How secure are your Windows systems?

UA Security Awareness Day
November 5, 2004

Rusma Mulyadi
Paul Tate

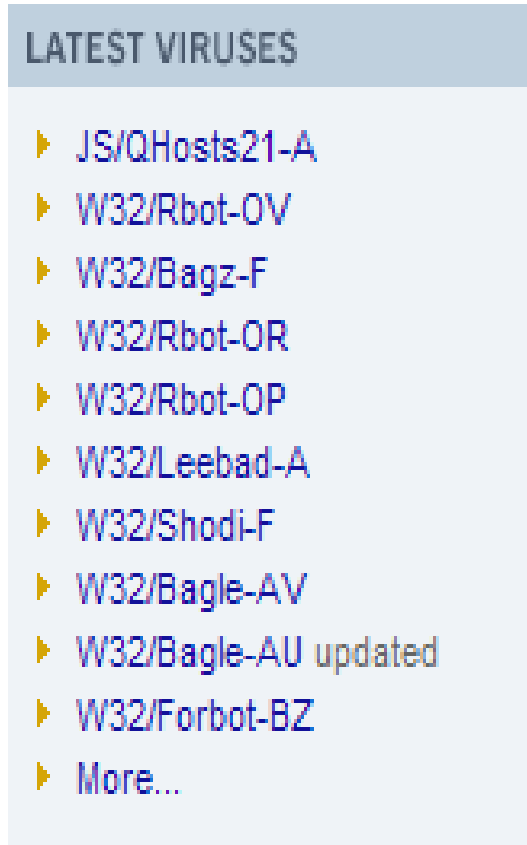
Agenda

- Sophos' 10 Latest Viruses
- Botnets
- Common worms propagation methods
- Network + Host based detections
- Manual removals*
- Defense-in-depth
- Questions + contact info
- References

Sophos' 10 Latest Viruses

- November 3rd, 2004
- (Ago|for|gt|phat|r|rx|sd)bot
- Email and P2P worms
- Infected machines since April'04:
  - Approx. 1800 unique hosts*

*multiple infections, only border NIDS



What is a botnet?

- Mostly from a slide by John Kristoff – NANOG32
- An army of compromised hosts (bots)
- Under a common command and control (c&c):
  - Commonly IRC-based
  - P2P – Phatbot
- The bot:
  - Servant code, exploit and attack tools
- The purpose:
  - DoS, id theft, keyloggers, phishing, spam
  - For fun and **profit**

Rbot Commands

<@pwnz> .findpass
<dark> [FINDPASS]: The Windows logon (Pid: <111>) information is: Domain: \\Windows, User: (Bill Gates/(no password)).

<@pwnz> .capture screen C:\Screenshot.jpg
<dark> [CAPTURE]: Screen capture saved to: C:\Screenshot.jpg.

- http://jayzafool.com/commands.html

Rbot Commands – Scans

advscan	Starts a scan using (check advscan.cpp) with on a delay of , for on If -a is specified, starts a scan using the A class on the bot. Likewise with -b. Using -r makes the rest of the ip become random. If a,b or r aren't specified, the [ip] must be in format: A.B.C.D. X can be used as one of the numbers, as it is evaluated as a random number.	<@pwnz> .advscan netbios 100 5 120 -b -r <dark> [SCAN]: Random Port Scan started on 192.168.x.x:139 with a delay of 5 seconds for 120 minutes using 100 threads.
scan	Starts a port scan at : with delays of .	<@pwnz> .scan 24.222.212.37 445 10 <dark> [SCAN]: Port scan started: 24.222.212.37:445 with delay: 10(ms).
scanstats	Returns various information about a scan. Returning how many exploits there has been found.	<@pwnz> .scanstats <dark> [SCAN]: Exploit Statistics: WebDav: 0, NetBios: 0, NTPass: 0, Dcom135: 0, Dcom445: 0, Dcom1025: 0, Dcom2: 0, MSSQL: 0, Beagle1: 0, Beagle2: 0, MyDoom: 0, lsass: 10, Optix: 0, UPNP: 0, NetDevil: 0, DameWare: 0, Kuang2: 0, Sub7: 0, Total: 0 in 0d 0h 0m.
scanstop	Stops whatever scans are in progress and kills the threads.	<@pwnz> .scanstop <dark> [SCAN]: Scan stopped. (11 thread(s) stopped.)

Rbot Commands – Attacks

ddos.stop	Stops whatever DDoS threads there are.	<@pwnz> .ddos.stop <dark> [DDoS] DDoS flood stopped. (1 thread(s) stopped)
ddos.syn ddos.ack ddos.random	Starts a DDoS (syn, ack, or random) on : for	<@pwnz> .ddos.random <dark> [DDoS]: Flooding: (24.222.212.37:337) for 120 seconds.
icmpflood	Starts a ICMP flood on for . If -r is present it spoofs the IP's.	<@pwnz> .icmpflood 24.222.212.37 120 -r <dark> [ICMP]: Flooding: (24.222.212.37) for 60 seconds.
pingflood	Sends to with sizes of and a delay of .	<@pwnz> .pingflood 24.222.212.37 120 1000 4096 100 <dark> [UDP]: Sending 1000 packets to: 24.222.212.37. Pack size: 4096, Delay: 100(ms).
pingstop	Stops a pingflood.	<@pwnz> .pingstop <dark> [PING] Ping flood stopped. (1 thread(s) stopped)
synflood	Synfloods : for seconds.	<@pwnz> .synflood 24.222.212.37 337 120 <dark> [SYN]: Flooding: (24.222.212.37:337) for 120 second
synstop	Stops a synflood.	<@pwnz> .pingstop <dark> [SYN]: Syn flood stopped. (1 thread(s) stopped.)
tcpflood	Methods can be: syn, ack or random. TCP floods : for seconds. If -r is specified, flood is spoofed.	<@pwnz> .tcpflood ack 24.222.212.37 337 120 -r <dark> [TCP]: Spoofed ack flooding: (24.222.212.37:337) for 120 seconds.
udpflood	UDPfloods :[port] (, all sizes of) with a second delay	<@pwnz> .udpflood 24.222.212.37 1000 4096 100 <dark> [UDP]: Sending 1000 packets to: 24.222.212.37. Pack size: 4096, Delay: 100(ms).
udpstop	Stops a UDP flood.	<@pwnz> .udpstop <dark> [UDP] UDP flood stopped. (1 thread(s) stopped)

What are the propagation methods?

- Vulnerable services
  - RPC-DCOM (MS04-012, MS03-039, MS03-026)
  - LSASS (MS04-011)
  - Web browsers (IE, Mozilla, etc.)
- Weak passwords (incl. MS-SQL)
- Emails: MyDoom, Beagle
- Peer-to-Peer

SANS Top 10 Windows Vuln. http://www.sans.org/top20

- W1 Web Servers & Services
- W2 Workstation Service
- W3 Windows Remote Access Services
- W4 Microsoft SQL Server (MSSQL)
- W5 Windows Authentication
- W6 Web Browsers
- W7 File-Sharing Applications
- W8 LSAS Exposures
- W9 Mail Client
- W10 Instant Messaging

Detections – Network-level

- Network-based IDS & RNA
  - HOST SYN SWEEP to TCP 80,**135**,139,**445**,1025,3127,6129...
  - Worm specific signatures
  - Abnormal FTP ports
- Network slowness reports – Packeteer
  - DoS launched by controlled bots
- Network audits – nmap, nessus, custom scripts
- Internal and external reports

Do these look familiar?

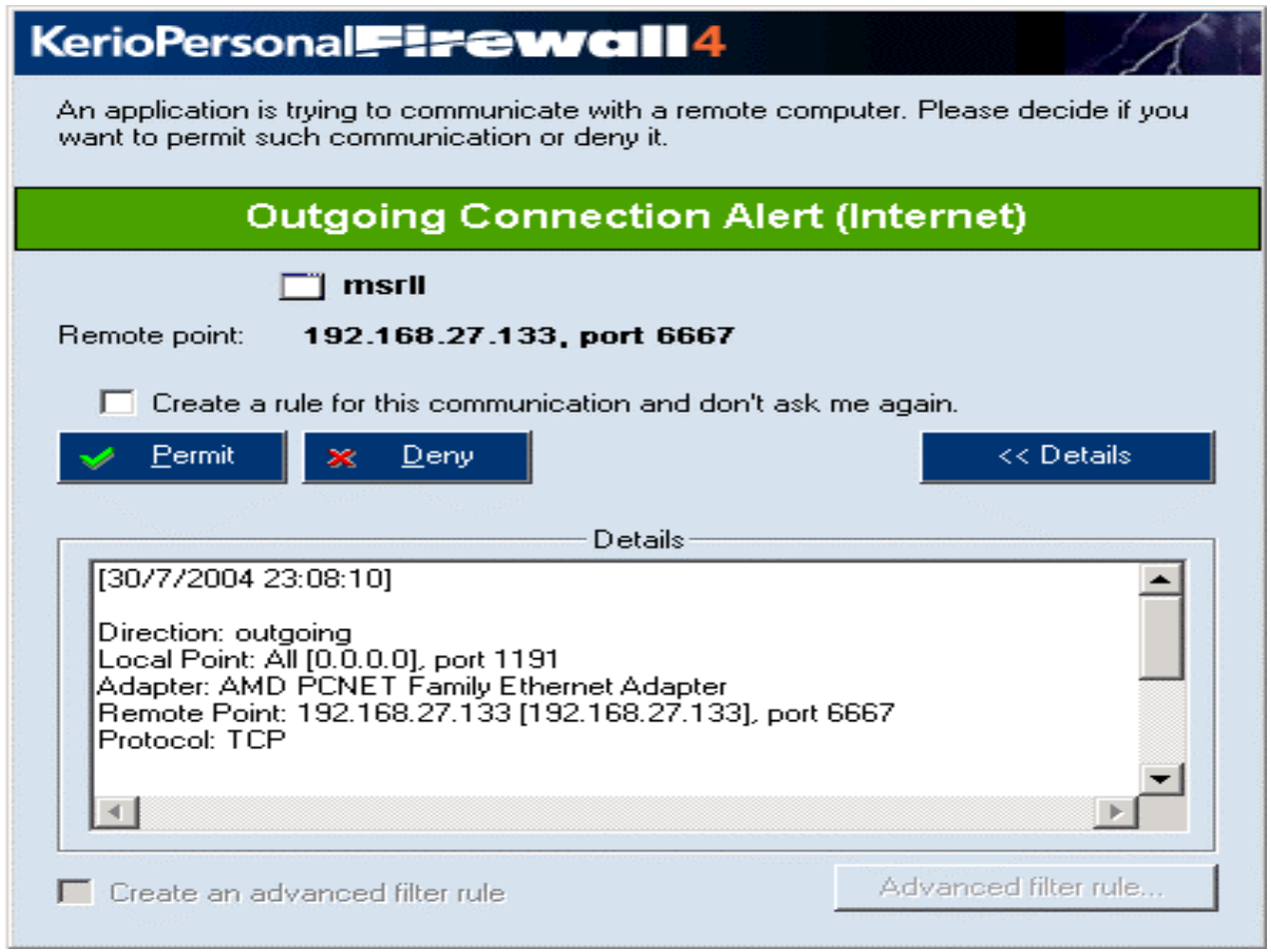
- Windows + TCP 113
  - USERID : UNIX : glniyvel
  - USERID : UNIX : ketz
- FTPd on abnormal ports
  - 220 StnyFtpd 0wns j0
  - 220 Serv-U FTP-Server v2.5i for WinSock ready…
  - 220 Serv-U FTP Server v4.0 for WinSock ready…
  - 220 Bot Server (Win32)

How about this?

Detections – Host-level

- Personal Firewalls alerts
- Anti-Virus software
- Adware/Spyware detection
  - Spybots Search & Destroy, Ad-Aware, HijakThis, BHODemon
- File integrity tools: md5sum
- Strange system behaviors

Personal FW – Outgoing alerts



Personal FW – Incoming alerts

Strange behaviors – new listening ports

```
C:\Tools>fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
1096  msrll          ->  113   TCP   C:\WINNT\system32\mfm\msrll.exe
420   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
8     System         ->  445   TCP
584   MSTask         ->  1025  TCP   C:\WINNT\system32\MSTask.exe
756   kpf4gui        ->  1026  TCP   C:\Program Files\Kerio\Personal Firewall 4\kpf4gui.exe
756   kpf4gui        ->  1028  TCP   C:\Program Files\Kerio\Personal Firewall 4\kpf4gui.exe
504   kpf4ss         ->  1030  TCP   C:\Program Files\Kerio\Personal Firewall 4\kpf4ss.exe
1000  kpf4gui        ->  1033  TCP   C:\Program Files\Kerio\Personal Firewall 4\kpf4gui.exe
1000  kpf4gui        ->  1035  TCP   C:\Program Files\Kerio\Personal Firewall 4\kpf4gui.exe
504   kpf4ss         ->  1037  TCP   C:\Program Files\Kerio\Personal Firewall 4\kpf4ss.exe
8     System         ->  1039  TCP
1096  msrll          ->  2200  TCP   C:\WINNT\system32\mfm\msrll.exe
504   kpf4ss         ->  44334 TCP   C:\Program Files\Kerio\Personal Firewall 4\kpf4ss.exe
504   kpf4ss         ->  44501 TCP   C:\Program Files\Kerio\Personal Firewall 4\kpf4ss.exe

8     System         ->  137   UDP
8     System         ->  138   UDP
8     System         ->  445   UDP
228   lsass          ->  500   UDP   C:\WINNT\system32\lsass.exe
756   kpf4gui        ->  1027  UDP   C:\Program Files\Kerio\Personal Firewall 4\kpf4gui.exe
756   kpf4gui        ->  1029  UDP   C:\Program Files\Kerio\Personal Firewall 4\kpf4gui.exe
1000  kpf4gui        ->  1034  UDP   C:\Program Files\Kerio\Personal Firewall 4\kpf4gui.exe
1000  kpf4gui        ->  1036  UDP   C:\Program Files\Kerio\Personal Firewall 4\kpf4gui.exe
228   lsass          ->  4500  UDP   C:\WINNT\system32\lsass.exe
504   kpf4ss         ->  44334 UDP   C:\Program Files\Kerio\Personal Firewall 4\kpf4ss.exe
```

Manual removal*

- Find the malicious process
  - Netstat: (Windows XP SP2)
    - -a: displays all connections and listening ports.
    - -b: includes executables
    - -v: more verbose (with –b)
    - -n: no address/port resolution
    - -o: displays PID so you can match it task manager
  - Fport: http://www.foundstone.com/
  - ActivePorts: http://www.ntutility.com/freeware
  - TaskInfo: http://www.iarsn.com/taskinfo.html

Manual removal...*

- Is it a legitimate service ports?
  - http://www.iana.org/assignments/port-numbers
  - http://www.dshield.org/port_report.php
  - http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html
- Is it a legitimate system files?
  - md5sum – http://www.etree.org/md5com.html
  - NIST Checksum DB – https://www.sirt.arizona.edu/checksumcheck/SearchbyFile.php

Manual removal...*

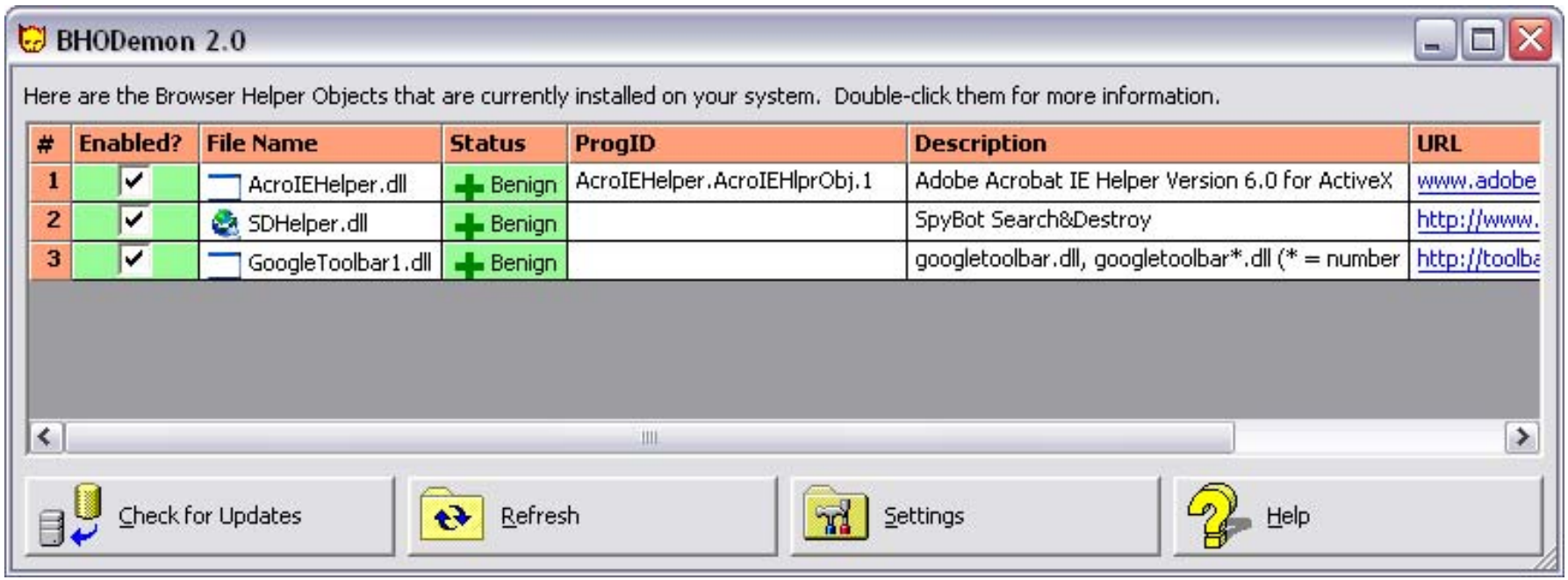
- Terminate the malicious process (e.g. pskill - http://www.sysinternals.com)
- Find & delete the malware:
  - Hidden files/folders
  - Hidden operating system files
- Clean up registry keys
- Check AV vendors' website for similar worm/virus variants
- Reboot and validate!
- Total SYSTEM REBUILD when necessary

Manual removal...* Places programs load from

- Start Menu – Startup Group
- Autorun.inf
- Registry
  - "Using Registry Editor incorrectly can cause serious, system-wide problems that may require you to re-install Windows to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved. Use this tool at your own risk."
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- Each user has a registry area named HKEY_USERS\[code number indicating user]\. For each user locate the entry:
  - HKU\[codenumber]\Software\Microsoft\Windows\CurrentVersion\Run\
  - HKU\[codenumber]\Software\Microsoft\Windows\CurrentVersion\RunServices\

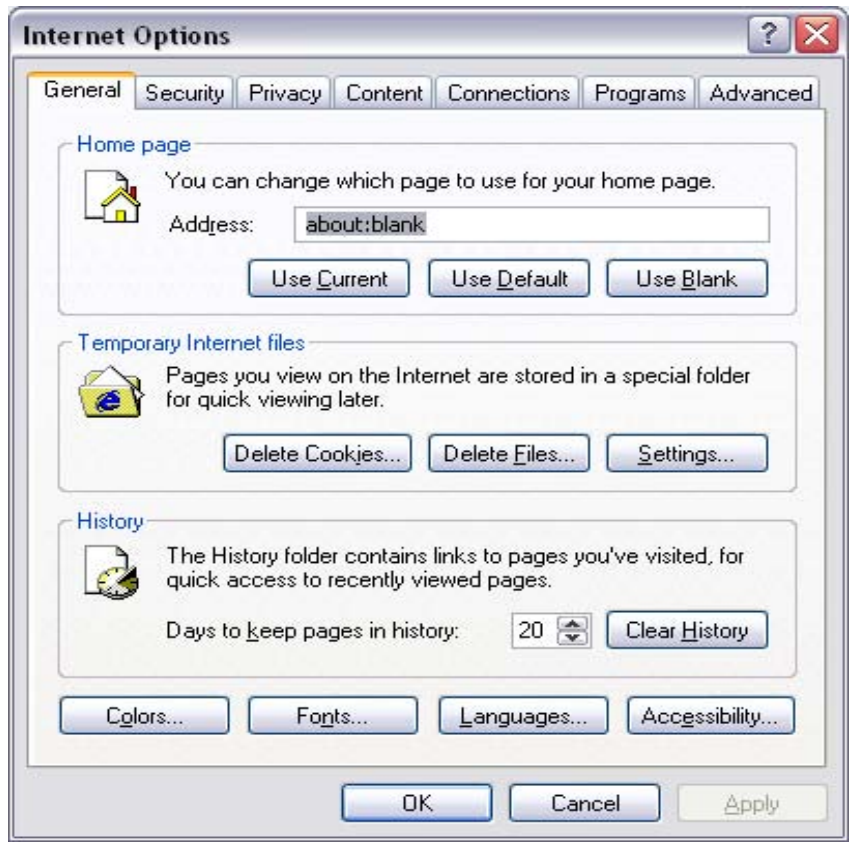
Manual removal...* Places programs load from...

- Browser Helper Objects
  - BHO demon



Manual removal...*
Places programs load from...

- Internet Explorer Helper Objects
  - Tools->Internet options
  - Click on the "Settings" button

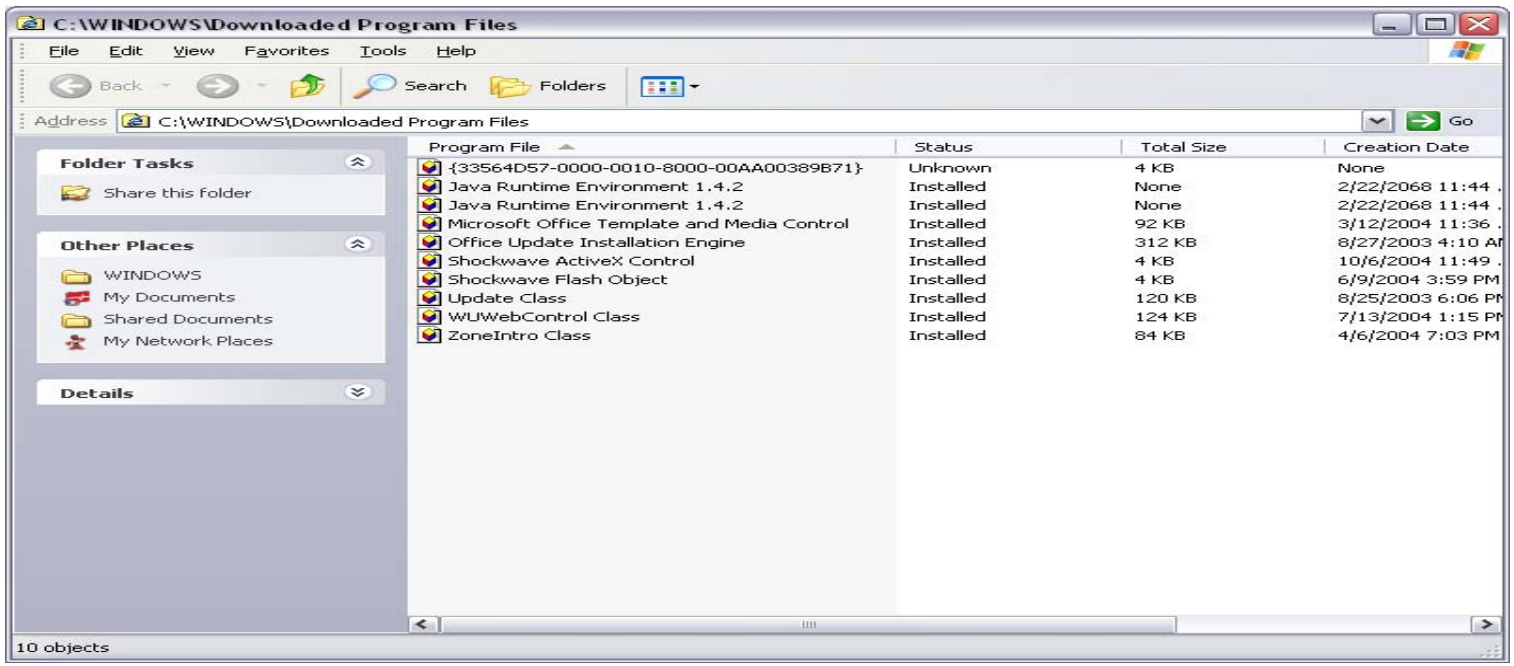


Manual removal...*
Places programs load from...

- Internet Explorer Helper Objects
  - Click on the "View Objects..." button

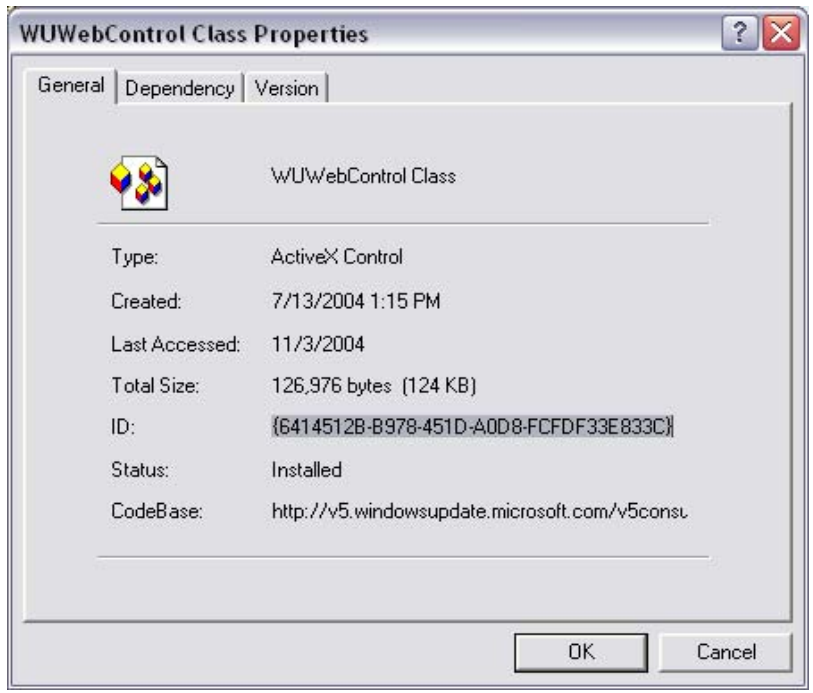
Manual removal...*
Places programs load from...

- Internet Explorer Helper Objects
  - Right Click on each object to see what it belongs to.



Manual removal...* Places programs load from...

- Internet Explorer Helper Objects
  - Code base sort of helps

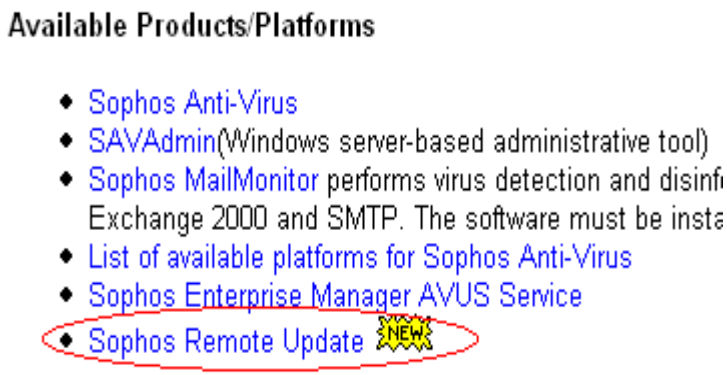


Defense-in-depth Network layer

- Router ACL & RACL
- Firewall & NIDS
- Vulnerability scanners
  - Nessus – www.nessus.org
  - SARA – http://www-arc.com/sara/
  - Nikto – web server scanner
    - http://www.cirt.net/code/nikto.shtml
  - Careful scans – consult/notify SIRT ☺

Defense-in-depth
Host layer

- Patch, patch, patch... ☺
- Host-based firewall – Kerio
- Host-based IDS and anomaly detection
- Anti Virus software – Sophos AV

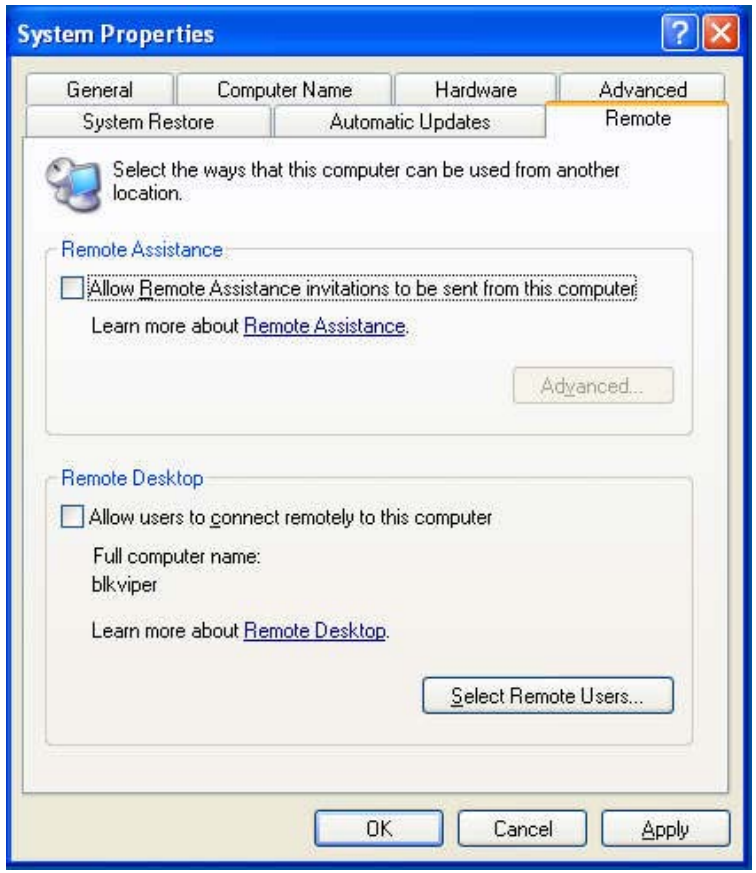


Defense-in-depth
Host layer

- Spyware/Adware detection tools
  - Spybots Search & Destroy, Ad-Aware, HijakThis, BHODemon
- Know your systems
- Backups
  - Make sure you test it!
  - In case you need it.

Knowing your systems

- Only run necessary services
  - Disable UPnP
  - Turn off Remote Assistance and Desktop Sharing



Knowing your systems...

- Understand ‘default’ configurations
  - Anonymous access – Null sessions
    - HKLM\SYSTEM\CurrentControlSet\Control\Lsa
    - Set “RestrictAnonymous” to 2
    - GPO
      - Disable “Network Access: Let Everyone permissions apply to anonymous users”
      - Enable “Network Access: Do not allow anonymous enumeration of SAM accounts and shares”
      - Disable “Allow anonymous SID/Name translation”
  - Default shares
    - HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
    - Add AutoShareServer –Dword value 0
  - Default passwords and user accounts
    - Blank passwords, unused accounts

Knowing your systems...

- Strong password policy & password audits
  - Always use NTLM2 when possible
  - Advance written permission before audits ☺
  - LC6, John the Ripper

Knowing your systems...

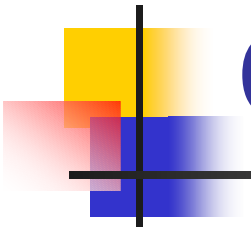
- Host-level audits
  - Written audit procedures are always GOOD
  - Checks for abnormal behaviors
  - Free command line tools + SMOP
  - Check your logs...
    - The Top 10 Log Entries that Show You've Been Hacked
      - http://loganalysis.org/news/tutorials/index.html

Knowing your systems... Host-level audits...

- Foundstone's Forensics Toolkits & fport http://www.foundstone.com/resources/freetools.htm
- Somarsoft Utilities – Dump(sec|evt|reg) http://www.somarsoft.com/
- PSTools - http://www.sysinternals.com/ntw2k/freeware/pstools.shtml
- Windows Resource Kits

Defense-in-depth
YOU-ARE-IT!

- Review your logs!! – did I just say it again?
- End-user education
  - http://security.arizona.edu/awareness.html
  - http://www.cert.org/homeusers/
- Policies and procedures
  - U of A Acceptable Use of Computers and Networks
    - http://security.arizona.edu/policies-guidelines.html
  - Departmental guides & policies
    - FSO - http://www.fso.arizona.edu/fso/computing/policies.asp
    - Rescomp - http://www.rescomp.arizona.edu/guides/aup.php
- Information sharing
  - SIRT-discuss + Netdiscuss
  - Send samples to AV vendors



Conclusions

- It’s a WILD network
- Layered of defenses
- YOU-ARE-IT!

Questions + contacts info

- Feedbacks?
- Rusma Mulyadi – rmulyadi@arizona.edu
- Paul Tate – ptate@email.arizona.edu
- SIRT Team – sirt@arizona.edu

References

- http://sophos.com
- http://www.merit.edu/~nanog/mtg-0410/pdf/kristoff.pdf
- http://jayzafool.com/commands.html
- http://www.lurhq.com/phatbot.html
- http://www.sans.org/top20

Useful resources

- https://www.sirt.arizona.edu/page.php?page=seclink
- https://www.sirt.arizona.edu/page.php?page=secOs
- http://security.arizona.edu/
- http://sitelicense.arizona.edu
- Spybots Search & Destroy: http://beam.to/spybotsd
- Ad-Aware: http://www.lavasoftusa.com/
- HijakThis: http://www.spywareinfo.com/~merijn
- BHODemon: http://www.definitivesolutions.com
- http://loganalysis.org/