TUTORIAL

TITLE: **A Case Study In Incident and Vulnerability Handling Coordination**

ABSTRACT: This 90 minute presentation will detail a 12-week examination of the handling of a vulnerability from its initial report to its use by intruders and the publication of an advisory and two special edition CERT/CC summaries. The presentation will demonstrate some of the possible things that can happen during the handling of a vulnerability.

Highlighted in the tutorial are:

- Coordination between the CERT/CC and the
    - BIND authors
    - OS vendors
    - Critical national infrastructure organizations
    - Sites involved in the incident

- How quickly exploit scripts are created and used by the intruder community once a vulnerability is known

PRESENTORS: Jeff Carpenter, FedCIRC Operations
Kathy Fithen, Manager FedCIRC Operations
Shawn Hernan, FedCIRC Operations

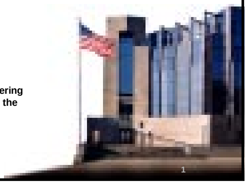
BIND Activity

March-June, 1998

Jeffrey J. Carpenter, Shawn Hernan, and Kathy Fithen

CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

The CERT Coordination Center is part of the Software Engineering Institute. The Software Engineering Institute is sponsored by the U.S. Department of Defense.



Introduction

This presentation is a chronological description of our work and observations on an inverse query BIND vulnerability discovered in 1998.

Week One

March

Sun	Mon	Tues	Wed	Thur	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
Week 1						
29	30	31				

April

Sun	Mon	Tues	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

May

Sun	Mon	Tues	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24 31	25	26	27	28	29	30

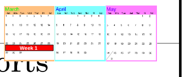
Initial Report

We receive a report indicating a problem with self referential records in BIND.

The next day, we receive three messages from Bob Halley regarding:

- **An inverse query buffer overflow**
- **A failure to validate memory references**
- **A problem with self-referential records**

March 24th & 25th, 1998



The Character of the Reports

There are three distinct reports.

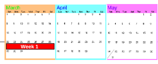
Each is of good quality, in advisory-like format:

- **Description**
- **Impact**
- **Work-arounds and fixes**

Signed by an key we have not validated.

From a person we don’t recognize (Bob Halley).

March 25th, 1998



Initial Analysis

The first problem potentially leads to a root compromise.

The second and third problems lead to denial-of-service.

Under ordinary circumstances, the first problem is unlikely to occur.

All three problems are addressed in next version of BIND.

March 26 & 27th, 1998

The Inverse Query Function

The Inverse Query function is little used

- Disabled by default under most distributions
- Optional part of specification (RFC 1034)
- Used to search on non-indexed information contained in a domain name server
- BIND actually simulates inverse query via the fake-iquery configuration variable

March 26th & 27th, 1998

Support for Inverse Query

There are multiple active versions of BIND:

V8.x
- Inverse query support controlled in configuration file

V4.9.x
- Inverse query support controlled in configuration file
- Also may be compiled in by default

March 26th & 27th, 1998

INVQ Compilation Option

Some systems distributed with V4.9.x have support for INVQ (inverse query) compiled into the binary.

- The absence of fake-iquery option in configuration file does not mean INVQ is not supported.
- Many system administrators overlooked that INVQ support might have been compiled in.

March 26th & 27th, 1998

The Inverse Query Vulnerability

- Is a fairly ordinary buffer overflow in the section of ns_req.c that processes inverse query requests.

March 26 & 27th, 1998

Exploiting Buffer Overflows

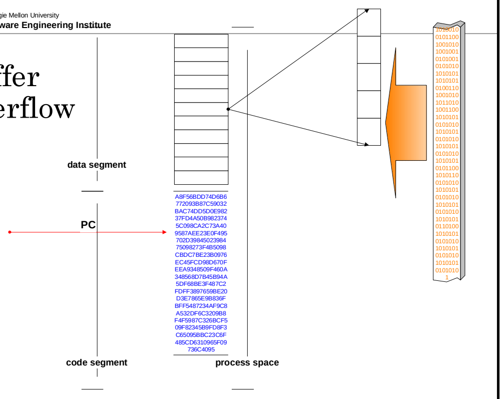
The specific exploit depends on many factors.

In general:

- Fill a buffer with code.
- Overwrite the return address with the address of the code.

March 26th & 27th, 1998

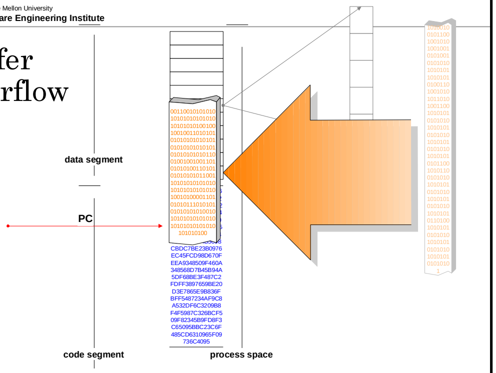
Buffer Overflow (1)



```
A8F56BDD74D6B6
772093B87C59032
BAC74DD5D0E982
37FD4A50B982374
5C098CA2C73A40
9587AEE23E0F495
702D39845023984
75098273F4B5098
CBDC7BE23B0976
EC45FCD98D670F
EEA9348509F460A
348568D7B45B94A
5DF68BE3F487C2
FDFF3897659BE20
D3E7865E9B836F
BFF5487234AF9C8
A532DF6C3209B8
F4F5987C326BCF5
09F82345B9FD8F3
C65095BBC23C6F
485CD6310965F09
736C4095
```

```
1010010
0101100
1001010
1001001
0101001
0101010
1010101
1010101
0100110
1001010
1011010
1001100
1010101
0101010
1010101
0101010
1010101
0101010
1010101
0101100
1010110
0101010
1010101
0101010
1010101
0101010
1010101
0110100
1010101
0101010
1010101
0101010
1010101
0101010
1
```

Buffer Overflow (2)



Responding to Buffer Overflows

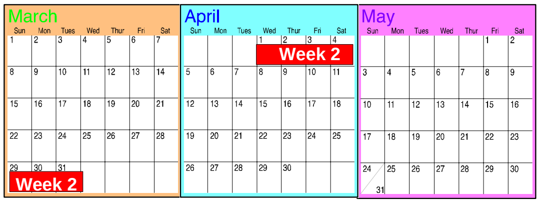
They can be prevented by proper bounds checking.

The impact can be mitigated by:
- **Marking the stack as read-only**
- **Removing privileges from binary**

Risk can be reduced by guarding the input channel.

March 26 & 27th, 1998

Week Two



March

Sun	Mon	Tues	Wed	Thur	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29 Week 2	30	31				

April

Sun	Mon	Tues	Wed	Thur	Fri	Sat
			1 Week 2	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

May

Sun	Mon	Tues	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24 31	25	26	27	28	29	30

Contacting the Author (1)

We contact Paul Vixie to validate Bob Halley's key.

Paul authenticates Bob as able to speak authoritatively for BIND issues.

We then validate Bob's key out-of-band.

March 30th, 1998

Contacting the Author (2)

We negotiate with Paul to publish his information as a Vendor-Initiated Bulletin (VIB):
- **All-in-one**
- **Patches via ftp**
- **Information on finding self referential cnames**

Paul informs us that he'll be publishing public beta code to correct the vulnerabilities.

March 30th, 1998

Contacting the Vendors

After verifying the problem, we send mail to affected vendors, saying we:

- **Plan to publish a VIB "on or around April 13"**
- **Included a draft VIB**
- **Included patches provided by Bob Halley and Paul Vixie**

March 30th, 1998

Responses from Vendors (1)

Most vendors responded to acknowledge our message and let us know they're looking into the problem.

March 30th, 1998

Responses from Vendors (2)

"This is absolutely PATHETIC. I warned about these kinds of issues more than 6 months ago."

- **We have no record of such a warning anywhere.**
- **This quote constitutes the entire text of the message.**

March 30th, 1998

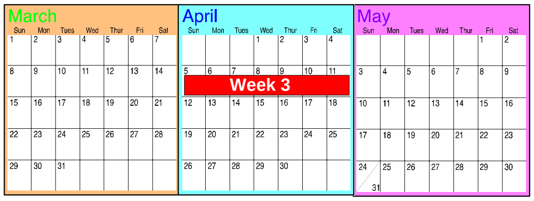
Responses from Vendors (3)

"[Vendor] has new BIND packages for [product] ready to go. I'd like to know what time frame you're planning this announcement for, so we can make sure we have our web pages updated simultaneously."

- **Quick patch production**
- **Note that we had provided them the time frame in the initial message.**

March 31st, 1998

Week Three



March

Sun	Mon	Tues	Wed	Thur	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

April

Sun	Mon	Tues	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Week 3

May

Sun	Mon	Tues	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24 31	25	26	27	28	29	30

Complicating Issues

Publicly available beta code.

One vendor made an announcement of "security fixes in BIND" at a users-group meeting.

- **Word has started to spread quickly**
- **Receiving questions about it**

April 5th, 1998

Accelerated Launch

We decide to move the announcement up to April 8th.

We contact Paul, who says:

- **No vendor has contacted him about the patches.**
- **The patches have been posted on the bind-workers mailing list.**

April 6th, 1998

Contacting the Vendors Again

We inform them of the accelerated launch schedule

- Unhappy responses

We provide them with pointers to Paul’s patches

- Urge them to be sure that their engineers are aware of these patches.

We urge for them to send us the latest information on patches to be included in the advisory.

April 7th, 1998

CERT Advisory CA-98.05

April 08, 1998 -- 15 days after the original report

- The vendors have the patches.
- Many vendors are still vulnerable at advisory launch time.
- In the worst case, a system administrator can compile Paul Vixie’s version of BIND for their systems.

April 8th, 1998

Test Programs Appear

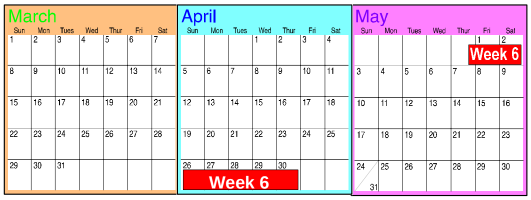
A message is posted to BugTraq including code to determine if fake-iquery is enabled or not.

- Rough indication of vulnerability
- Apparently from student at Central Michigan University with no prior knowledge of the vulnerability.

http://www.geek-girl.com/bugtraq/1998_2/0057.html

April 10th, 1998

Week Six



March

Sun	Mon	Tues	Wed	Thur	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

April

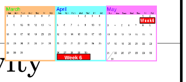
Sun	Mon	Tues	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Week 6

May

Sun	Mon	Tues	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24 31	25	26	27	28	29	30

Week 6


Week 6
Week 6

The First Reports of Activity

The first reports were not obviously related:

A root compromised site scanning other sites:

- Probably compromised via IMAP vulnerability
- Intruder appears to be scanning for BIND

Several other root compromised systems:

- Trojan horse programs installed
- Not known how intruder gained access
- Reports of named crashes and SYN flooding

May 1st, 1998

Week 6
Week 6

Copy of “hide” Archive Obtained

A site sends us the “hide” archive:

- Site is root compromised
- Trojan horse programs have been installed
- It is not clear how the intruder gained access

- Unauthorized transfer found in .ncftp file
- Administrator obtains a copy of the archive for analysis, and then sends us a copy

- Administrator of FTP server is alerted to the activity

May 1st, 1998

Contents of the “hide” Archive

When the archive is analyzed, it contains:

- Linux executables and shell scripts
- Trojan horse programs
  - inetd, named, tcpd, syslogd, ifconfig, ls, ps, pstree, netstat, top
- A sniffer program named “reset”
- An installation script named “ins”
- An installation program named “fix”
- Rootkit configuration files starting with “pmcf”?

May 1st, 1998

Another Intruder Archive

Another root compromised site sends us an archive:

- Contains several copies of the “hide” archive
- Also contains source code
  - Appears to be source code for the “named” program contained in the “hide” archive
  - Contains a backdoor that opens an xterminal window on the originating host
  - Backdoor is triggered by a connection from a specific port
  - This hostname is referenced in the “named” program in the “hide” archive

May 2nd, 1998

Week Seven

March

Sun	Mon	Tues	Wed	Thur	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

April

Sun	Mon	Tues	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

May

Sun	Mon	Tues	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24 31	25	26	27	28	29	30

Week 7

Exploit String Found in Core Dump

A site reports finding an exploit string in a core dump:

- Named servers had crashed twice recently.
- They find strange commands in the core dump.
- The string they find matches that supplied by the site who was scanning other systems.

- It also references the:
  - Site scanning other systems
  - “hide” archive
  - FTP server distributing the “hide” archive

May 3rd, 1998

The Exploit String

The exploit string appears to:

- Telnet to the scanning host on port 666
- Use ncftp to obtain the “hide” archive
- Unpack the archive
- Run the install script

May 3rd, 1998

Activity Is Interesting

This activity now has interesting characteristics:

- Reported by several sites
- Consistent MO is beginning to emerge
- May be automated (widespread scanning)
- Involves a vulnerability that is not clearly defined

So we gather additional information by contacting:

- The scanning site for logs, exploit scripts, etc.
- The FTP server site, for FTP transfer logs
- More root compromised sites reporting the activity

May 3rd, 1998

The Scope of the Activity

Information gathered from several sites help us determine the scope of the activity:

- **More sites reporting activity**
- **Sites have reported crashed name servers on April 29th and May1st**
- **Scanning site has logs showing 84 hosts that made connections to port 666**
- **FTP server sends us a transfer log showing over 730 hosts who have obtained the “hide” archive**
- **USENET articles indicate related activity**
- **Scanning site does not have exploit scripts**
- **Seems to be targeting delegated domain name servers (possibly by using zone transfers)**

May 5th, 6th & 7th, 1998

What We Know About the Activity

We know the following:

- **A site was scanning other systems.**
- **Sites are being root compromised.**
- **Trojan horse programs are being installed.**
- **Name servers are crashing.**
- **A large number of sites are involved.**

- **The activity appears to be circumstantially related to the BIND vulnerability.**

May 8th, 1998

Speculated Explanation

An intruder is scanning systems for a buffer overflow vulnerability in BIND.

The buffer overflow exploit is Linux specific.

If the system is a vulnerable Linux system, the intruder installs the contents of the “hide” archive as part of the exploit.

If the system is a vulnerable non-Linux system, then the named server crashes, leaving the exploit string in the core file.

May 8th, 1998

Unanswered Questions

Is the vulnerability one of the ones described in CERT Advisory CA-98.05?

If it is, which of the vulnerabilities is it?

If it is the inverse query vulnerability, how did the intruder find so many systems with the fake-iquery option enabled?

Are we even sure that the activity involves a vulnerability in BIND?

May 8th, 1998

More Unanswered Questions

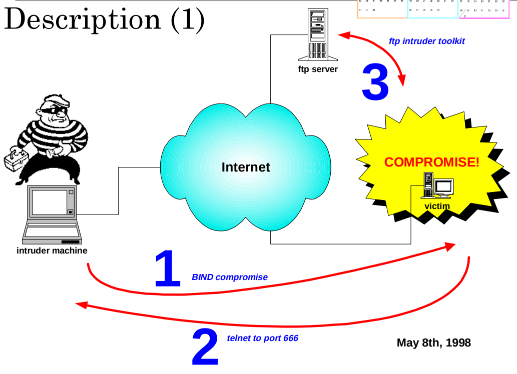
Why do we have a report of a crashed named server on a Linux system?

Do we have reports of any compromised non-Linux systems?

Where can we get a copy of the exploit code to learn more about the activity?

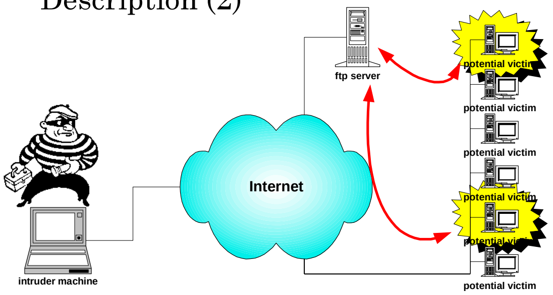
May 8th, 1998

Description (1)



May 8th, 1998

Description (2)



May 8th, 1998

ftp site logs

We receive logs from an ftp site showing hundreds of downloads of the toolkit.

May 8th, 1998

Week Eight

March

Sun	Mon	Tues	Wed	Thur	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

April

Sun	Mon	Tues	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

May

Sun	Mon	Tues	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
	Week 8					
17	18	19	20	21	22	23
24 31	25	26	27	28	29	30

Drafting a Description of the Activity

Our goals in describing the activity are:
- Alert compromised sites of this activity
- Useful for detecting and recovering
- Separate facts from speculation
- Encourage the application of BIND patches

Our internal review process includes:
- Multiple drafts
- Peer review
- Extensive discussion about the activity and the unanswered questions mentioned earlier

May 8th - 13th, 1998

Obtaining Contact Info

Obtaining contacts for over 700 hosts is not easy:
- Takes a long time (due to server delays)
- Input is a mix of hostnames and IP addresses
- No single server has complete contact information

We solve the problem with a Perl script:
- Uses RWhois for obtaining most contacts
- Uses other Whois servers when needed
- Translates between IP addresses and hostnames
- Parses output from multiple Whois servers

May 8th - 13th, 1998

Generating Email Messages

Generating over 700 mail messages isn't easy either, since each message:
- May have multiple recipients
- Includes different data (log entries, hostnames)
- Needs to be PGP signed
- May need to be reviewed before it is sent

We already have a Perl script that does most of this:
- Generates and sends in two steps
- Works with the contact information we collected

May 8th - 13th, 1998

Contacting the First Batch of Sites

We send mail to 233 sites, and receive:

- 9 email bounces
- 22 email responses
- 6 phone calls

within the first 8-10 hours after the mail is sent.

May 14th, 1998

New Information Received

Responses provide new information:

- A report from a compromised site that claims to have installed the patch for CA-98.05.
- Multiple reports that fake-iquery was not enabled.
- The identity of an FTP server used in similar attacks on April 29th.
- Several sites report intruder activity in addition to the activity we have described.
- Based on sites responding, almost all of the sites we contacted are compromised.
- Our first (and only?) complaint.

May 14th, 1998

Contacting the Second Batch of Sites

We send mail to another 236 sites, and receive:

- More email and phone calls
- Indications of activity as early as April 16th
- More reports of compromised systems that claimed to have applied the patches or were not vulnerable.

Complicated by:

- Multiple compromise dates
- Several sites applied the BIND patches in response to “strange named” behavior resulting from the Trojan horse named program.

May 15th, 1998

New Vulnerability in BIND?

Concerned that there might be a new vulnerability in BIND, we contact the BIND maintainers:

- Describe the activity
- Mention recent reports from sites claiming they weren’t vulnerable

They respond by saying:

- It looks like the vulnerability is the same one described in CERT Advisory CA-98.05.
- Red Hat Linux systems are vulnerable by default, due to a compile time option.

May 15th, 1998

Week Nine

March

Sun	Mon	Tues	Wed	Thur	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

April

Sun	Mon	Tues	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

May

Sun	Mon	Tues	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24 31	25	26	27	28	29	30

Week 9

A New Version of the Exploit String

A site reports observing a scan to BIND ports involving a modified exploit string:

- Uses FTP instead of ncftp
- Mentions a new scanning host
- References a new FTP server
- Exploit script appears to be evolving

Soon followed by additional reports of the exploit string being found in core files.

Decide to contact the FTP server site and obtain a copy of the logs.

May 17th - 21st, 1998

CERT Summary CS-98.04

The description of the activity is revised to produce a Special Edition CERT Summary:
- Update to contain new information
- Reword for more general audience
- Additional peer review

Summary is published on May 21st, 1998.

May 21st, 1998

Contacting Additional Sites

We send mail to additional sites
- 249 sites from the first FTP transfer log
- 319 sites from the second FTP transfer log

We continue to receive responses:
- Electronic mail
- Hotline calls
- Reports from other CSIRTs

May 22nd & May 25th, 1998

Potential Vul in Patched Version

We receive an exploit script which claims to exploit BIND 4.9.8 [sic].

We verify in our lab that it does not. ISC also states they believe 4.9.7 is not vulnerable to the script.

May 22nd, 1998

The ADM Inet w0rm

We discover a toolkit on a popular intruder toolkit web site and shortly after that a site reports it has been discovered running.

The toolkit has the following qualities:
- scans blocks of addresses for machines running domain name servers
- tests to see if the domain name server is vulnerable
- attempts to compromise
- has potential to be self-replicating

May 22nd, 1998

Analyzing the “Worm”

We analyse the toolkit in our lab and find that:
- it can compromise Intel-based Linux machines
- it has the potential to be self-replicating if two lines are uncommented
- it is inefficient in scanning
- with little effort, it could be greatly improved

May 22nd, 1998

Week Ten

April

Sun	Mon	Tues	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

May

Sun	Mon	Tues	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Week 10

June

Sun	Mon	Tues	Wed	Thur	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Weekend Activity

Over the holiday weekend, several sites report observing the toolkit running, but there is no evidence that the toolkit is spreading through replication.

May 23rd, 24th, & 25th, 1998

New MOs are Reported

Intruders begin mixing parts of existing tools to form new tools/toolkits.

We begin seeing an exploit of BIND where intruders open Xterminal windows back to the intruder's machine.

We see increased BIND incident reports with:

- sniffers running
- ssh Trojan horses

May 25th - 30th 1998

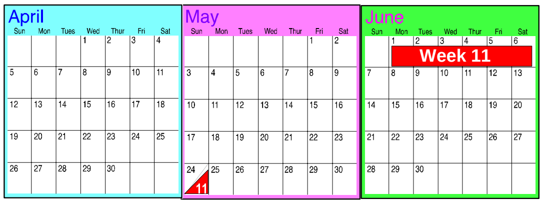
Second CERT Summary

A second Special Edition CERT Summary is drafted describing the latest tools intruders are using.

The summary is launched on May 28th.

May 25th - 28th, 1998

Week Eleven



April

Sun	Mon	Tues	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

May

Sun	Mon	Tues	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24 11	25	26	27	28	29	30

June

Sun	Mon	Tues	Wed	Thur	Fri	Sat
	1	2	3	4	5	6
	Week 11					
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Exploit Code Publicly Available

A message posted to BugTraq includes code to compromise Linux and FreeBSD Systems.

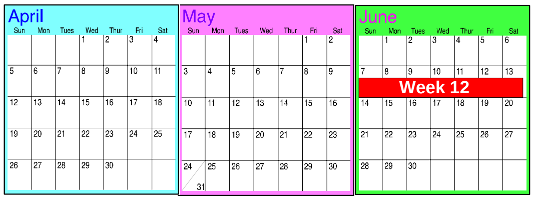
Specifically does not include an exploit for SunOS because "giving that out might actually cause some problems."

Makes references to CERT Advisory CA-98.05 and "Script Kiddies".

http://www.geek-girl.com/bugtraq/1998_2/0446.html

May 31st, 1998

Week Twelve



April

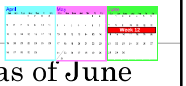
Sun	Mon	Tues	Wed	Thur	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

May

Sun	Mon	Tues	Wed	Thur	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24 31	25	26	27	28	29	30

June

Sun	Mon	Tues	Wed	Thur	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
Week 12						
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				



Activity Involving BIND as of June

We continue to receive reports of compromises involving BIND.

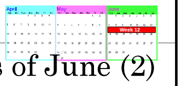
It appears that many of the primary and secondary name servers have now been patched, but intruders are now scanning IP addresses sequentially.

Awareness of the activity appears to be increasing, but there are still many **vulnerable systems.**

June 11th, 1998

Activity Involving BIND as of June (2)

Intruders continue to use DNS zone transfers to find target hosts as well as use scans of ranges of IP numbers.



Activity Involving BIND as of June (2)

We now have multiple reports of similar activity, with different archive names, hosts involved, and exploit strings.

Reports of related activity are now part of our daily routine, much like IMAP and PHF probes, root compromises involving RootKit, etc.

In all, over 1,600 hosts are known to CERT to have been compromised by the vulnerability in BIND.

We still receive reports from people saying that their domain name server is crashing and they do not know why.

June 11th, 1998

Apply Patches for the Vulnerability

Documents describing this activity:

- **CERT Advisory CA-98.05**
- **Special Edition CERT Summary CA-98.04**
- **Special Edition CERT Summary CA-98.05**

June 11th, 1998

CERT® Contact Information

24-hour hotline:	**+1 412 268 7090** **CERT personnel answer 8:30 a.m. — 5:00 p.m. EST(GMT-5) / EDT(GMT-4), and are on call for emergencies during other hours.**
Fax:	**+1 412 268 6989**
Anonymous FTP archive:	**ftp://ftp.cert.org/pub/**
Web site:	**http://www.cert.org/**
Electronic mail:	**cert@cert.org**
PGP Key ID	**2DE30EC1**
PGP Key fingerprint	**E6 DD E6 E9 97 6B 4C FB** **2E 91 02 68 DC B4 85 9A**
US mail:	**CERT Coordination Center** **Software Engineering Institute** **Carnegie Mellon University** **4500 Fifth Avenue** **Pittsburgh PA 15213-3890** **USA**