

Dealing with an Infectious Computer Virus

Washington State
Department of Revenue
Information Services
Division

Washington State Department of Revenue

Content

- Scenario
- The attack
- Attempts and resolution
- Lessons learnt : what worked / key tools
- Lessons learnt : what to put in place
- Questions/Discussion

Scenario: Environment

- 2000+ Network Devices
 - 1500 Workstations
 - 600 Laptops
 - 200 x86 Microsoft Windows Servers
- Single Mainframe Server
- 14 field offices
- Cisco layer-2 and layer-3 devices
- Single hub star topology ethernet IP network

Scenario: Environment

- State inter-agency shared and trusted network
- Separate DMZ for web applications
- Payment initialization transmitted through SFTP to bank

Scenario: In-place protection

- Enterprise anti-virus software (eTrust)
- Patch management and deployment solution (Patchlink)
- Directory Services policy and standardized client configuration
- Agency Cisco PIX firewall behind a state-level firewall (proprietary, non-Cisco)

Scenario: The Application layer

- Electronic Filing – Microsoft .NET web application
- HP non-Stop relational database containing all taxpayer information
- Microsoft SQL database containing synchronized taxpayer information with payment indicator field

Scenario: T -48hr

- City-wide power outage
 - Affected offices within the city limits
 - Workstations and switches and local servers
 - No impact on DOR Data Center

Scenario: T -24hr

- Scheduled maintenance
 - Reorganizing several server racks
 - Some re-cabling
- Unscheduled maintenance
 - Resolving impacts from power outage

The Attack: Day 1

- It's a Monday
- Sporadic connectivity problems
- Sluggish network performance

The Attack: Day 1 (Impact)

- Assumption #1 – Residual problems from power outage
 - Attempted restarts
 - Client PC performance problem went away
- Assumption #2 – Scheduled maintenance issue
 - Troubleshoot cabling
- 3:30pm no more problems

The Attack: Day 2 (Impact)

- 9 AM – Extreme network slowdown
- Rampant connectivity problems
- Assumption #1 and #2 out the window

The Attack: Day 2 (Analysis)

- Layer 2 analysis
 - Network fluke
 - High bandwidth utilization
 - Identified “Top Talkers”
 - Switch monitoring
 - Sequential IP-IP within class (scanning)
 - High processor and memory utilization
 - Communication attempt on port 135 (Windows authentication port)

The Attack: Day 2 (Analysis continued)

- Layer 3 analysis
 - Router monitoring
 - Higher than normal processor and memory utilization, but less than layer 2 and not crippling
 - Outgoing communication attempt through IRC port to two external IP addresses
 - IP addresses registered to two different Texas ISPs

The Attack: Day 2 (Analysis continued)

- Layer 5 analysis
 - Desktop applications and processes
 - Physically quarantined desktops identified as scanners from the layer 2/3 analysis
 - Identified unknown/suspicious running processes

The Attack: Day 2 (Research)

- Identified probable strain of worm (obscure)
- Attempted manual step-by-step registry modifications to confirm fix
- Confirm latest anti-virus signature on infected PC
- Submitted worm binary to eTrust
- Submitted worm binary to major anti-virus entities (Mcafee, Norton)

The Attack: Day 2 (Research)

- See complete Virus capabilities

The Attack: Day 2 **(Indirect Consequences)**

- Network connectivity problems prevented communication between DMZ and payment tracking servers, resulting in resubmitting debit requests because field not updated.

The Attack: Day 2 **(Designing the resolution)**

- Design an automated comprehensive solution to:
 - Block communication to ISPs
 - Suspend programs/processes used by virus
 - Remove programs/processes
 - Remove registry entries inserted by virus
- Develop a deployment strategy

The Attack: Day 2

(Blocking communication to ISPs)

- Blocked communication to ISPs at the Cisco Layer 3 router
 - For added precaution, disabled all network traffic in/out of the agency
- Attempt contact with ISPs (failed)
- Contacted authorities (WSP and FBI)
- Initiated state-level communication to give other agencies a heads-up

The Attack: Day 2

(Stop Virus program/processes)

- Wrote a quick batch program that will use kill.exe to terminate a running process and to delete the files
- Test

The Attack: Day 2

(Remove registry entries)

- Developed a quick C++ program to backup and then modify registry
- Test
- Include in the batch program

The Attack: Day 2

(Additional unknowns)

- Possible that patches would resolve re-infection of a sterilized PC.
- Patches were not completely up to date, so to be safe, all patches that would not cause new/unforseen problems were identified
- Prepare collection of patches to be deployed

The Attack: Day 2 **(Develop Complete Solution)**

- Created a startup (not login) policy that:
 - Removes rights to execute the main virus executable file: MDNZ32.EXE
 - runs the batch program.
 - Kill mdnz32 process if running, delete files, modify registry
- Patch Deployment
 - Push patches (except XP SP2)

The Attack: Day 2 **(Deployment Challenges)**

- It is approaching 5pm on Tuesday
- People leaving offices; Many PCs turned off all day and will be so through the night
- Solution will not get to PCs that were turned off

The Attack: Day 2 **(More Deployment challenges)**

- Insufficient bandwidth to activate policy
- Insufficient bandwidth to push patches
- If automation failed, IS needed to visit EVERY PC/laptop. (Morale issue)

The Attack: Day 2 **(Final Deployment Game Plan)**

- Contact every field office now to:
 - have every PC/laptop kept/turned on
 - Ask for a designated contact person able to be activated sometime during night
- Terminate all field office network connections to the hub

The Attack: Day 2

(Final Deployment Game Plan continued)

- Create auto-run CD with solution
- Send non-network IT engineer to Olympia-sites, and larger sites within reasonable driving distance with CD
- Identify sequence of offices

The Attack: Day 2/3

(The cleaning process)

- Contact target field office
- Have contact person restart all PCs/laptops
 - Leave PCs/laptops on
- Re-establish network connection to field office
- Deploy patch collection to local server
- Random sample of PCs to establish quality of solution
- Start patch deployment from local server to local clients
- Network monitoring
- Disable connection to field office

The Attack: Day 3 (Residual Cleanup Effort)

- Constant network monitoring for trend:
 - Sequential IP-IP communication on port 135 (scanning)
 - Identify and fix
- Coordinate a staggered reintroduction of laptops not previously cleaned on Day 2 back into the network
- If network traffic from a field office starts to get out of hand (very conservative), disconnect office immediately and address.
- DOR was 99.9% operational by 8am Day 3

The Media

- All three major networks scheduled interviews
- Two of the three camped outside the building and pointed lights and cameras through the windows till at least after the 11pm news
- Interviewed other agencies in an attempt to baseline their recovery efforts to DOR's
- Attempted to get committed resolution time
- Spin factor

Lesson learnt: What were the critical tools/knowledge

- The support, understanding, and the help of clients/customers (communication)
- Ability to carry out layer 2/3/5 network analysis
- Ability to control network communication status
- Ability to apply broad sweeping network policies
- Ability to modify registry
- Ability to push patches

Lessons learnt: What we did differently

- First time contact with FBI
 - Provide law enforcement and investigatory expertise
 - Crossed local jurisdiction of State Patrol
 - Last but not least, the most important thing...

Lessons learnt: New implementations

- Close ports internal to network
- Disable PC-to-PC peer communication at layer 2 device (switch)
 - Need an organized IP addressing scheme to be able to identify server IPs versus client PC IPs
- A much more aggressive patch testing and deployment schedule

Lessons learnt: Other options considered

- Intruder Detection Systems (\$\$\$\$\$)
 - Purchased Cisco SecurityWorks agent (CSA) for 750 laptops and 100 servers. In the process of deployment
- Network traffic pattern/trend analysis (\$\$\$)
 - Considering NetIQ
- PC with dual Operating System capability (\$\$)

Thank you

- Other business division impacts (time permitting)
- Questions/Discussion
- Contact Information:

Julian J. Soh
360-586-9826

julians@dor.wa.gov

Colin Corbin
360-586-7984

colinc@dor.wa.gov

James Petit
jamesp@dor.wa.gov