SecurityFocus

ARIS Top Ten 2001 Threats

Patches and Recommendations to Protect Your Enterprise

Executive Summary

In the heat of firewall breaches, worm propagation, and other malicious network traffic, it is difficult to assess the relative danger of individual threats. The SecurityFocus Threat Analyst Team has measured attacks from 2001 against each other to produce a list of the year's top threats. We have analyzed network attack data from March through December 2001 and have created a list of the top ten threats seen in the wild, including the systems they target and the vulnerabilities they exploit. We have created this list from actual network traffic gathered by the ARIS Threat Management System.

ARIS receives data from intrusion detection systems (IDSes) located in various demographic and geographic areas across the Internet. ARIS gathers, aggregates, and analyzes this data, creating a resource for subscribers and SecurityFocus analysts to track patterns of malicious network traffic. The information enhances security for networked systems by highlighting trends in software platforms that are heavily targeted for attacks, remote networks that are often sources of malicious traffic, and countries that are the source and destination of these attacks.

Throughout the document, you will see references to vulnerabilities and attack signatures. For clarity, these references are in the context of services offered by SecurityFocus. When we refer to a specific attack signature, we use the name of the attack as ARIS uses it. ARIS supports many IDSes, and maps the various signatures reported by these products to a common name, simplifying the process of aggregating the data from multiple IDSes. You can find more information about ARIS at http://aris.securityfocus.com/, and find the vulnerabilities in the SecurityFocus vulnerability database at http://www.securityfocus.com/bid.

Contents

Analysts

Dan Hanson, Mario van Velzen, Sean Hittel, and Jensenne Roculan

January 31, 2002

The top ten threats of 2001, based on IDS data submitted to the ARIS database, are as follows:

1. Nimda Worm
2. Code Red Worm
3. Code Red II Worm
4. Spam Mail
5. CGI Attacks
6. SubSeven Trojan
7. Microsoft FrontPage Attacks
8. DNS Attacks
9. FTP Attacks
10. SSH CRC-32 Compensation Detection Attack

This report discusses each of these threats, which we list in order of the percentage of ARIS users that have detected the attack and the aggregate number of incidents. This report also provides significant technical descriptions, patches, recommendations, and antivirus updates for protecting yourself against each attack.

1. Nimda Worm

Associated Operating Systems:	*Microsoft Windows 95, 98, ME, NT, 2000*

Technical Overview

The Nimda worm first appeared on September 18, 2001. In **Figures 1** and **2**, later in this report, you can clearly see the exponential spikes in traffic associated with the vulnerabilities that Nimda exploits. Nimda uses known bugs in unpatched installations of IIS and the Outlook email client to spread. Many attacks are associated with a Nimda infection, including the following:

- Generic HTTP Directory Traversal Attack
- Generic HTTP "cmd.exe" Request Attack
- Microsoft IIS 4.0 / 5.0 Extended Unicode Directory Traversal Attack
- Nimda Incoming Worm Attack
- Microsoft IIS/PWS Escaped Characters Decoding Command Execution Attack

Nimda spreads in four primary fashions:

- **Email:** The worm can be delivered through email containing an attachment named readme.exe of the MIME-type audio/x-wav. This email exploits the Microsoft IE MIME Header Attachment Execution vulnerability, which means that a vulnerable client only needs to preview the message to trigger infection. The subject of the email is variable and may originate from spoofed email addresses under the guise of trusted sources.
- **Web server attacks:** The worm attempts to search for and infect vulnerable IIS Web servers that have been compromised by the Code Red II worm backdoor root.exe. Nimda also seeks to gain control of the Web server via the Microsoft IIS/PWS Escaped Characters Decoding Command Execution and the Microsoft IIS and PWS Extended Unicode Directory Traversal vulnerabilities.
- **Web browsing code:** Users simply browsing the Web may become infected with Nimda, which modifies the content of files served from infected Web servers in the following fashion:

- Nimda adds the following content of HTML and JavaScript at the end of all .html, .htm, and .asp files in order to load readme.eml:

  ```
  <html><script language="JavaScript">window.open("readme.eml",
     null,"resizable=no,top=6000,left=6000")</script></html>
  ```

  People browsing Web pages with a vulnerable browser will automatically download the executable and run it, infecting their machines. The .eml and .nws file types, which represent embedded mail messages and embedded news messages, cause the Internet Explorer browser to view the contents and display the embedded message.

- Because the readme.eml message was crafted to run the readme.exe file through the MIME Header Attachment Execution vulnerability, vulnerable machines will not show that Nimda is infecting them.

- Because it infects index.htm and index.html files, the worm could also infect machines when the user views the folders with the View as Web Page setting turned on.

- **Open network shares:** Nimda is able to propagate via open network shares that have not been properly secured to deny access from unauthorized sources. This allows for the possibility of distribution within internal networks. Common names include readme.exe, readme.eml, riched20.dll, and admin.dll. Because various office tools, including Microsoft Word and WordPad, use riched20.dll, the worm infects these programs if they start within that directory.

Nimda exploits four known Microsoft vulnerabilities:

- **Microsoft IIS/PWS Escaped Characters Decoding Command Execution Vulnerability**
  http://www.securityfocus.com/bid/2708
- **Microsoft IE MIME Header Attachment Execution Vulnerability**
  http://www.securityfocus.com/bid/2524
- **Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability**
  http://www.securityfocus.com/bid/1806
- **Microsoft Office 2000 DLL Execution Vulnerability**
  http://www.securityfocus.com/bid/1699

Patches

To prevent infection via email, apply any of the following patches or upgrade to Internet Explorer 6.01:

- **Patch for MS01-020**
  http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp
- **Internet Explorer 5.01 Service Pack 2**
  http://www.microsoft.com/windows/ie/downloads/recommended/ie501sp2/default.asp
- **Internet Explorer 5.5 Service Pack 2**
  http://www.microsoft.com/windows/ie/downloads/recommended/ie55sp2/default.asp
- **Internet Explorer 6.01**
  http://www.microsoft.com/windows/ie/downloads/ie6/default.asp

To prevent Code Red infection and to prevent Nimda infection via the Web traversal vulnerabilities, use the IIS Lockdown tool or apply the following fixes:

- **IIS Lockdown Tool (default mode)**
  http://www.microsoft.com/technet/security/tools/locktool.asp
- **Patch for MS01-044**
  http://www.microsoft.com/technet/security/bulletin/MS01-044.asp
- **Windows NT 4.0 Security Roll-up Package**
  http://www.microsoft.com/downloads/release.asp?ReleaseID=31240

Applying any of the following updates or patches can also eliminate the Web traversal vulnerabilities:

- **Windows 2000 Service Pack 2**
  http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/default.asp
- **Windows NT 4.0 Security Roll-up Package**
  http://www.microsoft.com/downloads/release.asp?ReleaseID=31240
- **URLScan (default rule set)**
  http://www.microsoft.com/technet/security/URLScan.asp
- **Patch for MS00-086**
  http://www.microsoft.com/technet/security/bulletin/MS00-086.asp
- **Patch for MS01-044**
  http://www.microsoft.com/technet/security/bulletin/MS01-044.asp

Recommendations

- Password-protect or otherwise control access to open network shares.
- Run a host-based IDS or file integrity checker to be alerted if executables and DLL files are changed.
- Make sure all your users of IE, Outlook, and Outlook Express are patched (see the preceding "Patches" section).

In addition, the following hardening tools and checklists are available from Microsoft:

- **IIS 4**
  http://www.microsoft.com/technet/prodtechnol/iis/reskit/iis40rg/iisrkc08.asp
- **IIS 5**
  http://www.microsoft.com/technet/prodtechnol/iis/deploy/depovg/securiis.asp

An IIS 5 Hotfix Checking Tool also exists to check for patches that have not been installed. You can get it from Microsoft TechNet at http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168.

Antivirus Updates

Updated signatures from major antivirus vendors catch the email generated by Nimda.

2. Code Red Worm

Associated Operating Systems:	Microsoft Windows NT, 2000, XP Beta

Technical Overview

On June 18, 2001, eEye Digital Security released an advisory regarding a new security hole in IIS: http://www.eeye.com/html/Research/Advisories/AD20010618.html. This advisory led to signatures that are seen as the MS Index Server and Indexing Service ISAPI Extension Buffer Overflow vulnerability. On July 11, some administrators reported seeing attacks targeting this vulnerability and some Web site defacements occurred. July 13 saw an exponential growth pattern (see **Figures 1** and **2** later in this report) that indicated a worm.

Further analysis led to discoveries that the worm was written to do the following:

- Spread until the twentieth of the month
- Attack whitehouse.gov until the twenty-eighth of the month
- Sleep until the end of the month

Initially, poor selection of pseudo-random addresses meant each worm attacked the same set of addresses, reinfecting the same vulnerable servers and disrupting service for these addresses in particular. New variations of the worm improve on this weakness in address selection.

It is interesting to note that Code Red spreads without copying any files to disk. Rather, it exists solely in memory, and this capability made it a unique worm, ensuring that if a server were rebooted, the worm would be cleared from the server. If an unpatched server is rebooted, the worm is cleared, but the vulnerability remains and chances of reinfection are high. The safest procedure is to disconnect the host from the network, reboot, and apply the patches before reconnecting to the Internet.

Patches

Microsoft has made patches available to address this problem. You can find links to these patches at http://www.securityfocus.com/bid/2880.

Recommendations

Uninstall the Index Server/Indexing Service on any Web server on which it is not required or used. Apply the patch if uninstalling is not an option. Disable the file mappings for any files types that are not required for proper functioning of a Web site.

In addition, the following hardening tools and checklists are available from Microsoft:

- **IIS 4**
  http://www.microsoft.com/technet/prodtechnol/iis/reskit/iis40rg/iisrkc08.asp
- **IIS 5**
  http://www.microsoft.com/technet/prodtechnol/iis/deploy/depovg/securiis.asp

An IIS 5 Hotfix Checking Tool also exists to check for patches that have not been installed. You can get it from Microsoft TechNet at http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168.

3. Code Red II Worm

Associated Operating Systems:	*Microsoft Windows NT, 2000, XP Beta*

Technical Overview

The Code Red II worm used the same attack vector as the original Code Red worm seen in early July. Code Red II carried a more malicious payload and first appeared on August 3. The spikes in the attacks associated with Code Red II can be seen starting in the last week of July and the first week of August in **Figures 1** and **2** later in this report.

Code Red II uses the same means of compromise as the original Code Red but may be detected as a unique attack by some IDS systems that contain specific signatures. In addition to being detected by the Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack signature, the request for cmd.exe in the payload also triggers the Generic HTTP "cmd.exe" Request Attack signature.

Code Red II is more malicious because it installs a backdoor that allows unauthorized administrative access. An increased risk that tertiary malicious activities may have taken place makes it generally recommended that you format and reinstall your operating systems unless you can verify system integrity.

The Code Red II propagation phase was set to run until October 1, when it would reboot, which would clear the worm portion from the memory. Note, however, that the backdoor would still be present.

Patches

Microsoft has made patches available to address this problem. You can find links to these patches at http://www.securityfocus.com/bid/2880.

Recommendations

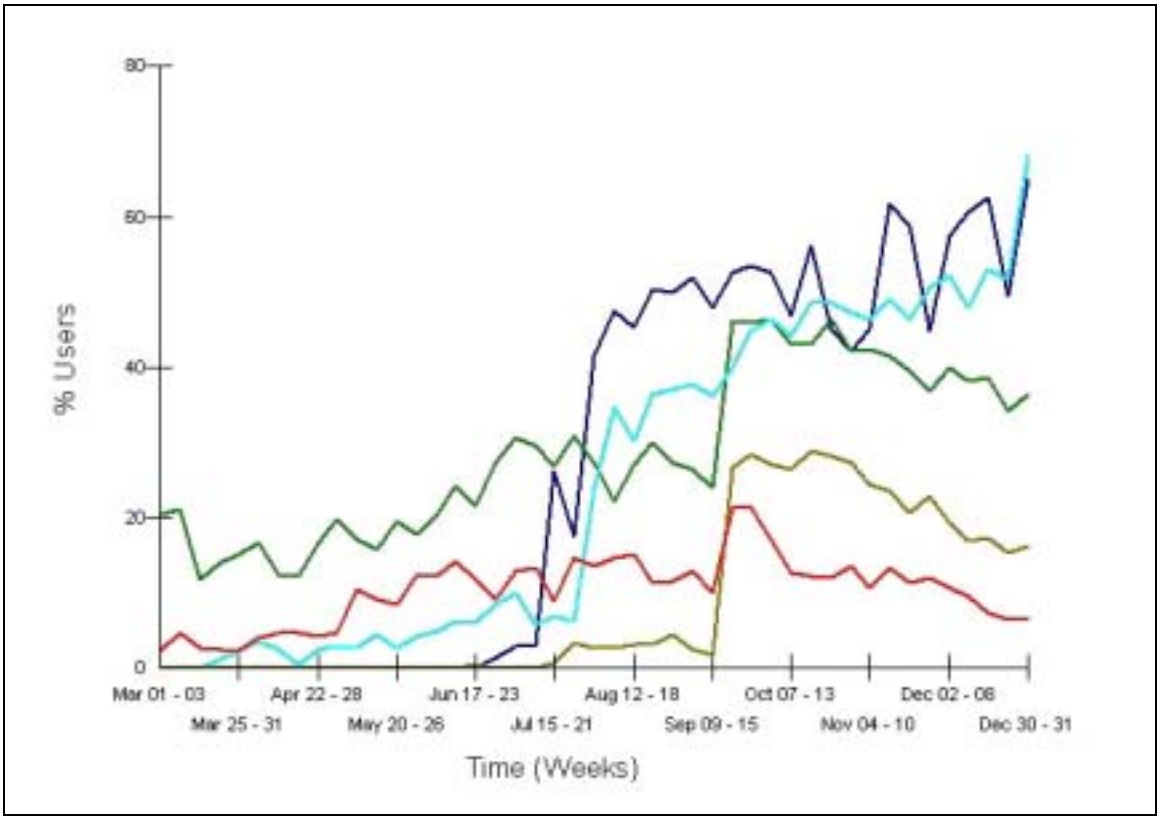
Hardening tools and checklists are available from Microsoft, as follows:

- **IIS 4**
  http://www.microsoft.com/technet/prodtechnol/iis/reskit/iis40rg/iisrkc08.asp
- **IIS 5**
  http://www.microsoft.com/technet/prodtechnol/iis/deploy/depovg/securiis.asp

An IIS 5 Hotfix Checking Tool also exists to check for patches that have not been installed. You can get it from Microsoft TechNet at http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168.

Attack Data

Figure 1 shows a notable increase occurs in early July in the number of users detecting ISAPI Buffer Overflow Attack traffic. We can attribute the first increase to Code Red. After the initial attack, a decrease (as the worm goes into distributed denial of service or DDoS attack mode on July 20) is followed by another increase. This time the increase is accompanied by a rise in the cmd.exe attack signature.

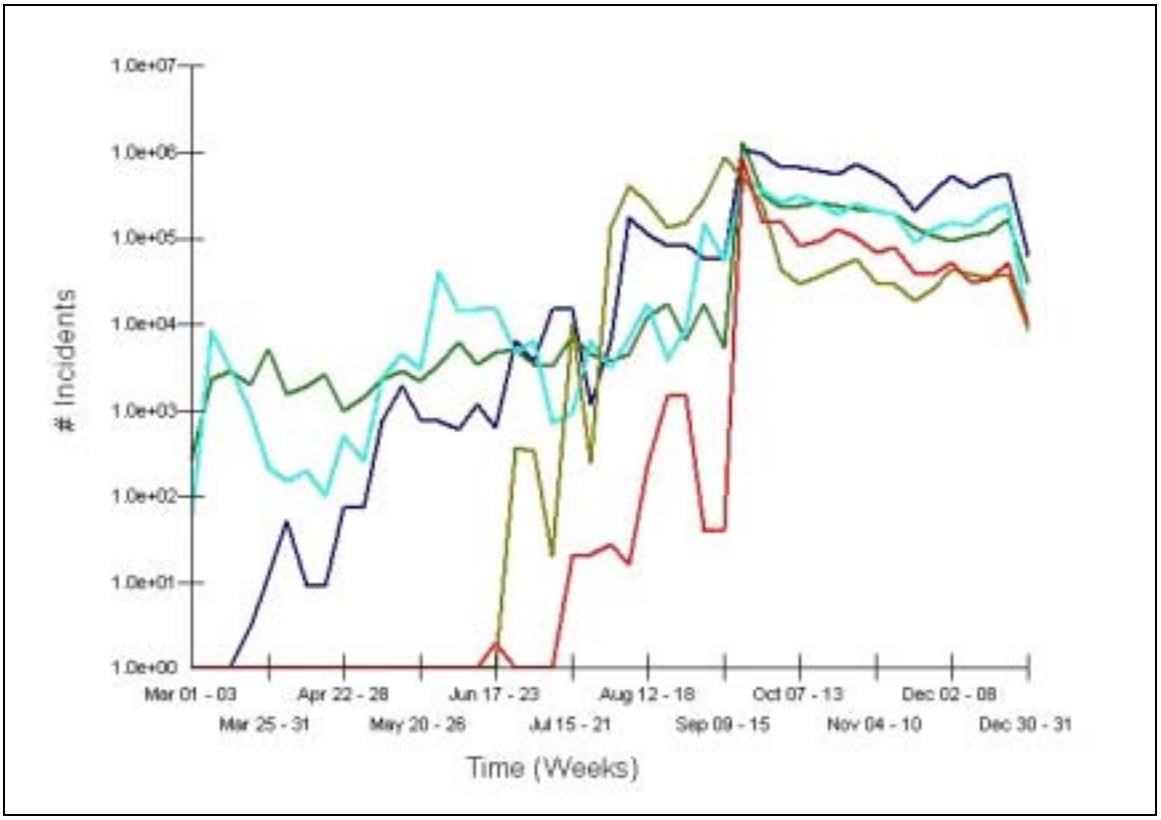


		% Users	# Attacks
	Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack	39.20	3486450
	Generic HTTP Directory Traversal Attack	38.07	4095950
	Generic HTTP 'cmd.exe' Request Attack	34.75	9473282
	Microsoft IIS/PWS Escaped Characters Decoding Command Execution Attack	16.57	1944598
	Microsoft IIS 4.0 / 5.0 Extended UNICODE Directory Traversal Attack	14.77	3861256

Figure 1. Code Red and Nimda Activity by User Percentage from March to November, 2001

The rapid increase shortly following the decrease in users detecting the ISAPI Buffer Overflow Attack can be attributed to Code Red II due to the accompanying increase in the number of users seeing the Generic HTTP “cmd.exe” Request Attack. In early September, a sharp increase occurs in the number of users detecting the attacks associated with Nimda.

In **Figure 2**, ARIS users see the same patterns for Code Red and Code Red II based on the number of detected incidents of the attacks and, in mid-September, Nimda brings all the signatures to one common apex.



		% Users	# Attacks
	Generic HTTP 'cmd.exe' Request Attack	34.75	9473282
	Generic HTTP Directory Traversal Attack	38.07	4095950
	Microsoft IIS 4.0 / 5.0 Extended UNICODE Directory Traversal Attack	14.77	3861256
	Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack	39.20	3486450
	Microsoft IIS/PWS Escaped Characters Decoding Command Execution Attack	16.57	1944598

Figure 2. Incidence of Code Red and Nimda Activity from March to December, 2001

4. Spam Mail

Associated Operating Systems:	*Not OS-Specific*

Technical Overview

Spam is a problem that many Internet users are familiar with, wading through piles of unsolicited email advertising everything from sex to the newest biomedical wonder. Tracking down and stopping spammers is difficult because spammers rely on other people's vulnerable systems to deliver their email for them.

If your system is used as a relay or delivery mechanism for spam, it is conceivable that other domains might block delivery of mail from your domain until you fix the problem, not to mention that you are paying for the bandwidth used to deliver these unsolicited mails.

ARIS users are seeing attempts to deliver spam in high numbers with the following two signatures:

- SMTP Spam Relay Attack
- Matt Wright FormMail Attacks

SMTP relay is a well-known problem. A mail server can be set up to relay email from client systems and deliver them to a target network and host. It is relayed because the client opens an SMTP connection to the server, injects the mail, and then the server attempts the address resolution and completes the delivery. If multiple recipients are specified, one injected mail message from the client will result in many outgoing connections from the relaying server.

Spammers use this functionality by finding an open relay. An open relay is a host that is set to accept messages from anyone and deliver anywhere. This attack uses existing SMTP infrastructure to send the unsolicited email.

The Matt Wright FormMail attack uses a different protocol entirely. The attack is based on HTTP and uses a feature of many Web sites where a feedback form emails the contents of the form to a person. Many packages will process this input on the server and send the mail, and many of these packages are vulnerable to the same style of attack, but ARIS users are seeing attacks targeting Matt Wright's FormMail package in high numbers.

An attacker finds a vulnerable site and uses a script to submit an HTTP request that includes a string of addresses that are to be targeted. The script takes the input, parses it, forms the mail, and sends the message. The only location where the IP address of the originator of the message is ever stored is in the HTTP log file.

Patches

Matt Wright has made a new version of this package available at http://worldwidemart.com/scripts/formmail.shtml.

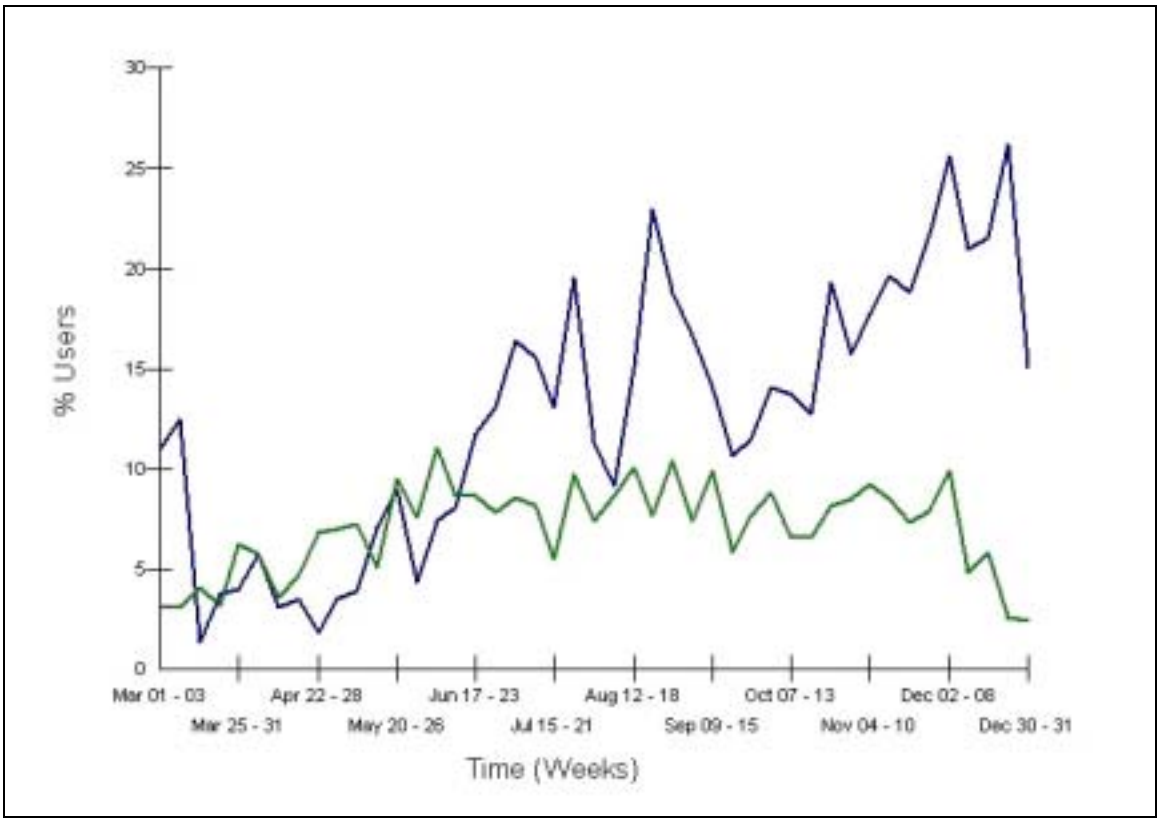
Recommendations

To control SMTP relay, configure your mail server to accept relays only from certain hosts or networks that are considered safe and under your control. Instructions for doing this are available from your vendor. Common SMTP implementations are as follows:

- **Sendmail (newest version):**
  http://www.sendmail.org/tips/relaying.html
- **Qmail:**
  http://www.lifewithqmail.org/lwq.txt (see Section 3.2)
- **Exchange:**
  http://www.slipstick.com/exs/relay.htm
- **Novell GroupWise:**
  http://support.novell.com/cgi-bin/search/searchtid.cgi?/2954070.htm
  http://support.novell.com/cgi-bin/search/searchtid.cgi?/10062320.htm

Attack Data

While the number of ARIS users detecting SMTP relaying attempts has remained relatively constant, attempts to use the FormMail package to send the unsolicited email have increased throughout the year, as shown in **Figure 3**.



	% Users	# Attacks
Matt Wright FormMail Attacks	18.61	67031
SMTP SPAM Relay Attack	9.91	239453

Figure 3. Percentage of Users Seeing Spam Attacks from March to December, 2001

5. CGI Attacks

Associated Operating Systems:	*Not OS-Specific*

Technical Overview

One feature of many Web sites is content or behavior that is directly related to user interaction. This might be as simple as a counter or as complex as a credit card processing application. Many scripts might be vulnerable to one type of attack or another, but two very widespread attacks on scripts commonly found on the Internet are:

- Matt Wright GuestBook 2.3 CGI Attack
- Muhammad A. Muquit Count.cgi Attack

Attackers can use either of these attacks to gain access or execute arbitrary commands on targeted hosts remotely.

Matt Wright wrote the GuestBook script to parse form field entries and display them back on the Web page, enabling users to submit comments and information about themselves. A vulnerability exists in certain configurations; it is possible for an attacker to insert Server Side Includes statements that are run by the server when the page is requested.

Count.cgi is a script that generates a user hit counter to display the traffic to the Web site. The script is vulnerable to buffer overflows, enabling a malicious user to overwrite arbitrary locations in memory, providing the ability to run arbitrary code on the host.

Attackers can use either of these vulnerabilities to gain access to the host at the privilege level of the Web server. In certain installations and with certain servers this might be a highly privileged user. In other installations where the Web server operates in the context of an unprivileged user, the Web site can be defaced or other privilege escalation vulnerabilities can be exploited to gain privileged access to the host.

Patches

A newer version of Count is available from http://www.muquit.com/muquit/software/Count/Count.html.

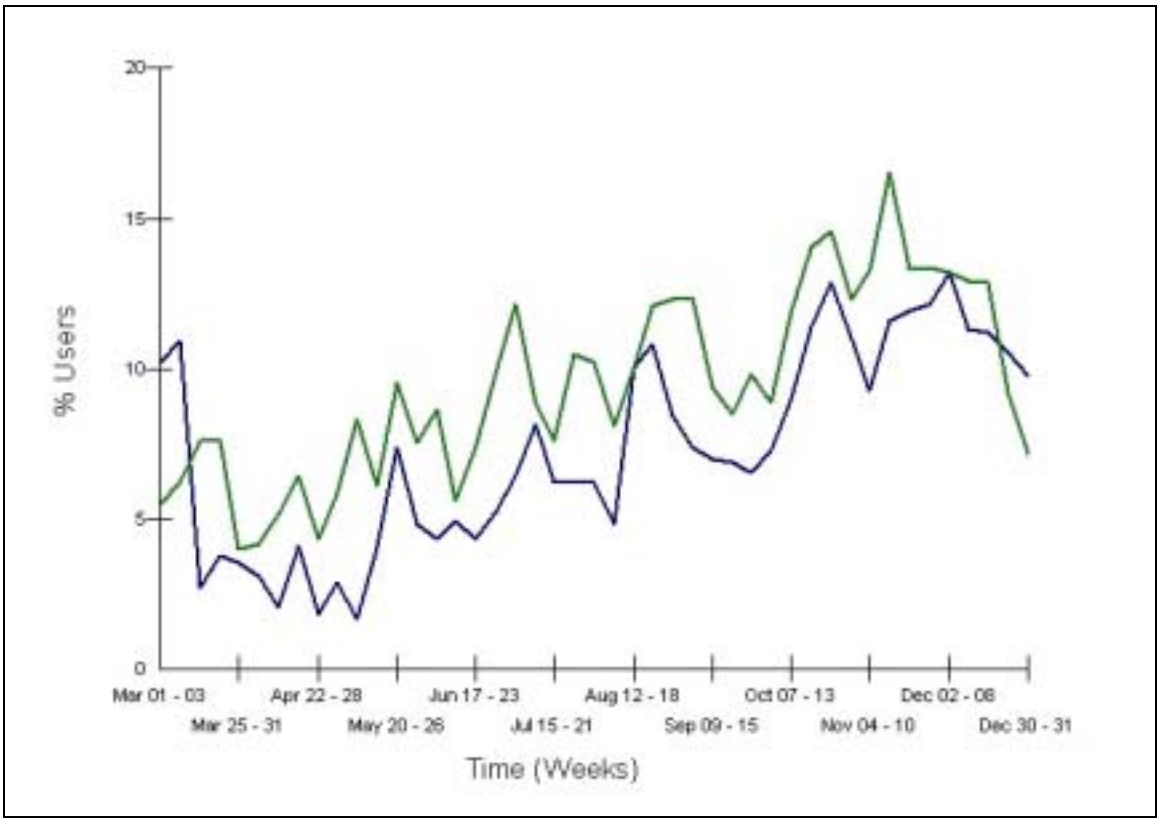
The latest version of GuestBook from Matt Wright's Web site is Version 2.3.1. This version of GuestBook parses for Server Side Includes tags in the input fields, but looks for a SSI string that is *not* required for SSI directives to be processed on certain Web servers.

Recommendations

We strongly recommend auditing all scripts used in Web pages. If you do not require scripts, disable execute access to any directory available through the Web site. Remove script mappings from the Web server if possible.

Attack Data

Figure 4 shows a steady increase over the year in the activity targeting two very common CGI scripts. Both the GuestBook and Count CGI scripts contain vulnerabilities that may allow a malicious user to manipulate data and possibly gain privileges on the targeted host.



	% Users	# Attacks
Matt Wright GuestBook 2.3 CGI Attack	18.84	73907
Muhammad A. Muquit Count.cgi Attack	18.66	52506

Figure 4. Percentage of Users Seeing CGI Attacks from March to December, 2001

6. SubSeven Trojan

Associated Operating Systems:	*Microsoft Windows 95, 98, ME, NT 4.0, 2000, XP*

Technical Overview

SubSeven is a powerful remote administration program. This type of malicious software, once installed on the target host and run, lets an attacker connect via the network to the system, take control of it, and monitor any activity on it.

SubSeven is usually divided into two components—the *server*, which is installed on target Windows hosts, and the *client*, which is used by the attacker to connect to the victim host. To connect to an infected machine, the attacker needs to know the IP address of the target host. SubSeven does contain a notification agent that can let the attacker know the IP address of the targeted host when it receives one and connects to the Internet.

SubSeven uses many default ports to communicate depending on the version that a host is compromised with. 1243, 6711, 6712, 6713, 6776 are all implicated, as is 27374 in version 2.1.

SubSeven activity triggers multiple ARIS signatures, but the two most active are as follows:

- SubSeven Backdoor Probe
- SubSeven Backdoor Server Attack

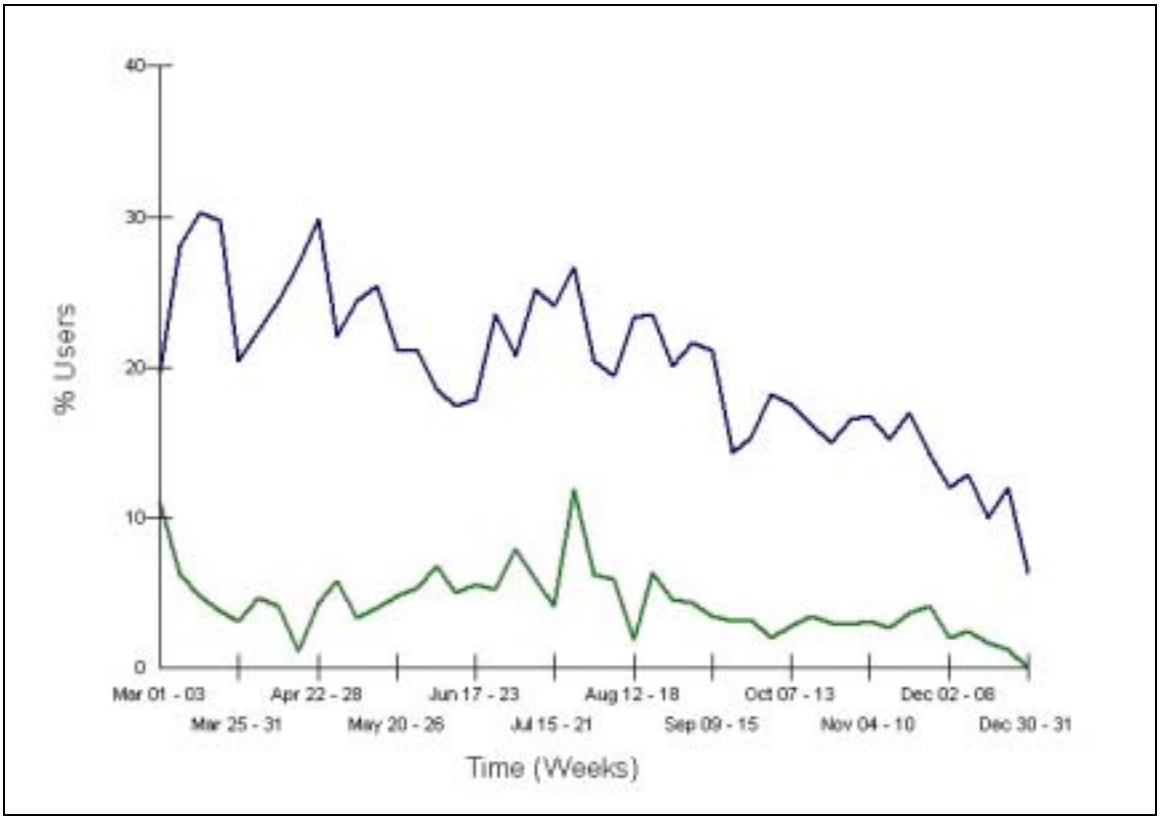
Recommendations

If you are unsure if a host has been compromised, audit for listening ports that would indicate if SubSeven (or another backdoor) is operating on the system. Scanners exist that you can download and run in your network environment to verify which ports are open and listening on hosts.

SubSeven requires a vector to gain access to the computer. The vector might be a user receiving an attachment that installs the backdoor, or it might be downloaded as part of another attack to maintain access to the system in the event that the original method of entry is patched. Consequently, SecurityFocus highly recommends that you use a virus scanner with current virus signatures to guard against infection by SubSeven or other similar products. We also recommend a host-based IDS or file integrity checker to notify you of modified or added files.

Attack Data

While SubSeven activity has been decreasing over the year, it is still a serious risk to hosts that have been compromised and is still being actively scanned for on a large number of networks, as **Figure 5** indicates.



	% Users	# Attacks
SubSeven Backdoor Probe	17.92	82282
SubSeven Backdoor Server Attack	6.29	65527

Figure 5. Percentage of Users Seeing SubSeven Activity from March to December, 2001

7. Microsoft FrontPage Attacks

Associated Operating Systems:	*Microsoft Windows 95, 98, NT, 2000*

Technical Overview

A myriad of FrontPage vulnerabilities have left Microsoft Windows servers vulnerable to attack. Over the year, ARIS users saw a large number of attacks targeting FrontPage Server Extensions for a Denial of Service (DoS) attack, as well as a directory traversal vulnerability targeting the FrontPage Personal Web Server. Although the directory traversal vulnerability is old (it was released January 17, 1996), it is still being actively targeted for exploitation.

The ARIS attack signatures are as follows:

- Microsoft FrontPage Server Extensions DoS Attack
- Microsoft FrontPage PWS Directory Traversal Attack

The vulnerabilities that these attacks exploit are as follows:

- **Microsoft FrontPage PWS Directory Traversal Vulnerability**
  http://www.securityfocus.com/bid/989
- **Microsoft IIS Front Page Server Extension DoS Vulnerability**
  http://www.securityfocus.com/bid/2144

The DoS attack targets Microsoft Windows 2000 machines running FrontPage 2000 Server extensions version 1.1 and earlier. If exploited server resources can be exhausted (CPU usage reaching 100 percent), the service must be manually restarted.

The directory traversal vulnerability lets a malicious user embed characters to traverse out of the Web directory. Attackers can use this vulnerability to gain access to any file on the server.

Patches

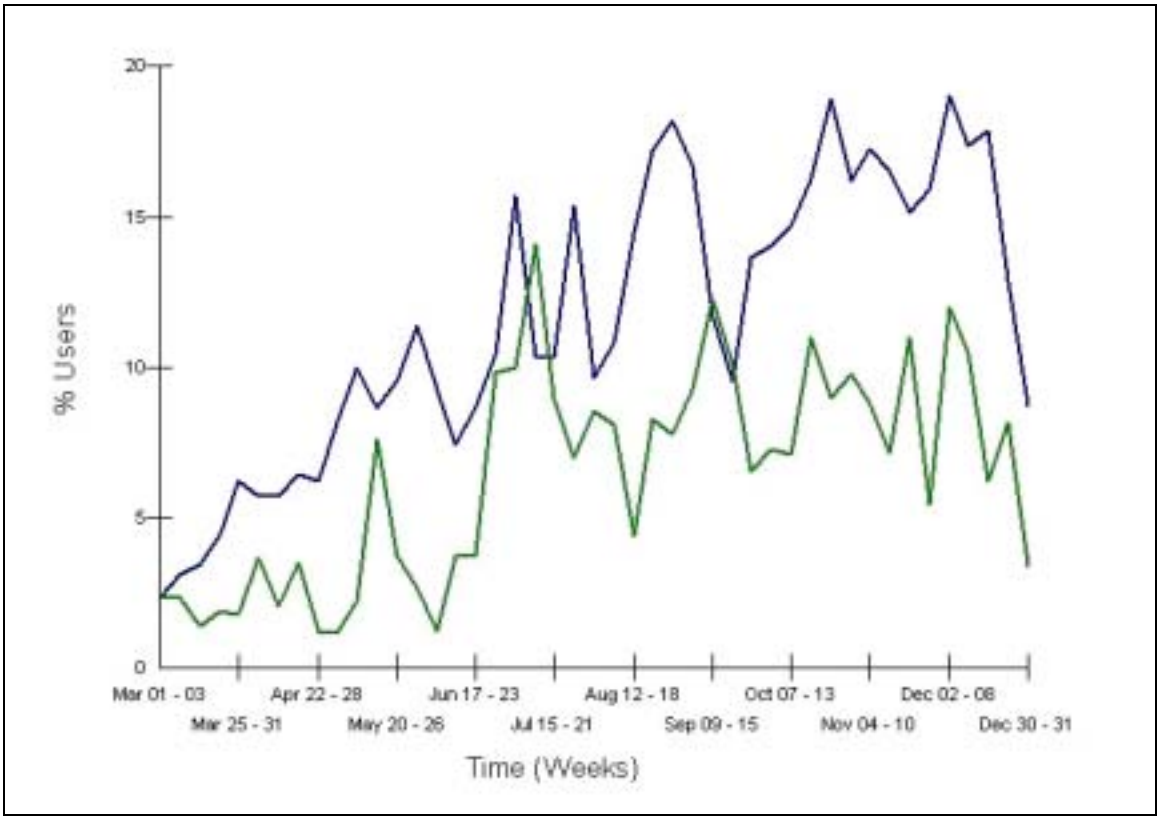
Upgrade to the latest version of FrontPage Server extensions and the FrontPage Personal Web Server.

Recommendations

Unless you have a functional reason to leave them running, disable all the FrontPage Server Extensions and any other unneeded services. If you are running the Server Extensions, verify that you are using the most recent version. Run a host-based IDS or file integrity checker to verify that no files were changed in the event of a compromise.

Attack Data

FrontPage has been gaining ground as a target for denial of service and compromise attempts. While not seeing the raw numbers of attacks that might be seen for Nimda, a significant portion of the ARIS user base has seen traffic targeting these services, as shown in **Figure 6**.



	% Users	# Attacks
Microsoft FrontPage Server Extensions DoS Attack	20.93	51209
Microsoft FrontPage PWS Directory Traversal Attack	17.52	42689

Figure 6. Percentage of Users Seeing FrontPage Attacks from March to December, 2001

8. DNS Attacks

Associated Operating Systems:	*Not OS-Specific*

Technical Overview

Domain Name Service (DNS) services are integral to the proper function of the Internet infrastructure. Their very importance leads them to be the focal point of a direct attack, providing the opportunity for an attacker to perform reconnaissance about the topology, naming conventions, and other critical data that can be used to increase the effectiveness of future attack.

The biggest risk to a DNS server is a direct attack that compromises the integrity of the name server's database, or uses the trusted nature of the server to provide access into other parts of the network. Numerous buffer overflows in BIND (Berkeley Internet Name Domain) versions and implementations demonstrate that this is a technique that will often open a path into a network.

Networks that use a common DNS to service internal and external clients can unwittingly give away very valuable information that can aid an attacker in performing future attacks, including social engineering

attacks. If internal DNS servers are compromised, the compromise can facilitate many man-in-the-middle attacks and traffic redirection, compromising business data and other critical information.

Patches

You should upgrade all prior versions of BIND to the latest version to prevent a number of buffer overflow weaknesses.

Note: BIND version 9 is a rewrite of much of the underlying code-base in BIND and adds a great deal of functionality and support. If you are still running BIND 4, upgrade immediately at the following sites:

- **BIND 8.2.5:**
  http://www.isc.org/products/BIND/bind8.html
- **BIND 9.2.0:**
  http://www.isc.org/products/BIND/bind9.html

Recommendations

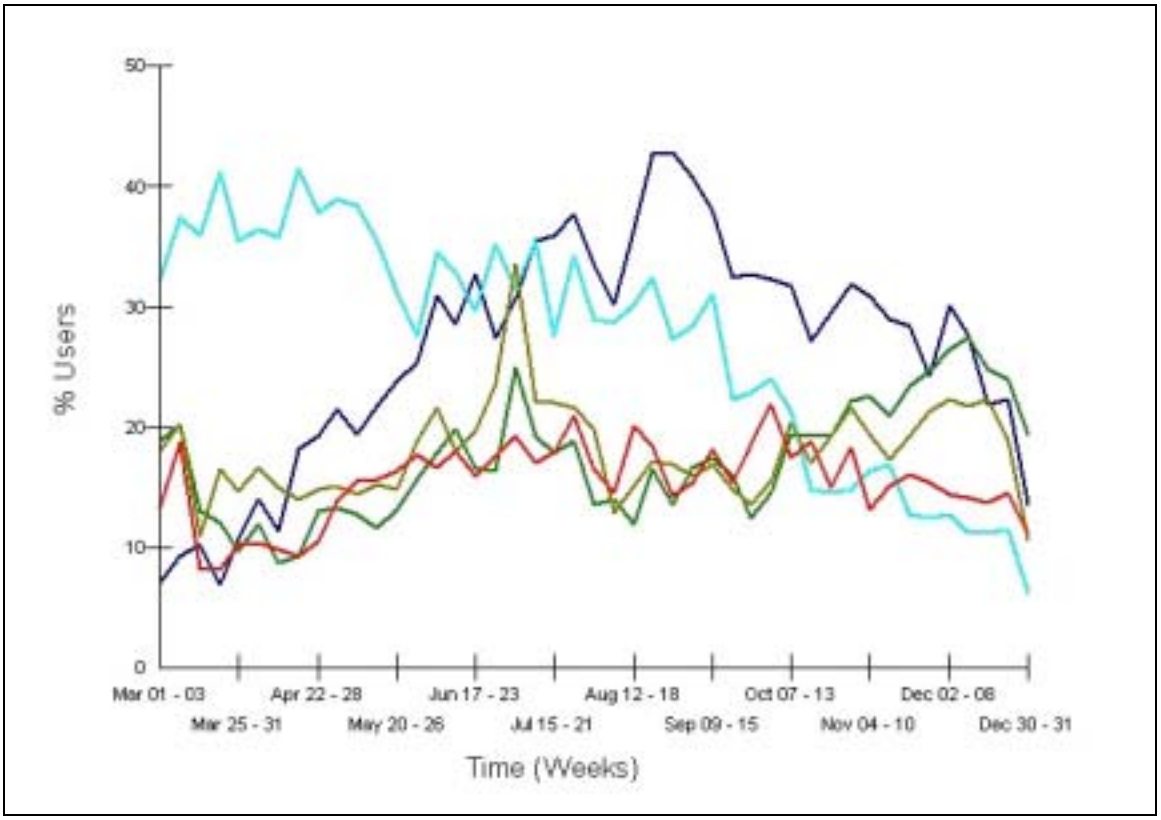
Upgrade to the latest versions of your chosen DNS. Separate the services for internal and external clients to minimize the information that an attacker can retrieve. Locate the DNS used for internal services in a safe location inside your firewall and do not allow connections from outside. Disable zone transfers except to authorized hosts that need the information (secondary name servers, for example).

Some distributions of popular Unix operating systems (OpenBSD later than version 2.4) run BIND in a `chroot()` jail. This is a good idea that limits the immediate opportunities to an attacker in the event of a breach, but there are ways to break out of a `chroot()` jail. See the following documents for procedures for running BIND 8 and BIND 9 in a `chroot()` jail. The instructions are written from the perspective of a Linux environment, but the procedure is similar for other Unix operating systems.

- **BIND 8:**
  http://www.linuxdoc.org/HOWTO/Chroot-BIND8-HOWTO.html
- **BIND 9:**
  http://www.linuxdoc.org/HOWTO/Chroot-BIND-HOWTO.html

Attack Data

DNS hosts are popular targets for both attacks and reconnaissance information about an upcoming attack. Unsurprisingly, the most prevalent malicious traffic on port 53 is port scans and probes for DNS version and operating system information. **Figure 7** shows an increase over the year in the number of users detecting UDP port scan probes to detect hosts that are running DNS services on port 53. The Chaos Variable Probe is a method for fingerprinting the BIND version that is running on a host.



	% Users	# Attacks
ISC BIND DNS (BIND) CHAOS Variable Probe	25.79	283551
Generic UDP Portscan Probe	24.84	6028599
Generic DNS Server Probe	22.68	272187
Generic TCP Port Scan with Invalid Flags	20.84	1332911
Generic DNS Zone Transfer Probe	20.14	1048642

Figure 7. Percentage of Users Seeing Attacks targeting DNS (Including Probes) from March to December, 2001

9. FTP Attacks

Associated Operating Systems:	*Not OS-Specific*

Technical Overview

FTP services are targets for attackers for two primary reasons. If an attacker is able to create directories on FTP sites providing anonymous FTP access or if a user and password is known, an attacker can covertly set up a “warez” site on the host for the storage and distribution of attack tools, pirated software, or other questionable files. This site uses your bandwidth and disk space, and enables the attacker to distribute the files anonymously.

The second reason that FTP is an attractive target is because FTP is a service that has been around for many years. Advances in attackers’ abilities to exploit complex programming errors recently opened the

service up to a critical new threat. The Wu-Ftpd file globbing vulnerability that has affected many Linux distributions as well as other Unix systems is a very strong example of this fact.

You can find details of those vulnerabilities as follows:

- **Wu-Ftpd File Globbing Heap Corruption Vulnerability**
  http://www.securityfocus.com/bid/3581
- **Multiple Vendor FTP glob Expansion Vulnerability**
  http://www.securityfocus.com/bid/2496

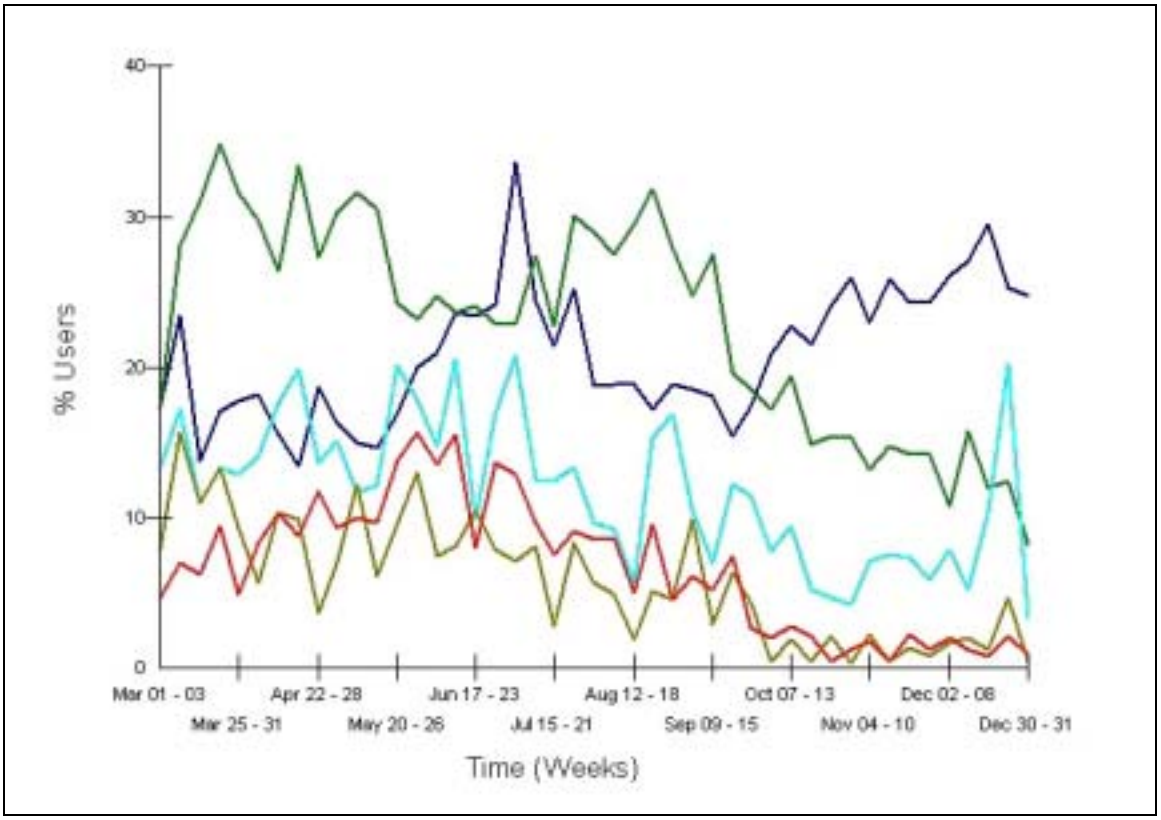
Recommendations

FTP is an insecure service; the login passwords and the transferred files themselves are passed unencrypted over the network and can be easily sniffed. The code that the service is built on, in many cases, descends from a legacy server where security was not a priority in its design and implementation. If FTP services are mandatory, verify that current patches are installed, disable anonymous logins if unneeded, and run a host-based IDS or file integrity checker to verify that files have not been added or changed in the event of a compromise.

As an alternative to FTP, you might want to consider SCP (encrypted login information and data transfer) or HTTP (instead of anonymous FTP). These alternatives have their own security issues but they do mitigate some of the associated risk. If your system is already running either SSH or a Web server, it reduces the number of services that need to be maintained and limits potential vulnerabilities and entry points for attackers.

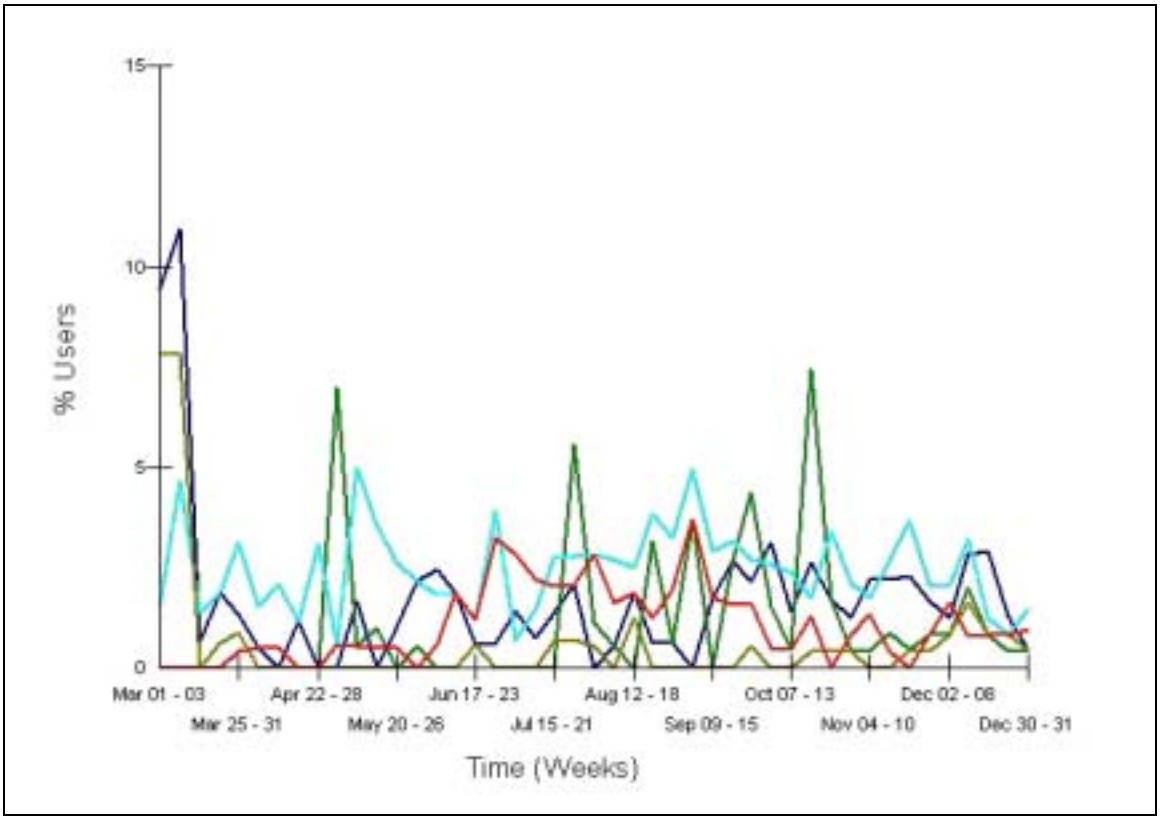
Attack Data

The data in **Figures 8** and **9** shows that although the numbers of users detecting attacks did not increase over the year, probing for FTP servers is more common, and a probe with invalid flags has become more common toward the end of the year.



	% Users	# Attacks
Generic TCP Port Scan with Invalid Flags	23.32	4184562
Generic FTP Port Probe	20.58	62999
Generic TCP SYN FIN Scan Probe	17.34	155966
Generic TCP OS Fingerprint Probe	11.94	1086
Synscan SYN Scan Port Probe	10.93	195758

Figure 8. Percentage of Users Seeing Attacks Targeting FTP services (Including Probes) from March to December, 2001



	% Users	# Attacks
FTP 'SITE EXEC' Attack	4.70	2995
FTP Data Source Porting Attack	4.19	17127
Generic Unix FTP 'passwd' File Download Attack	3.88	1910
Generic FTP CWD ~root Attack	3.43	618
Generic FTP Wildcard Attack	2.16	84268

Figure 9. Percentage of Users Seeing Attacks Targeting FTP Services (Excluding Probes) from March to December, 2001

10. SSH CRC-32 Compensation Detection Attack

Associated Operating Systems:	*Not OS-Specific*

Technical Overview

SSH was developed as a secure replacement for the remote access and file transfer programs such as rlogin telnet and ftp. SSH and supporting programs enable a user to log in to and transfer files to and from a remote host. Authentication is handled securely and data is encrypted (and can optionally be compressed if operating over a slower link) to prevent disclosure of confidential information through eavesdropping.

SSH is usually considered a trusted service and, because the protocol is used for user authentication, it is usually required to run in a privileged context. Both of these circumstances result in a situation where a

vulnerability in the service has far-reaching consequences. The SSH CRC32 Compensation Detection vulnerability is an overflow that targets code put in place to detect a previous vulnerability in the protocol. The vulnerability only occurred in protocol version 1 and servers that supported this protocol (even if it fell back to protocol 1 for backward compatibility). Michal Zalewski discovered the original vulnerability on February 8, 2001, and you can find details at http://www.securityfocus.com/bid/2347.

The SSH CRC-32 Compensation Detection Attack sometimes appears in a security or system log and has the following pattern:

```
hostname sshd[xxx]: Disconnecting: Corrupted check bytes on input.
hostname sshd[xxx]: Disconnecting: crc32 compensation attack: network
   attack detected
hostname sshd[xxx]: Disconnecting: crc32 compensation attack: network
   attack detected
```

This pattern might appear multiple times in logs because the attack is a brute force method and many attempts could be required before the attack succeeds.

Routers that use SSH for administration may also be vulnerable to attacks targeting protocol 1 of SSH. Cisco's SSH implementation currently contains support for protocol 1 only.

Patches

We strongly urge you to upgrade to a non-vulnerable version of SSH. You can find patch and updated version information at http://www.securityfocus.com/bid/2347, which includes patch information for SSH Secure Communication Corporation (multiple versions), OpenSSH (multiple versions), and Cisco (PIX Firewall, Switches, and multiple IOS versions).

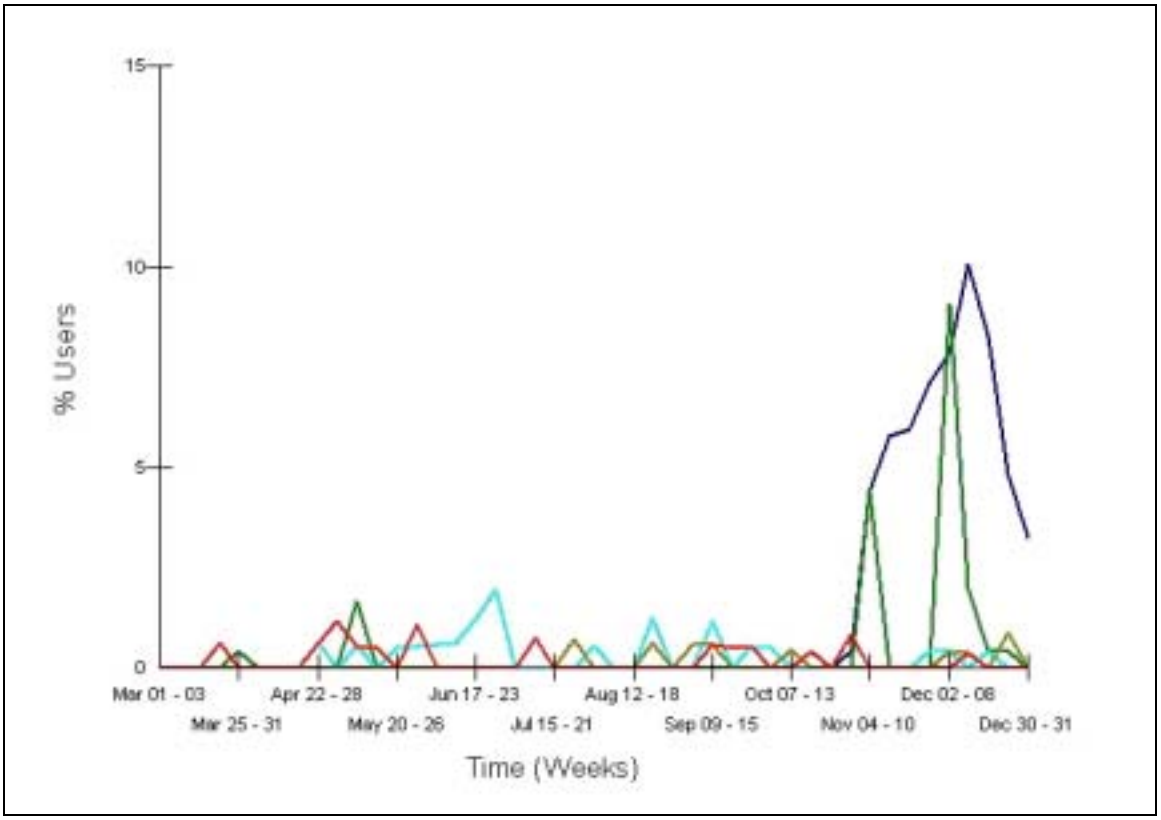
Vendors may have packages that contain the patch or have newer versions available. Check your vendor's Web site for access to these patches.

Recommendations

In addition to making sure that you are running a patched version for known vulnerabilities, we also recommend that you disable SSH protocol 1 support (check the documentation in your specific SSH implementation for how to do this). Auditing which locations need SSH access and allowing only those hosts or netblocks to access SSH is another way to limit your exposure in the event of a new exploit or vulnerability.

Attack Data

As **Figure 10** indicates, activity targeting the SSH CRC32 Compensation Detection vulnerability rose rapidly in the third week of October and peaks in early December. Activity in SSH was notable in the numbers of attacks detected and the potential severity of the exploit as well as data regarding the percentage of vulnerable SSH services.



		% Users	# Attacks
	SSH CRC-32 Attack Detection Compensation Exploit Attack	4.83	119556
	FTP Data Source Porting Attack	3.69	59570
	Generic X86 Buffer Overflow (setuid(0)) Attack	1.23	32
	Generic Teardrop/Land Denial of Service Attack	0.85	354
	Generic X86 Buffer Overflow (setgid(0)) Attack	0.85	25

Figure 10. Percentage of Users Seeing Attacks Targeting the SSH Service from March to December, 2001

About SecurityFocus

SecurityFocus™ is a leading provider of enterprise security threat management systems. SecurityFocus provides global early warning of cyber attacks, customized and comprehensive threat alerts, and countermeasures to prevent attacks before they occur. As a result, SecurityFocus customers can mitigate risk, manage threats, and ensure business continuity. The company also licenses the world's largest, most complete vulnerability database, hosts the most popular security community, Bugtraq™, and publishes original security content on its Web site at www.securityfocus.com. SecurityFocus, headquartered in San Mateo, California, is a privately held company backed by leading investors including ArrowPath Venture Capital (formerly E*TRADE Venture Capital) and Mobius Venture Capital (formerly SOFTBANK Venture Capital).

Corporate Headquarters:
1660 S. Amphlett Blvd., Suite 128
San Mateo, CA 94402
U.S.A.
866-577-6300 Toll-free
650-655-6300 Main
650-655-2099 Fax
aris-an@securityfocus.com

Canadian Office:
100-4th Avenue S.W., Suite 710
Calgary, AB T2P 3N2
Canada
403-213-3939 Main
403-233-9179 Fax