

Enterprise Computer Incident Response for Rapid Replicating Threats

Christopher Vera

CISSP, GCFA, SCSA, CCNA, MCSE

Brief History

- Six years in Information Security
- Stood up
 - ◆ CIRT
 - ◆ Vulnerability Management
 - ◆ Security Awareness programs
 - ◆ for Fortune 500 & international companies
- Reduced average per incident costs from \$1M to \$15K

The Agenda

- Define Rapid Replicating Threat
- Compare: Vuln Management vs CIRT
- CIRT for Rapid Response
 - ◆ The four R's for rapidCIRT
- Final Thoughts

Rapid Replicating Threats

- Malicious code that spreads quickly through a network
 - ◆ Worms
 - ◆ Blended Threats
 - ◆ Botnets
- Most include tools: remote control, keylogging, others

Comparisons

Vulnerability Management

- Proactive
- Strategic
- Seeks to prevent damage
- Topic for another day

CIRT

- Reactive
- Tactical
- Seeks to minimize damage
- VM hammer
- Today's topic

CIRT 101

- The Four R's of Incident Response

- ◆ Readiness

- ◆ Recognition

- ◆ Response

- ◆ Recovery



65% of your effort

Readiness

Elements of RapidCIRT

- Authority
- Roles & Responsibilities
- Procedures
- Tools
- Awareness/Training/Practice

Authority

- Include the right players
 - ◆ Network
 - ◆ Server
 - ◆ Desktop
 - ◆ Security
 - ◆ Helpdesk
- Documented charter
 - ◆ Derived from company policy
 - ◆ In a nutshell: Minimize damage
- “ToMBin” Total Management Buy-in

Roles & Responsibilities

- Roles & responsibilities are always assigned as part of Readiness.
- This presentation will discuss R&R in Response.

Career Question

“At what point do you disconnect your entire company from the Internet during a rapid replicating computer incident?”

Procedures

- Procedures outline what to do when certain criteria are met
 - ◆ Steps: What do I do?
 - ◆ Criteria: When do I do it?
 - ◆ Escalation: Who do I tell?
- Detailed
 - ◆ Got checklists?
- Not unnecessarily detailed
 - ◆ Minimize “point here, click ok” detail
- Answers the Career Question

Readiness Tools

- Asset management
 - ◆ System purpose & criticality
 - ◆ System owner
 - ◆ Known vulnerabilities
- Collaboration
 - ◆ Internal E-mail
 - ◆ Secure Instant Messaging
 - ◆ Secure web conferencing
 - ◆ Phone (something out-of-band)

Training & Practice

- Training
 - ◆ rCIRT member role functions
 - ◆ Incident recognition
 - ◆ Evidence collection
- Practice
 - ◆ Tabletop exercises
 - ◆ Planned Drills

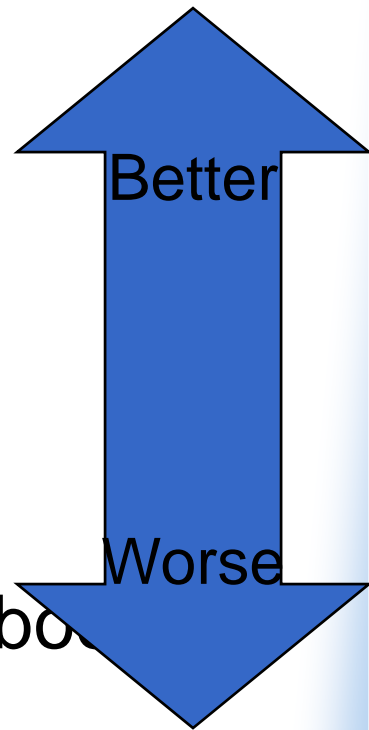
Recognition

Recognition

- Most of the time
 - ◆ Follow up on false positives & tune them out
 - ◆ Eyes on the dashboards
 - ◆ Finger on the “big red button”
- Weeks & weeks of boredom followed by several hours of intense excitement

Recognition Tools

- How will you see it coming?
 - ◆ Event correlation
 - ◆ Intrusion detection/prevention
 - ◆ Honey pots
 - ◆ Router ARP tables
 - ◆ Anti-virus alerts
 - ◆ E-mail server slows to a crawl
 - ◆ Users complain their desktops keep rebooting



Security Awareness

- Security-aware users provide a human Intrusion Detection System
- The best security awareness provides some Intrusion Prevention
- Provides marketing for rCIRT
- Implement a Security Awareness Program

Response

Roles & Responsibilities

- rCIRT Lead
- Research
- Monitors
- Sweepers
- Cleaners
- Communications

rCIRT Lead

- Executive decision maker when procedures fail & management is unavailable
- Organizes overall effort
- Ensures processes & procedures are followed
- Keeps “big picture” focus
- Keeps management informed of status
- Maintains “meeting minutes” of incident in progress
- Drafts final reports

Research

- Gathers information about the threat
 - ◆ From infected systems
 - ◆ From security websites
 - ◆ From security vendors
 - Anti-virus
 - IDS/IPS

Monitors

- Watches for incoming events
- Reports suspicious & infected systems to rCIRT
- Updates recognition tools with signatures
- Updates scorecard

Sweepers

- Use scorecard to remove threats
- Remove the threat from production network
 - ◆ Quarantine network
 - ◆ Shut down the switch port
- Sometimes shares the monitor role if the rCIRT is using more sophisticated tools

Cleaners

- Removes malicious code or reimages victim system
 - ◆ Local system touch
 - ◆ Quarantine network touch
- Apply necessary patches & AV signatures to prevent reinfection

Communications

- Contact impacted users & business units
- Not very glamorous, but critical
 - ◆ Prevents infected users from troubleshooting & putting infected host back on network
 - ◆ Lets users know when they can expect their system back

Communicate

- Keep management informed
- Keep users informed
- Define Service Level Objectives in procedures
 - ◆ What to tell them
 - ◆ When & how often to tell them
- Makes special requests easier

Response Tools

- Quarantine network
 - ◆ Easier for Research to investigate
 - ◆ Less expensive for Cleaners to fix victims
 - ◆ Harder for victims that require data recovery
- Vulnerability Scanners
 - ◆ Find vulnerable & infected systems quickly
 - ◆ VM hammer
- Automated Software Delivery
 - ◆ Patch deployment
 - ◆ System reimaging
 - ◆ AV signatures

Recovery

Restore or Preserve?

- The charter says “minimize damage”
 - ◆ Translation: Get back to production ASAP
 - ◆ Preserving evidence takes time
- Gathering evidence has its own rewards
 - ◆ Was data compromised?
 - ◆ Dormant botnet?
 - ◆ Possible prosecution?
 - ◆ Possible insurance benefits?

The Compromise

- Accurate recordkeeping
- Quick system snapshots
 - ◆ Volatile data (memory)
 - ◆ File system
 - ◆ Windows registry
- Similar to a house break-in
 - ◆ Thieves may never be caught but
 - ◆ Strong documentation allows you to recover stolen property

Keep It Quick

- Save the binary analysis for CSI
 - ◆ Collect a sample for your AV vendor
- Perfect a reimaging process
 - ◆ Quick OS, app & data restore keeps users productive
 - ◆ Productive users keep managers happy

Keep It Clean

- Patch cleaned hosts before putting back on production network
- Install latest AV signatures
- Software firewalls are still difficult to manage in an enterprise

Reporting Inside

- Root Cause Analysis
 - ◆ Fix the problem, not the blame
 - ◆ Well, rarely the blame
 - ◆ Keep the scope enterprise-wide
 - Vulnerabilities exploited
 - Vulnerability time window
 - Attack surfaces of impacted hosts
 - Recurring points of entry

Reporting Outside

- Interested entities
 - ◆ CERT
 - ◆ FBI
 - ◆ Media - no comment!
- Consult your company decision makers first!
- Roll into procedures
- California rCIRTs: It may not be up to you to interpret SB1386

Gather Metrics

- Metrics prove its working
- Metrics justify future business cases
- Some sample metrics
 - ◆ Cost of incident (devise your formula)
 - ◆ Number of incidents annually
 - ◆ Time between vulnerability announcement & first infection
 - ◆ Exploited vulnerability
 - ◆ Repeat offenders from last incident

Final Thoughts

- Automate it
 - ◆ Computers respond faster than humans
 - ◆ Automate repetitive tasks
- Never over-automate it
 - ◆ Rapid replicating threats can be emulated
 - ◆ Keep humans on the trigger
- My old vision
 - ◆ A rapid replicating incident should be like a computer game the rCIRT can't wait to play
- My new vision
 - ◆ A rapid replicating incident should be a boring affair that is resolved quickly & effortlessly

Don't Panic!

Resources

- CERT
 - ◆ <http://www.cert.org>
- CIRT - Framework and Models
 - ◆ <http://www.securitydocs.com/library/2964>
- NIST
 - ◆ <http://www.nist.gov>
- SANS
 - ◆ <http://www.sans.org>
- Forum of IR & Security Teams
 - ◆ <http://www.first.org/>