Incident Response in the age of APT

Adnan Baykal
Director
Multi-State Information Sharing and Analysis Center
Computer Emergency Response Team (CERT)

What is an Incident

- This needs to be defined for each organization
- In general it can be described as an unexpected/ anomalous event in an information system or network
  - Unauthorized access or attempts
  - Denial of Service
  - Virus Infection
  - Improper use of organization's resources
  - Website Compromise/Defacement
  - Espionage

Key to Incident Response

- Remain Calm
  - This reduces overall stress levels
  - If not, communication become difficult
  - It helps avoid making critical errors
- Take Notes
  - Log everything you can
  - If you are going too fast to take note, then slow down.
  - Record all your actions
    - With date and timestamps
    - Audi recorder can help

Incident Response

- it is a six step process
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons Learned

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

- Sun Tzu

Preparation

- Know your systems
  - Network Maps
  - Firewalls
    - Regularly audit firewall rules
  - IDS/IPS devices
    - do you have one?
    - Host/Network Based?
  - Patch Levels
  - Anti-virus programs
    - Are they up-to-date?
  - Software Inventory
  - Logging capabilities
    - What are you logging?
    - What can you log during an incident?

Preparation

- Know your strengths/weaknesses
  - What kind of capabilities do you have?
    - Malware Analysis
    - Computer Forensics
    - Network Forensics
    - Firewall administration
    - Network administration
    - Policy Auditing
    - Backups
  - Do you have backups for key personnel?
    - What if your Firewall admin is disgruntled
      - Can you still monitor the network or make firewall change?
  - Do you have the right tools
    - Are they up to date?
    - Are your staff properly trained/certified?

Preparation

- Know your contacts
  - Incident Response Team
    - HR
    - Counsel
    - Network Admin
    - Server/Desktop Support
    - PR
    - Physical Security
  - AV vendors
  - IDS/IPS vendors
  - Other product vendors
  - CSCIC
  - State Police
  - FBI

Preparation

- Have a plan, know your plans
  - For each types of incident, have plans to
    - Identify
    - Contain
    - Eradicate
    - Recovery
  - Practice, practice, practice

Identification

- Key Indicators for Incident
  - System Crashes
  - New User Accounts
  - Increase network utilization
  - New files with strange names
  - Unexplained web page changes (defacements)
  - Account lockouts
  - Other anomalies

Identification

- Classification
  - Unauthorized Access
  - Malicious Code
  - Web Defacement
  - Hardware/Software Failure
  - Denial of Service
  - ……..
- What is the Scope of the incident
  - Business Impact Assessment
  - Single or multiple systems
  - Single or all operating systems
    - Maybe affecting only windows 2000 servers
  - Single or multiple IP addresses

The general who wins the battle makes many calculations in his temple before the battle is fought. The general who loses makes but few calculations beforehand.

-Sun Tzu

Containment

- This is a crucial step in the response
- Goal is to limit the extent of the incident
- Need to follow predetermined steps and procedures
- Need to make critical decisions
  - Shutdown a system
  - Disconnect from network
  - Disable services
  - Monitor network

Containment

- Do not alter any system until complete back up can be taken
  - Preferably bit-by-bit forensic image of the computer
  - Live memory dump
    - Do this before unplugging the network cable and
    - Before turning of any services
    - Before modifying the firewall
  - Acquire Logs from all available and applicable systems and devices

Containment

- Do NOT LOG ON TO COMPROMISED SYSTEMS as ADMINS
  - This is specially true if dealing with malware incidents
    - Malware can spread to other devices using the admin credentials
    - Malware can steal admin password
- Build a containment plan
  - Use the data from the identification phase
  - It should have verifiable objectives
- Determine the risk of continuing operation
  - This is an executive decision

Containment

- Some containment strategies are
  - Null Routing
  - Change passwords
  - Remove accounts used by attacker
  - Kill suspicious processes running on the system
  - Break/alter trust relationships

Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.

-Sun Tzu

Eradication

- Once incident is contained, we have to remove the incident causing agents from the environment
- Determine the cause of the incident
  - Perform computer forensics
  - Malware analysis
  - Network Forensics
  - Log Analysis
- Analyze and correlate anything and everything you can

Eradication

- Remove or Rebuild
  - If the incident involves a rootkit, rebuild is strongly recommended
    - how do you know if you can trust the backup media
- What if it is a zero day
  - Change of architecture necessary?
- Strengthen defenses
  - Improve detection and protection methods
  - Egress and ingress filtering
  - Look for backdoors on other systems
- Perform vulnerability analysis on the network

Recovery

- Bring the systems back online… or not…
  - System owners call
  - Make a recommendation in writing
  - If possible, bring the systems back online during off hours
    - Eases the close monitoring of the devices
  - Validation of the restored systems
    - Is it working the way it is suppose to?
    - Work with the system owners to verify that system(s) is working properly
  - Monitor the affected systems/networks closely for unusual activity.

Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win.

-Sun Tzu

Lessons Learned

- Goal is to document what happened and improve capabilities
- Document
  - Need to write a final report
    - This needs to be done right after the recovery phase
    - Everyone in the response team and involved parties need to review and comment
- Lessons learned meeting
  - Discussion should focus on
    - The final report
    - Identification of what failed and how it can be improved
    - **Not** blaming individual