An Update on the Code Red Worm

20 August 2001

Gary C. Kessler
Champlain College
Vermont InfraGard Chapter
Burlington, VT

50 Creek Glen
Colchester, VT 05446
http://www.garykessler.net

kumquat@sover.net
+1 802-879-3375
+1 802-238-8913 (cell)
+1 630-604-5529 (fax)

What is Code Red?

- Code Red is a worm that exploits a known buffer overflow vulnerability in IIS 4.0/5.0
  - » Scans TCP port 80 on random IP addresses to find systems with exploitable vulnerability
  - » Infected systems look for 100 additional systems
  - » Malformed GET can also affect non-IIS software
  - » Resides only in RAM; rebooting clears the worm
- Code Red I causes high traffic loads on the Internet, Web defacements, DDoS attack on "whitehouse.gov", and crashed systems
- Code Red II causes extraordinarily high traffic loads, crashed systems, and installs backdoors

Code Red Targets

- Primary targets are Windows NT 4.0 and Windows 2000 systems running IIS 4.0 or IIS 5.0
  - » IIS 5.0 autoinstalls on Windows 2000 Server
  - » PWS (Peer Web Services) **is** IIS 5.0 and runs on W2K Professional (but doesn't autoinstall)
  - » One source also mentioned Windows XP beta running IIS 6.0 beta...
- PWS (Personal Web Server) runs only on Windows 9x/ME and is not prone to Code Red exploit

Other Code Red Victims

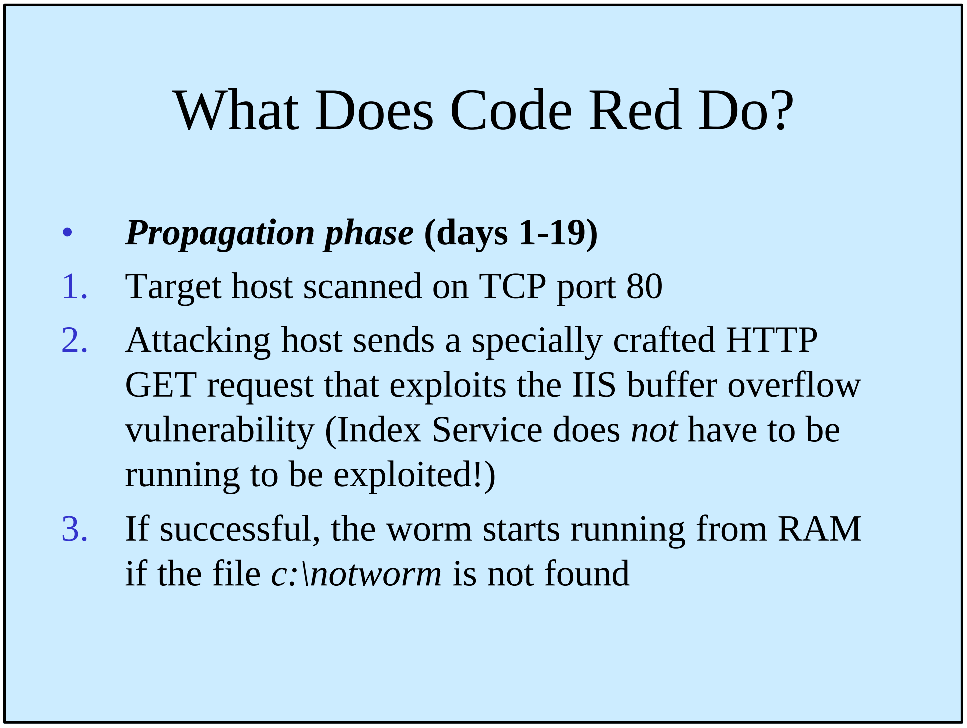
- Some other systems listen on TCP port 80 and crash upon receiving the malformed GET
  - » Cisco 600 DSL routers
  - » Some printers using HP JetDirect
  - » Others??

Time Line

- On 18 June 2001, Microsoft issues Security Bulletin MS01-33 warning about a buffer overflow condition in the IIS Indexing Service ISAPI filter and provides a patch
  - » Administrative scripts (.ida) and Internet data queries (.idq) filters do not do proper bounds checking
  - » eEye Digital Security also issues a warning (18 June)
  - » CERT/CC issues CA-2001-13 (19 June)
- On July 13, eEye reports receiving logs indicating huge volumes of attack traffic targeting .ida
  - » Code Red name given to worm

Time Line (2)

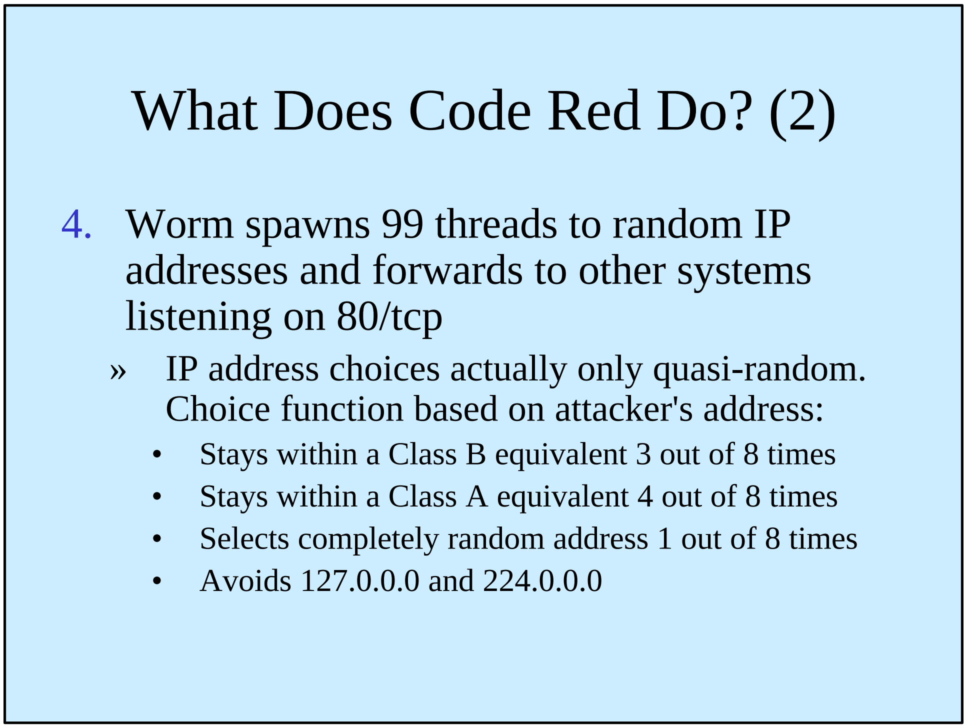
- Early reports indicated that worm would launch a DDoS attack on the White House's IP address on the 20th of the month
  - » *www.whitehouse.gov* IP address was changed
  - » Full-blown analysis begins
- Lots of conflicting information appeared on 29-30 July about possible attacks on 1 August
  - » Volume of 80/tcp traffic does increase after 1 Aug. and surpasses July volume in a few days



What Does Code Red Do?

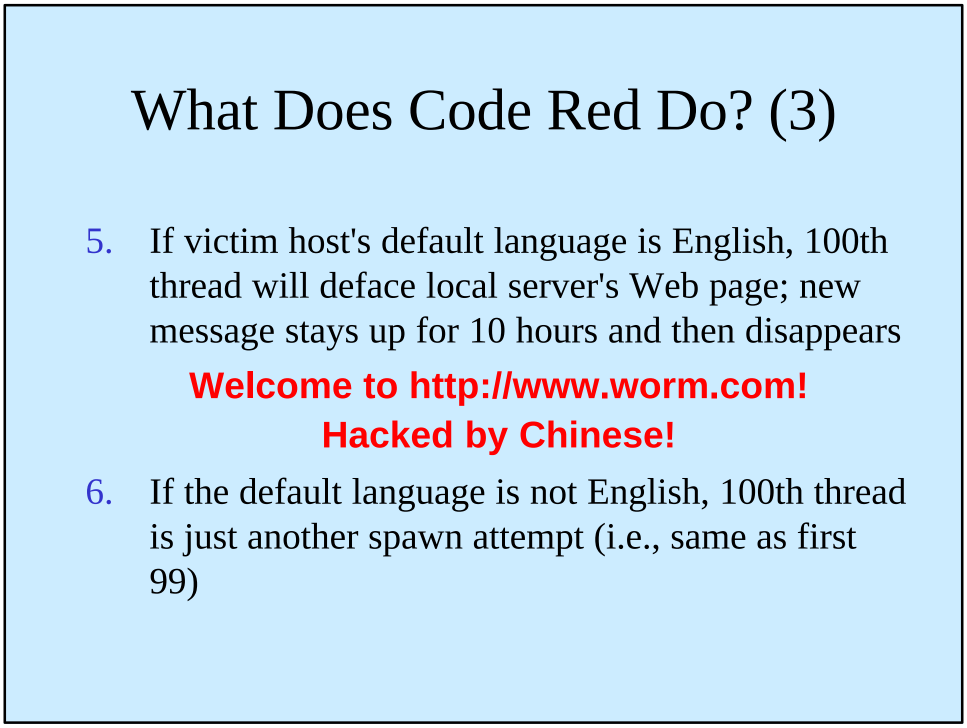
- ***Propagation phase* (days 1-19)**

1. Target host scanned on TCP port 80
2. Attacking host sends a specially crafted HTTP GET request that exploits the IIS buffer overflow vulnerability (Index Service does *not* have to be running to be exploited!)
3. If successful, the worm starts running from RAM if the file *c:\notworm* is not found



What Does Code Red Do? (2)

4. Worm spawns 99 threads to random IP addresses and forwards to other systems listening on 80/tcp
   - » IP address choices actually only quasi-random. Choice function based on attacker's address:
     - Stays within a Class B equivalent 3 out of 8 times
     - Stays within a Class A equivalent 4 out of 8 times
     - Selects completely random address 1 out of 8 times
     - Avoids 127.0.0.0 and 224.0.0.0

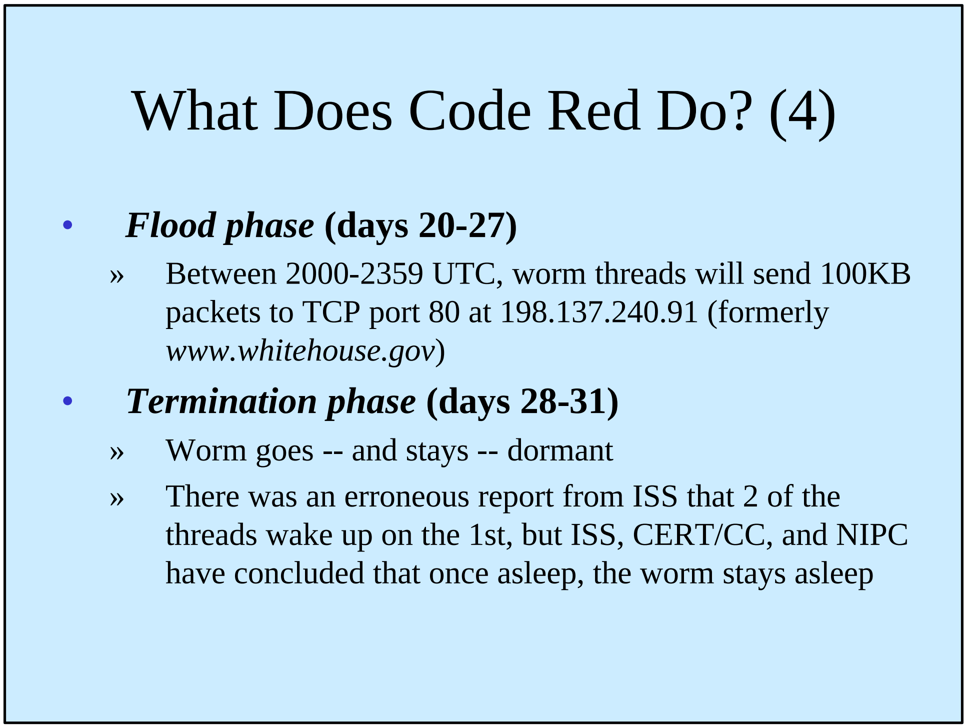


What Does Code Red Do? (3)

5. If victim host's default language is English, 100th thread will deface local server's Web page; new message stays up for 10 hours and then disappears

Welcome to http://www.worm.com!
Hacked by Chinese!

6. If the default language is not English, 100th thread is just another spawn attempt (i.e., same as first 99)



What Does Code Red Do? (4)

- ***Flood phase* (days 20-27)**
  - Between 2000-2359 UTC, worm threads will send 100KB packets to TCP port 80 at 198.137.240.91 (formerly *www.whitehouse.gov*)
- ***Termination phase* (days 28-31)**
  - Worm goes -- and stays -- dormant
  - There was an erroneous report from ISS that 2 of the threads wake up on the 1st, but ISS, CERT/CC, and NIPC have concluded that once asleep, the worm stays asleep

Versions of Code Red

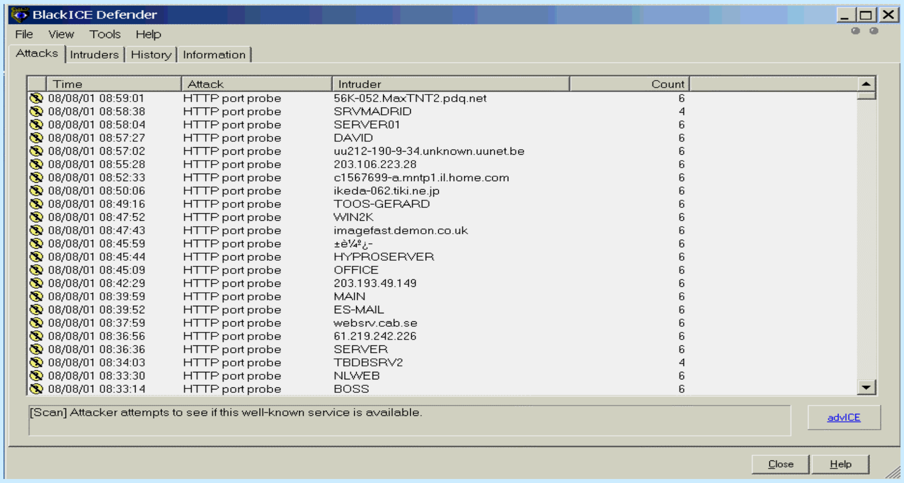
- Code Red, the original, described here
  - » Three variants
- Code Red II is new code but exploits similar vulnerability as Code Red
  - » Two variants; initially appeared on 4 Aug.
  - » No Web defacement nor DDoS but spreads *very* fast (300 or more threads per victim)
  - » Installs backdoors in the system, e.g., registry changes, Trojan *explorer.exe*, disables SFC

What You Might See in a Log File

From OmniHTTPd *access_log*

```
211.5.255.44 - - [16/Aug/2001:11:30:49 -0400] "GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9
090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%uc
bd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0
078%u0000%u00=a  HTTP/1.0" 400 357
205.214.95.164 - - [16/Aug/2001:11:38:22 -0400] "GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9
090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%uc
bd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0
078%u0000%u00=a  HTTP/1.0" 404 310
```

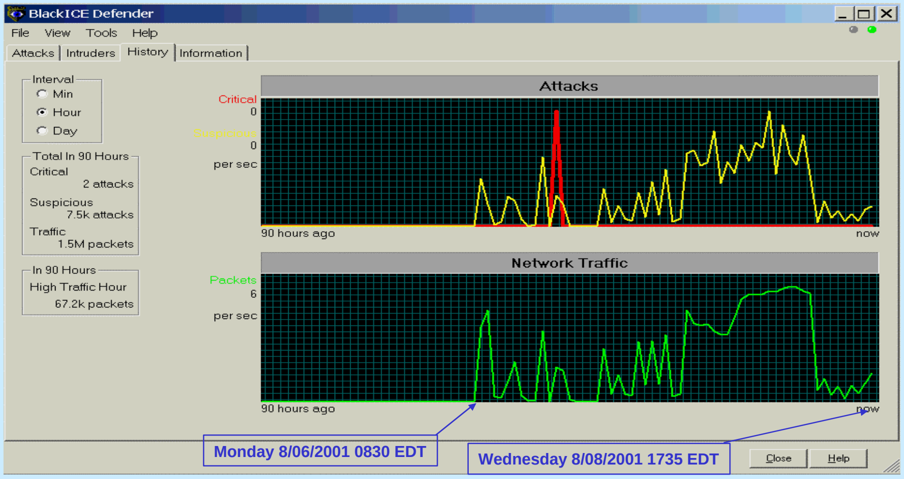
An Increase in Port 80 Scans



Time	Attack	Intruder	Count
08/08/01 08:59:01	HTTP port probe	56K-052.MaxTNT2.pdq.net	6
08/08/01 08:58:38	HTTP port probe	SRVMADRID	4
08/08/01 08:58:04	HTTP port probe	SERVER01	6
08/08/01 08:57:27	HTTP port probe	DAVID	6
08/08/01 08:57:02	HTTP port probe	uu212-190-9-34.unknown.uunet.be	6
08/08/01 08:55:28	HTTP port probe	203.106.223.28	6
08/08/01 08:52:33	HTTP port probe	c1567699-a.mntp1.il.home.com	6
08/08/01 08:50:06	HTTP port probe	ikeda-062.tiki.ne.jp	6
08/08/01 08:49:16	HTTP port probe	TOOS-GERARD	6
08/08/01 08:47:52	HTTP port probe	WIN2K	6
08/08/01 08:47:43	HTTP port probe	imagefast.demon.co.uk	6
08/08/01 08:45:59	HTTP port probe	±è¼º¿-	6
08/08/01 08:45:44	HTTP port probe	HYPROSERVER	6
08/08/01 08:45:09	HTTP port probe	OFFICE	6
08/08/01 08:42:29	HTTP port probe	203.193.49.149	6
08/08/01 08:39:59	HTTP port probe	MAIN	6
08/08/01 08:39:52	HTTP port probe	ES-MAIL	6
08/08/01 08:37:59	HTTP port probe	websrv.cab.se	6
08/08/01 08:36:56	HTTP port probe	61.219.242.226	6
08/08/01 08:36:36	HTTP port probe	SERVER	6
08/08/01 08:34:03	HTTP port probe	TBDBSRV2	4
08/08/01 08:33:30	HTTP port probe	NLWEB	6
08/08/01 08:33:14	HTTP port probe	BOSS	6

[Scan] Attacker attempts to see if this well-known service is available.

An Increase in Port 80 Scans (2)

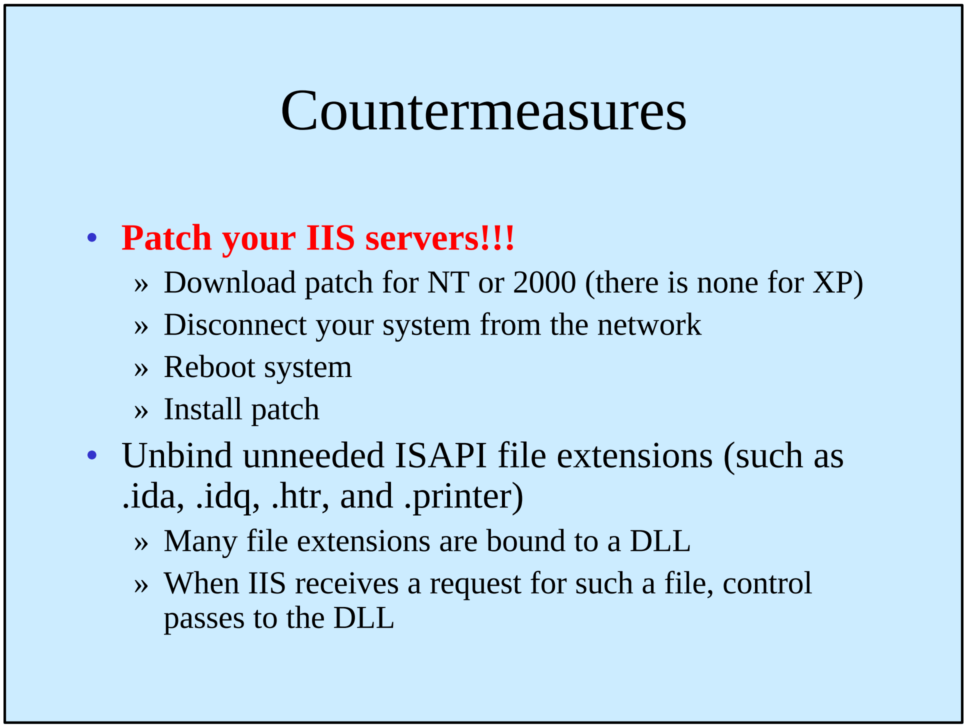


Total In 90 Hours
Critical 2 attacks
Suspicious 7.5k attacks
Traffic 1.5M packets

In 90 Hours
High Traffic Hour 67.2k packets

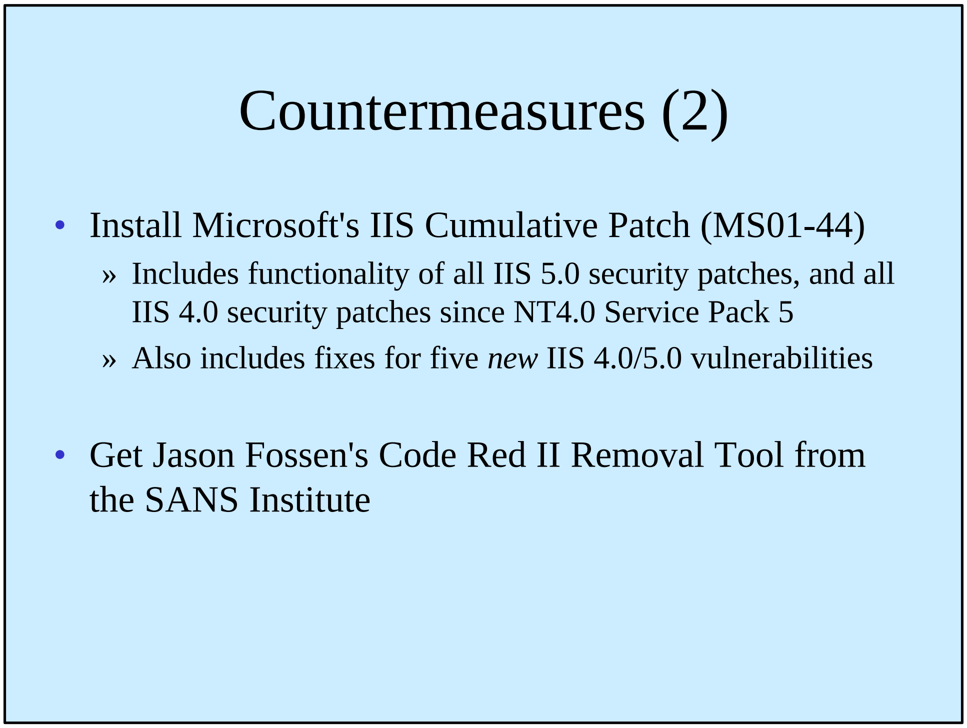
Monday 8/06/2001 0830 EDT

Wednesday 8/08/2001 1735 EDT



Countermeasures

- **Patch your IIS servers!!!**
  - » Download patch for NT or 2000 (there is none for XP)
  - » Disconnect your system from the network
  - » Reboot system
  - » Install patch
- Unbind unneeded ISAPI file extensions (such as .ida, .idq, .htr, and .printer)
  - » Many file extensions are bound to a DLL
  - » When IIS receives a request for such a file, control passes to the DLL



Countermeasures (2)

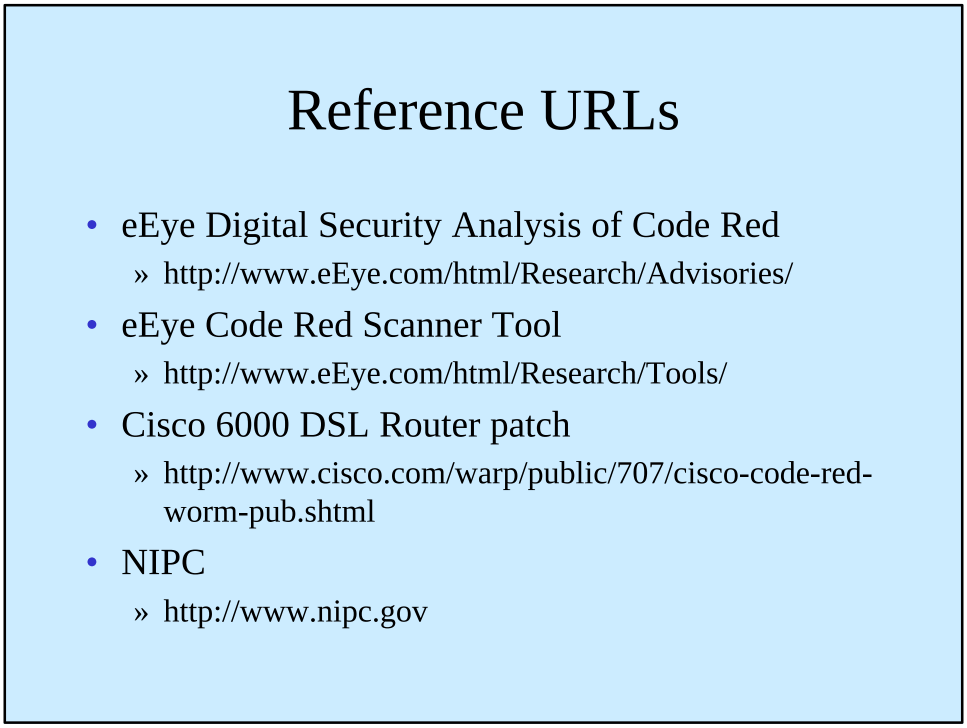
- Install Microsoft's IIS Cumulative Patch (MS01-44)
  - » Includes functionality of all IIS 5.0 security patches, and all IIS 4.0 security patches since NT4.0 Service Pack 5
  - » Also includes fixes for five *new* IIS 4.0/5.0 vulnerabilities
- Get Jason Fossen's Code Red II Removal Tool from the SANS Institute

Other Things to Consider

- Don't use IIS
  - » Consider Apache, OmniHTTPd, others...
- Don't use any Windows-based Web server...
- Send logs to DShield.org
  - » Clients for BlackICE Defender, Checkpoint Firewall-1, Cisco PIX, Linksys EtherFast Cable/DSL Router, Linux IPchains/IPtables, Norton Personal Firewall, Psionic Portsentry, Snort, ZoneAlarm, and more....

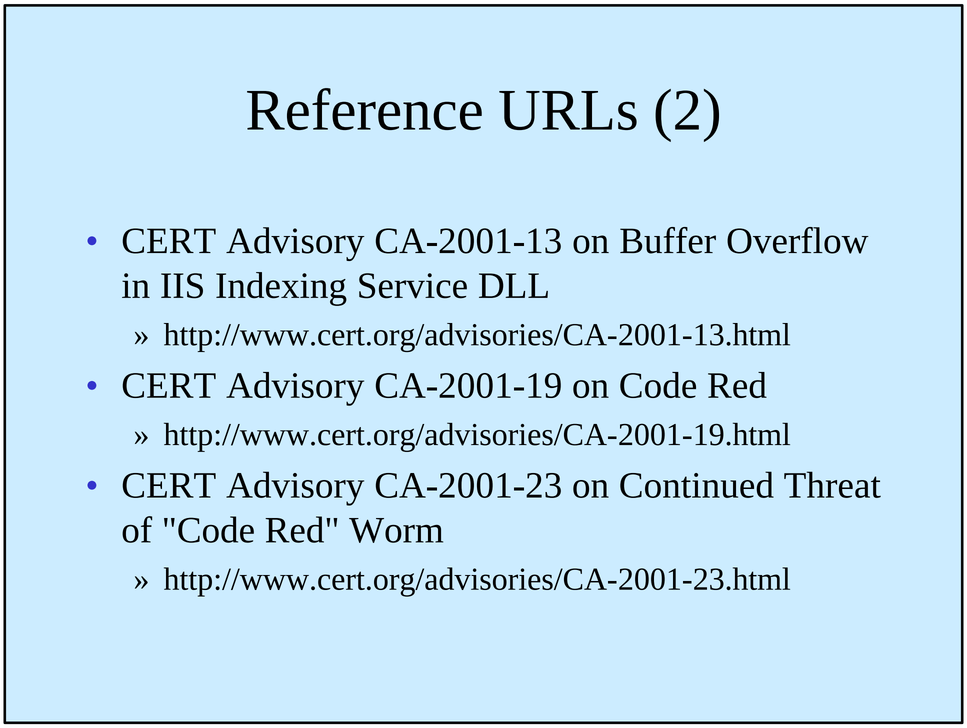
A Couple of Other Observations

- What was Code Red, really?
  - » A proof-of-concept?
- Code Red totally obscured other real threats in July and August
  - » Where was the news about Sircam?



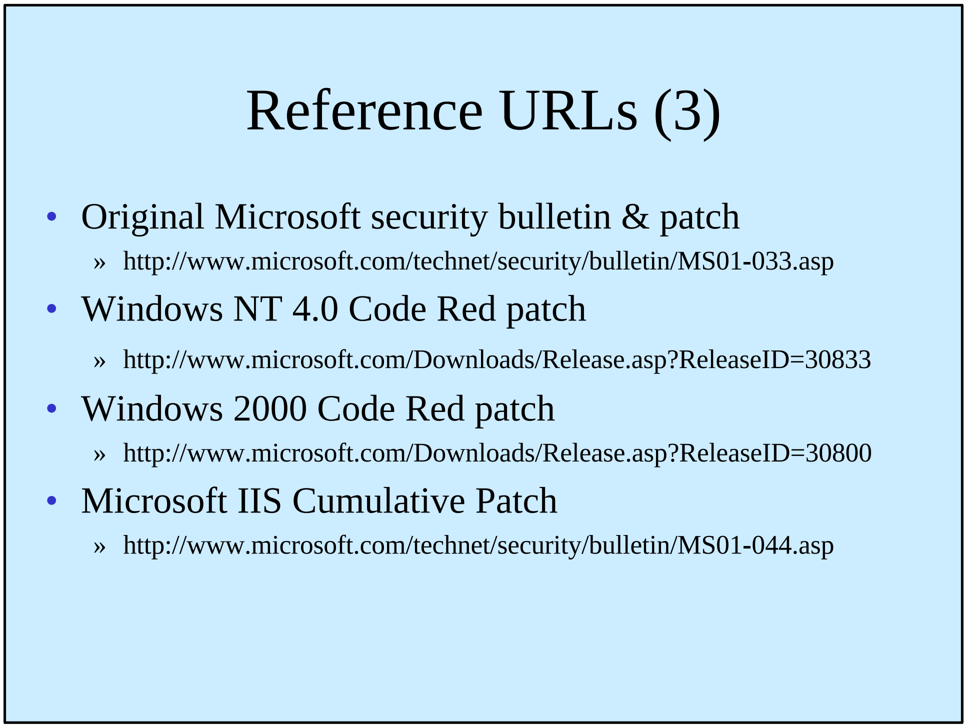
Reference URLs

- eYe Digital Security Analysis of Code Red
  - » http://www.eEye.com/html/Research/Advisories/
- eEye Code Red Scanner Tool
  - » http://www.eEye.com/html/Research/Tools/
- Cisco 6000 DSL Router patch
  - » http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml
- NIPC
  - » http://www.nipc.gov



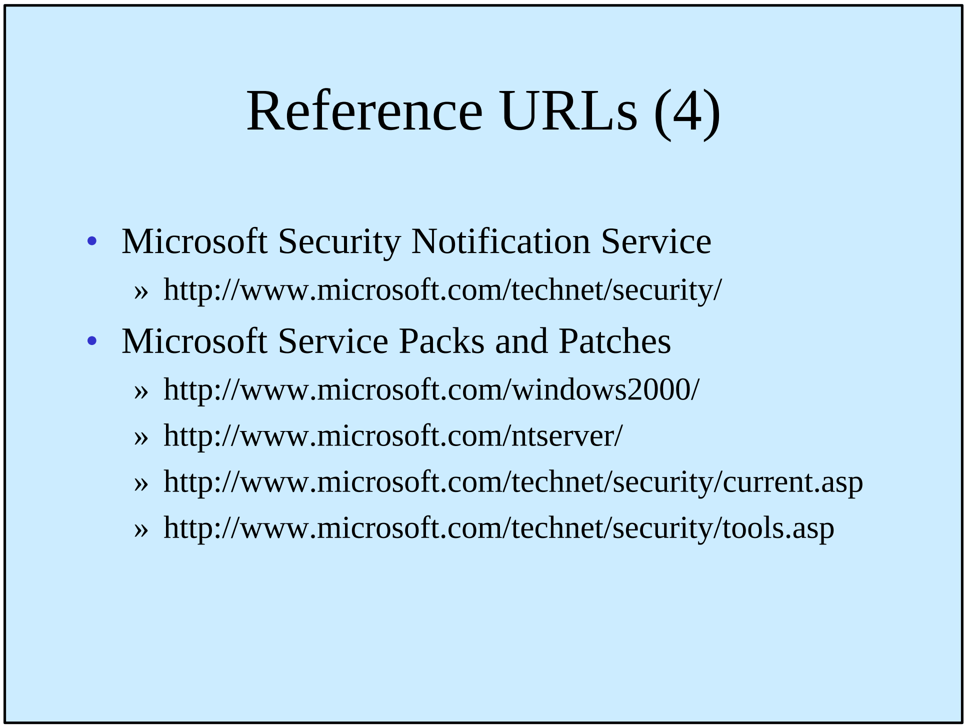
Reference URLs (2)

- CERT Advisory CA-2001-13 on Buffer Overflow in IIS Indexing Service DLL
  - » http://www.cert.org/advisories/CA-2001-13.html
- CERT Advisory CA-2001-19 on Code Red
  - » http://www.cert.org/advisories/CA-2001-19.html
- CERT Advisory CA-2001-23 on Continued Threat of "Code Red" Worm
  - » http://www.cert.org/advisories/CA-2001-23.html



Reference URLs (3)

- Original Microsoft security bulletin & patch
  - » http://www.microsoft.com/technet/security/bulletin/MS01-033.asp
- Windows NT 4.0 Code Red patch
  - » http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833
- Windows 2000 Code Red patch
  - » http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800
- Microsoft IIS Cumulative Patch
  - » http://www.microsoft.com/technet/security/bulletin/MS01-044.asp



Reference URLs (4)

- Microsoft Security Notification Service
  - » http://www.microsoft.com/technet/security/
- Microsoft Service Packs and Patches
  - » http://www.microsoft.com/windows2000/
  - » http://www.microsoft.com/ntserver/
  - » http://www.microsoft.com/technet/security/current.asp
  - » http://www.microsoft.com/technet/security/tools.asp

Reference URLs (5)

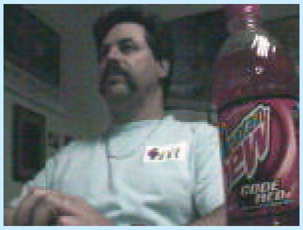
- SANS Institute NewsBites
  - » http://www.sans.org/newlook/digests/newsbites.htm
- SANS Institute Windows Digest
  - » http://www.sans.org/newlook/digests/ntdigest.htm
- Jason Fossen's Code Red II Removal Tool
  - » http://www.incidents.org/react/AntiCodeRed2.vbs
- DShield.org
  - » http://www.dshield.org

Reference URLs (6)

- www.incidents.org
  - » http://www.incidents.org/
- Digital Island's Code Red page
  - » http://www.digitalisland.net/codered/
- CAIDA's Code Red Analysis
  - » http://www.caida.org/analysis/security/code-red/
- NTBugTraq
  - » http://www.ntbugtraq.com/

Acronyms and Abbreviations

CA	CERT Advisory
CAIDA	Cooperative Association for Internet Data Analysis
CERT/CC	CERT Coordination Center
DDoS	Distributed denial of service
DLL	Dynamic linked library
DSL	Digital Subscriber Line
EDT	Eastern Daylight Time (UTC -0400)
HTTP	Hypertext Transfer Protocol
IIS	Internet Information Service (MS)
IP	Internet Protocol
ISAPI	Internet Service Application Program Interface (MS)
ISS	Internet Security Systems
KB	kilobytes (10^3)
MS	Microsoft
NIPC	National Infrastructure Protection Center
PWS	Peer Web Services (Win2K Pro IIS 5.0)
PWS	Personal Web Server (Windows 9x/ME)
RAM	Random access memory
SFC	System File Checker
TCP	Transmission Control Protocol
UTC	Universal Time, Coordinated (aka Greenwich Mean Time or Zulu)



The author preparing this presentation...