

1. Initial infection

** Email infection

- * Social engineering
 - Directly attach executable file with deceiving messages (Goner, Reezak, Love bug)
- * Email attachment of executable file with double extension (eq. abc.gif.exe) (W32/Sircam)
- * Automatic execution of Embedded MIME types (Nimda)
 - Use IE's vulnerability CA-2001-06

** Direct server compromise

- * Solaris sadmind buffer overflow (Sadmind/IIS)
- * Buffer overflow in IIS indexing service DLL (Code Red, Code Red II)

** Direct file transfer

- * Copy code to open shares and modify system files to get started (W32/Sircam)

2. Local activities and propagation

** Email address collection

- * Search .htm/.html files in user's web cache folder (Nimda)
- * From email messages retrieved via MAPI service (Nimda, Reezak)
- * Read all the "*.wab" files (Win32/Sircam)

** Email sending

- * Send emails with the payload every 10 days (Nimda)
- * Send emails with its own smtp client capability (Win32/Sircam)
- * Send emails using open relay servers (Win32/Sircam)

** Scanning

- * Scan and execute IIS Directory Traversal vulnerabilities VU#11677 and CA-2001-12 (Nimda)
- * Scan and execute IIS Unicode vulnerabilities VU#11677 (Sadmind/IIS)
- * Scan and execute IIS backdoors left by Code Red II IN-2001-9 (Nimda)
- * Scan and execute IIS backdoors left by admind/IIS CA-2001-11 (Nimda)
- * Scan and execute Solaris sadmind buffer overflows (Sadmind/IIS)
- * Scan and execute IIS index service buffer overflow to propagate (Code Red/Code Red II)

** File transferring

- * Using tftp (Nimda)
- * Direct copy via open shares (Nimda)
- * Use ICQ's file transfer feature (Goner)

** File modification and Trojan horses

- * Append javascript to the end of html files on IIS server to infect clients (Nimda)
- * Modify system ".dll" and ".exe" files to add Trojan horses (Nimda)
- * Modify "RICH20.DLL" to spread when "RTF" documents (Word, Wordpad) are opened (Nimda-A)
- * Deface web pages with IIS vulnerabilities (Sadmind/IIS)
- * Deface web pages if server language is English (Code Red)
- * Create a Trojan horse copy of "explorer.exe" and copy it to "C:\" and "D:\", which calls the

- real "explorer.exe" to mask its existence, and create a virtual mapping which exposes the "C:" and "D:" drives (Code Red II)
- * Modifies "system.ini" or "Win.ini" to get restarted after reboots (Nimda, SubSeven)
- * Delete system files (Goner, Reezak)

** System modification and backdoor installation

- * Open network sharing of hard disks (Nimda)
- * Create Administrator-equivalent accounts (Nimda)
- * Install a rootshell listening on TCP port 600 on Solaris (Sadmin/IIS)
- * Copy %SYSTEM%\cmd.exe to "root.exe" in the IIS "scripts" and "MSADC" folders (Code Red II)
- * Write registry to get restarted whenever the system reboots (Goner, Back Orifice, NetBus, SubSeven)
- * Append code execution command to the end of "autoexec.bat" (W32/Sircam)

** Other activities

- * On some days of each month carry out packet-flooding DOS attack (Code Red)
- * Sleeps forever if a copy (an atom) already exists (Code Red II)
- * If system language is Chinese(Taiwanese) or Chinese(PRC), spawn 600 threads and scan for 48 hours. Otherwise, spawn 300 threads and scan 24 hours (Code Red II)
- * Use IRC to transmit a victim host's IP (Back Orifice plug-in)
- * Retrieve cached, RAS, ICQ, etc. passwords (SubSeven)
- * Open a browser and go to a user-defined site (SubSeven)
- * Disable some keys on the keyboard (Reezak)

** Track/existence covering

- * Use a compression mechanism to avoid anti-virus detection (Nimda-C, Goner)