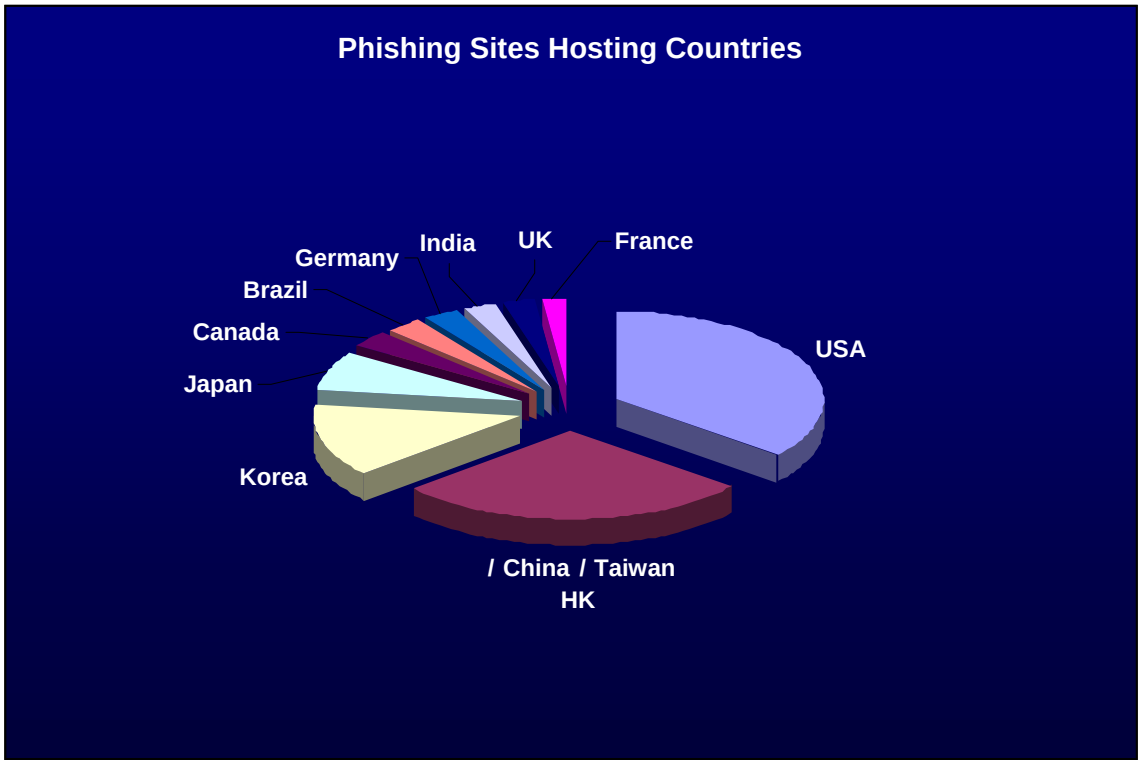
The most targeted industry sector for phishing attacks continues to be Financial Services, from the perspective of total number of unique baiting sites as well as number of companies targeted. This sector averaged 75% of all hijacked brands in November with four new institutions reported in the month. The ISP sector continues to grow with one new ISP appearing the reports for November and accounting for 16% of all attacks.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

Although the United States is still the top country for hosting phishing-based websites with 27%, we have seen a rise in sites hosted in China over the last month. This is mainly due to the large number of EarthLink and MSN attacks that will be discussed in greater detail later in this report. Percentages of phishing-based websites for other countries include: China 21%, Korea 10%, Japan 5.5%, Canada 2.6%, Brazil 2.1%, Germany 2.1%, India 1.84%, UK 1.76%, and France 1.54%. It should also be noted that the remaining sites were spread amongst 50 other countries, which is the largest amount of countries to date.



Phishing through Malicious Code on the Rise

We are starting to see increased use of attackers using malicious code in order to gain access to user credentials to banking sites and other pertinent information. There is a variety of attack vectors being used to run this code on the end users machines, however due to several un-patched documented vulnerabilities within web browsers, the web is the common source for these. Social engineering is commonly used within email to lure users to run programs and visit websites which are hosting malicious code. Although the characteristics of the sites containing malicious code are not all the same, most of them wait for end-users to access known financial and ecommerce sites and then either replace the site with their own hosted version or capture the keystrokes of the end-user. Keyloggers also have been part of many blended attacks and have spread through many recent highly publicized worms.

Watch for malicious code statistics and other details in upcoming reports.

Anatomy of a Phish Attack: EarthLink and MSN attacks

Starting the week of November 23rd, 2004, Websense® Security Labs™ received numerous reports and captured numerous emails which were attempting to dupe EarthLink customers into divulging their username, password, social security number, credit card, and other personal information. Starting November 29th, we started seeing the exact same characteristics of the attack aimed at a new target—MSN customers.

Over the last week we have continued researching the characteristics of the sites which are hosting these attacks and have compiled the following research.
*note: URLs have been removed to protect the end-users.

Introduction

Starting November 23rd we received hundreds of reports of a new EarthLink phishing attack. Reports are still coming in and several sites are still online. The research below outlines our opinion on some of the techniques on how the attacker(s) are compromising the machines and setting up their attacks.

Technical Details

All sites that are hosting the Earthlink attack are located in China in the 218 net blocks. We have identified hosts in the following networks:

- 218.201
- 218.104
- 218.28
- 218.8

Although most of the MSN sites were also in China, we have also seen some sites that are hosted in India in the 202.157 network block.
Host Details

- All hosts researched have the following ports open and receiving requests: 21, 221, 80, 280, 880, 25, and 225.
- All hosts are running a version of Microsoft® Windows Server with a variety of vulnerabilities. The most common is the IIS WebDAV exploit (see: http://www.microsoft.com/technet/security/bulletin/ms03-007.mspx).
- All hosts are running a small HTTP server in addition to IIS on port 880. The HTTP server (http://home.lanck.net/mf/srv/index.htm) has been used several times in the past to host phishing attacks on non port 80 sites. The small HTTP server was developed in Russia and has legitimate use, however the small profile of it and multiple features such as: built-in email capability, FTP, and CGI capability make it tool for phishers also. HTTP crawler returns:

  HTTP/1.1 200,SHS,Earthlink.net - Verify your account information

Error page when connecting to server which signifies the server type:

```
<br><center><table width=500 height=60 border=1 cellspacing=0
cellpadding=1><tr vallign=top cellpadding=0 cellspacing=0><td height=4
bgcolor=#8030e0> <table width=494 height=8 border=0 cellspacing=0
cellpadding=1><tr cellpadding=1 cellspacing=0><td bgcolor=#5030a0
width=60 height=4><font size=0 color=#ffffff
class=f3>Unregistred</font></td><td bgcolor=#6030b0 width=60
height=4><font size=0 color=#ffffff class=f3>copy</font></td><td
bgcolor=#7030c0 width=60 height=4 align=right><font size=0 color=#ffffff
clasinds=f3>of <b>Small</b></font></td><td bgcolor=#8030d0 height=4><font
size=0 color=#ffffff class=f3><b>HTTP server</b></font></td><td
bgcolor=#9030e0 width=60 height=4><font size=0 class=f3> </font></td><td
bgcolor=#a030f0 width=60 height=4><font size=0 class=f3> </font></td><td
bgcolor=#b030ff width=60 height=4><font size=0 class=f3> </font></td><td
bgcolor=#c0c0c0 width=12 height=4><a
href=http://srv.mf.inc.ru/news.htm><font size=0 color=#00c0f0
class=f3><b>/\\</b></font></a></td></tr></table></td></tr><tàòü
ðåêëàìó</font></b></a></td></tr></table></center><br>Connection closed by
foreign host.
```

Notice the following URL: http://srv.mf.inc.ru/news.htm. This will redirect you to: http://home.lanck.net/mf/srv/index.htm (The home of the small HTTP server).

- All hosts appear to be running FTP and email on non-standard ports in conjunction with the IIS server. These are running on the standard ports appended with a number 2 (example 225 instead of 25 and 221 instead of 21). When connecting to these ports you receive the following message:

```
$telnet 218.8.XXX.XXX 225
Trying 218.8.XXX.XXX
Connected to 218.8.XXX.XXX
Escape character is '^]'.
400 DETECTED HACKER
Connection closed by foreign host.
$telnet 218.8.XXX.XXX 221
Trying 218.8.XXX.XXX…
Connected to 218.8.XXX.XXX.
Escape character is '^]'.
HTTP/1.0 400
Content-Type: text/html
<hr><pre><font size=+2><b>
DETECTED HACKER
```

Conclusion

A network-based scanner was used to scan the 218 networks and identify hosts which are vulnerable to the IIS WebDAV exploits. We consistently see scans of this type on our network of Honey Pot machines. Characteristics are usually HTTP requests like the following (note: this was truncated).

```
XXX.XXX.XXX.XXX - - [22/Nov/2004:09:43:45 -0500]
"SEARCH
/\x90\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
```

Once the attacker identifies hosts which can be compromised, the small HTTP server is then installed with a standard configuration which allows the attacker to receive HTTP post information through a CGI script.

Most likely, the attacker then utilizes a BOT network to send massive amounts of emails to users, luring them to connect to one of the sites via an embedded URL. We have received several examples that are from spoofed email addresses, all coming from different machines.
Once a user clicks on the URL, the attacker then connects to the machine in one of three ways: through a known URL where all the account information is posted, to the compromised machine's FTP server, or automatically receives the details via email.

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:
John Thielens, johnt(at)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(at)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 639 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 and in June 2004 was incorporated as an independent corporation controlled by its steering committee and executives.