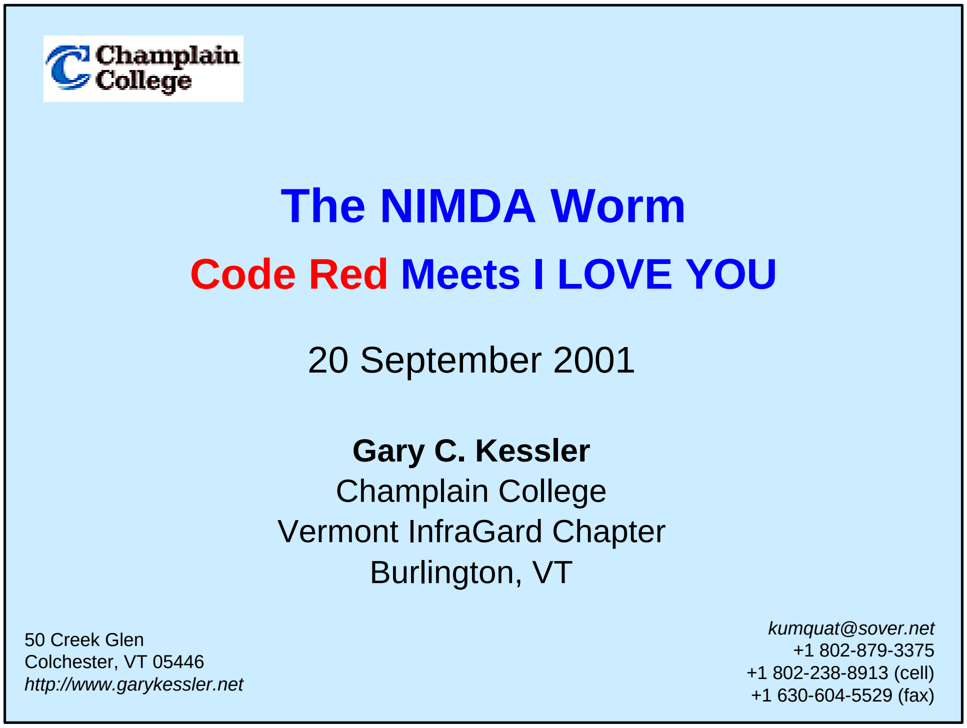


The NIMDA Worm

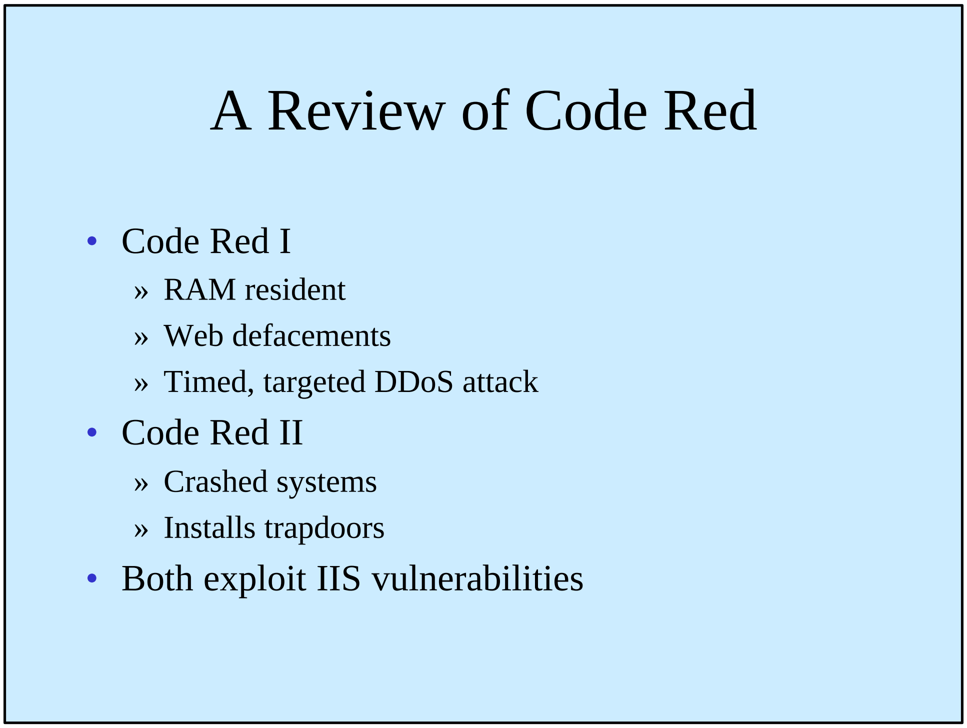
Code Red Meets I LOVE YOU

20 September 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)



A Review of Code Red

- Code Red I
  - » RAM resident
  - » Web defacements
  - » Timed, targeted DDoS attack
- Code Red II
  - » Crashed systems
  - » Installs trapdoors
- Both exploit IIS vulnerabilities

Nimda Characteristics

- Nimda has been compared to Code Red... but it is some much more...
  - » Exploits vulnerabilities in IIS, IE, and MAPI
- Multiple propagation vectors
  - » Client to client via e-mail or network shares
  - » Web server to client via browser compromise
  - » Client to Web server via IIS exploits or Code Red II trapdoor

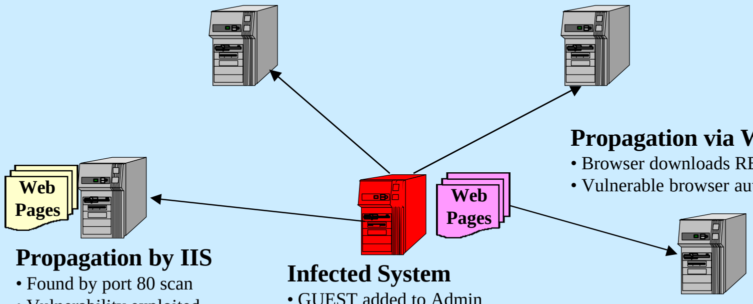
Nimda

- First seen on Tuesday, 18 September 2001
- Code contains following string:

```
Concept Virus (CV) V.5, Copyright(C) 2001 R.P. China
```

  - » Not the same as the Concept virus
  - » Name derived from ADMIN
- Significant jump in number of HTTP port 80 scans
  - » Much faster propagation than Code Red
  - » Increased tftp traffic

Propagation Vectors



Propagation by Network Shares
- Worm code written to writeable share

Propagation by E-mail
- E-mail client using IE HTML reader
- Autoexecutes README.EXE

Propagation via Web Pages
- Browser downloads README.EML via JS
- Vulnerable browser autoexecutes

Propagation by IIS
- Found by port 80 scan
- Vulnerability exploited
- ADMIN.DLL obtained via tftp

Infected System
- GUEST added to Admin
- Sharing turned on
- README.EXE file forwarded via e-mail
- If Web server, all HTML content pages compromised

IIS Propagation

- Infected system scans TCP port 80 looking for Web servers
  - » Most address scanning is local; random IP address use ~25%
- When a Web server is found, attacker attempts various exploits
  - » sadmind vulnerability
  - » Code Red II root.exe or other backdoor
  - » IIS Directory Traversal vulnerability
- Victim server obtains worm code (admin.dll) from attacker using tftp from cmd.exe

Web Browser Propagation

- Worm creates copies called readme.eml
  - » Small JavaScript code pointing to this page added to all Web-content files at infected site
- Browser visits site, activates page's JS code, and downloads readme.eml
  - » Vulnerable versions of Internet Explorer will auto-execute the file

E-Mail Propagation

- Nimda sends itself to e-mail addresses found in InBox and Address Book
  - » MIME-encoded, 56KB attached file named readme.exe
  - » Second section of file ("audio/x-wav") contains worm
  - » Long, repetitive subject line
- E-mail clients using IE 5.1 or earlier to display HTML will automatically execute the attachment if the **message** is opened or previewed.

Network Share Propagation

- Worm copies itself to
  - » All local directories on victim host
  - » All open, writeable network shares
- Worm also sets up shares on victim host

Other Noteworthy Actions

- GUEST is made member of Administrator group (PDC and stand-alone server only?)
  - » By default, GUEST account is active and has no password!
- Infects many programs and registry keys
- Consumes significant system resources
- Some reports that hardware damage occurs

Protection

- If you must use IIS
  - » Keep it up to the latest patch (see MS01-044) on a **clean** system
  - » The IIS Cumulative Patch does *not* clean your system of Code Red II backdoors
- If you use Internet Explorer
  - » Secure against MIME auto-execution
  - » IE 5.01 requires patch (MS01-020)
  - » IE 5.5 SP2 and IE 6.0 are already immune

Protection (2)

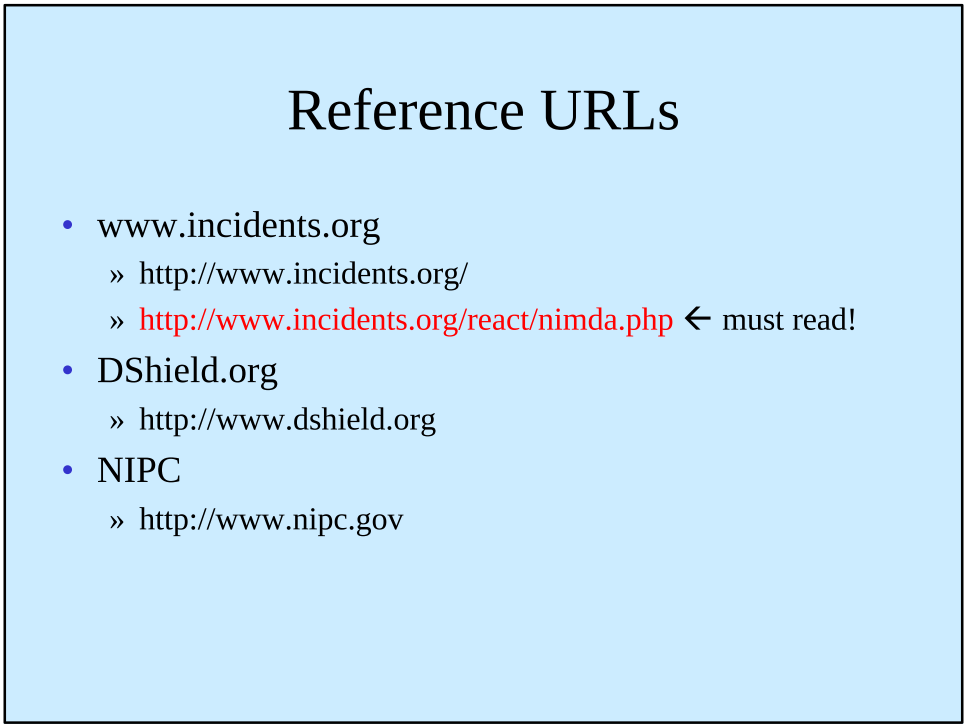
- Disable any and all unused accounts
  - » Enable Guest or anonymous access only if necessary
- Disable JavaScript (and Java and ActiveX) at your browser
  - » Turn on only if needed at a safe site
- Do not execute readme.exe or *any* e-mail attachment unless expected, known, and verified
- Use most up-to-date anti-virus signature files
- Unbind file and print sharing from TCP/IP
  - » Even in Windows 2000

Clean Up...

- There is no tool yet available that will "clean" Nimda from a system
- Alterations to infected systems, particularly Web servers, are so numerous that best current practice is to rebuild the system
  - » This may entail pulling all (suspect?) systems off the network, checking them one by one, and putting them back on after inspection or rebuild

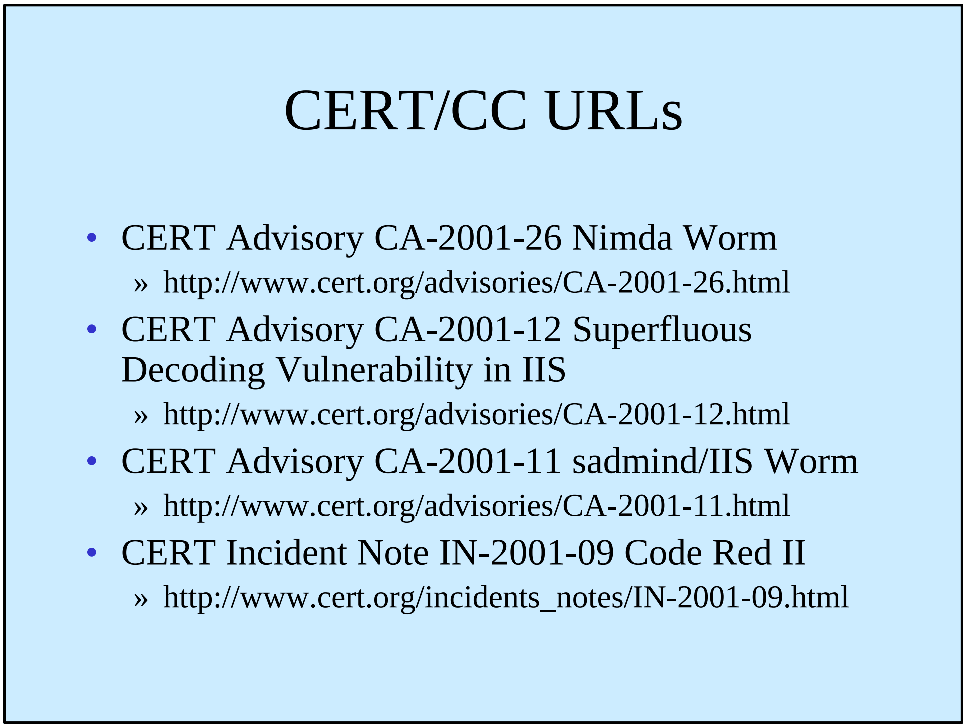
Other Things to Consider

- Reject code that is routinely exploited
  - » Don't use a Windows-based Web server...
    - Don't use IIS
  - » Don't use Internet Explorer
  - » Don't use Outlook, Outlook Express, or other MAPI e-mail clients
- Send logs to DShield.org



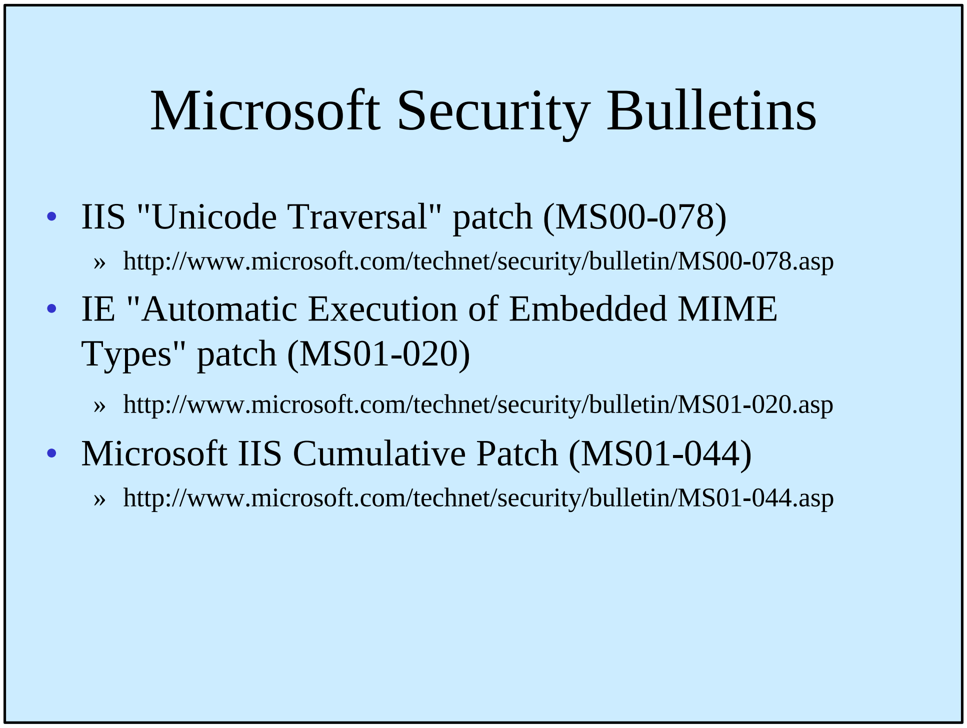
Reference URLs

- www.incidents.org
  - » http://www.incidents.org/
  - » http://www.incidents.org/react/nimda.php ← must read!
- DShield.org
  - » http://www.dshield.org
- NIPC
  - » http://www.nipc.gov



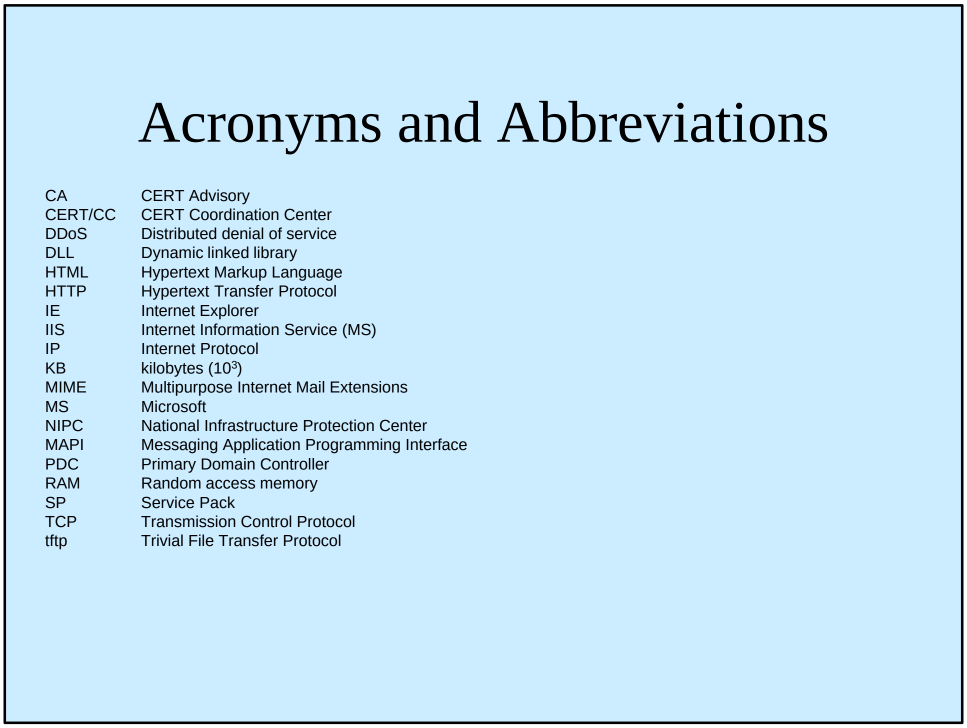
CERT/CC URLs

- CERT Advisory CA-2001-26 Nimda Worm
  - » http://www.cert.org/advisories/CA-2001-26.html
- CERT Advisory CA-2001-12 Superfluous Decoding Vulnerability in IIS
  - » http://www.cert.org/advisories/CA-2001-12.html
- CERT Advisory CA-2001-11 sadmind/IIS Worm
  - » http://www.cert.org/advisories/CA-2001-11.html
- CERT Incident Note IN-2001-09 Code Red II
  - » http://www.cert.org/incidents_notes/IN-2001-09.html



Microsoft Security Bulletins

- IIS "Unicode Traversal" patch (MS00-078)
  - » http://www.microsoft.com/technet/security/bulletin/MS00-078.asp
- IE "Automatic Execution of Embedded MIME Types" patch (MS01-020)
  - » http://www.microsoft.com/technet/security/bulletin/MS01-020.asp
- Microsoft IIS Cumulative Patch (MS01-044)
  - » http://www.microsoft.com/technet/security/bulletin/MS01-044.asp



Acronyms and Abbreviations

CA	CERT Advisory
CERT/CC	CERT Coordination Center
DDoS	Distributed denial of service
DLL	Dynamic linked library
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IE	Internet Explorer
IIS	Internet Information Service (MS)
IP	Internet Protocol
KB	kilobytes (10^3)
MIME	Multipurpose Internet Mail Extensions
MS	Microsoft
NIPC	National Infrastructure Protection Center
MAPI	Messaging Application Programming Interface
PDC	Primary Domain Controller
RAM	Random access memory
SP	Service Pack
TCP	Transmission Control Protocol
tftp	Trivial File Transfer Protocol