WORM SCENARIO INCIDENT RESPONSE

Efundola Osibamowo

December 22, 2024

CONTENTS

INCIDENT RESPONSE FOR THE WORM AND DDOS AGENT ATTACK

INCIDENT OVERVIEW

A new worm is spreading via email attachments and through opened Windows file shares. Once it infects a system, it installs a Distributed Denial of Service (DDoS) agent. The worm had spread quickly—before the organization's antivirus (AV) software received updated signatures. The organization's response to this worm infection hinges on quick identification of infected hosts, strong containment measures, and preemptive steps to limit further infections before antivirus signatures become available.

The goal of this Incident Response Report is therefore to contain the infection from what seems to be a Zero-Day attack, eradicate the worm, recover infected systems, and implement measures to prevent re-infection and future outbreaks.

INCIDENT RESPONSE (IR) STEPS

1. PREPARATION

Goals: Since the organization is in the middle of an incident, this step may be brief, but it's critical to confirm IR readiness to ensure that the IR team is organized, understands roles and responsibilities, and has the tools needed.

- **Confirm the IR Team:** Confirm all the roles i.e. Lead IR Coordinator, Communication Liaison, Technical Analysts, Forensic Specialists, etc.
- **Communication Channels:** Set up secure communication channels (via a secure chat platform or out-of-band communication) for the IR team to coordinate.
- **Policies and Procedures:** Review the organization's incident response policy and ensure everyone understands escalation paths and documentation requirements.

2. IDENTIFICATION AND ANALYSIS

Goals: Identify all infected systems, determine the worm's indicators of compromise (IOCs), and understand the scope and spread.

- **Indicator Development:**
  - Perform quick forensic analysis on at least one infected host. Extract IOCs such as file hashes, filenames, registry entries, or suspicious processes.
  - Correlate logs from firewalls, IDS/IPS, and SIEM solutions to identify affected hosts, known malicious IPs, domains, or command-and-control (C2) communications.
- **Host Identification Techniques:**
  - **Endpoint Analysis:** Check endpoint detection logs and antivirus logs (even without updated signatures) to detect behavioral anomalies (e.g., processes replicating themselves or creating unauthorized network connections), and endpoint management system reports.
  - **Network Traffic Analysis:** Use network monitoring tools or IDS/IPS solutions to identify anomalous traffic patterns caused by the worm (e.g. repeated attempts to access Windows shares or communications with external DDoS command-and-control servers contacting suspicious C2 domains) and lateral movement patterns (excessive SMB traffic).

- **Email Gateway and Email Logs:** Review email gateway logs to identify accounts or systems that received the malicious attachment, opened it or forwarded the infected emails. Those endpoints are high-risk for initial infection.
- **Scanning Tools:** Use network scanning tools to detect known worm artifacts. If a IOC-based scanning is possible, push it out via the endpoint management tool.
- **Custom Scripts:**
  Develop scripts to search for specific Indicators of Compromise (IoCs), such as known file hashes, processes, or registry changes made by the worm.

- **Containment Validation:**
  - Determine how many hosts are infected.
  - Prioritize critical systems first—servers supporting essential business operations.

3. CONTAINMENT

Phase I Goals: Immediate actions to prevent the worm from entering the organization before updated AV signatures are released.

- **Email Gateway Filters:**
  - Quarantine all inbound email attachments containing executable content (e.g., .exe, .scr, .vbs), if temporarily blocking them is not feasible
  - Implement content filtering on the email system to halt the delivery of any identified malicious attachments still in the queue.
- **Email Security Measures:**
  - Employ sandboxing to detonate and analyze attachments in a controlled environment before delivering them to recipients.
  - **User Communication:**
    - Send out a company-wide alert to employees: **Do not open suspicious attachments**.
    - Provide guidance on how to recognize malicious emails and instruct them to report it to the IR team or help desk.
- **Endpoint Controls**:
  - If possible, enable host-based firewalls to restrict inbound SMB connections on workstations and servers.
- **Network Controls**
  - Update firewalls and Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) to block connections to and from known or suspected command-and-control (C2) servers or to shut down system resources, as required.
- **Threat Intelligence:**
  - Monitor real-time threat intelligence feeds for early warnings of new malware campaigns.
  - Apply available security advisories to preemptively configure defenses.

Phase II Goals: To contain the worm's propagation and prevent the worm from spreading before antivirus signatures are released.

Since antivirus signatures are unavailable, prevention measures would focus on reducing the attack surface and leveraging existing tools:

- **Network Isolation/Segmentation:**
  - Quarantine infected hosts by removing them from the network by using Network Access Control (NAC) or manually disconnecting network cables, if safe to do so.

    - Use VLANs or firewalls to segment infected subnets and isolate them from other parts of the network to prevent lateral movement.
    - Temporarily disable or heavily restrict protocols like Server Message Block (SMB) traffic, used for file sharing, where possible.
    - Isolation of High-Risk Systems: Proactively disconnect critical or high-risk systems (e.g., servers hosting sensitive data) from the network or for a longer-term measure, set up alternative secure environments for ongoing business operations - to reduce exposure to initial infection or lateral movement until the threat is mitigated.
- **Disable Windows File Sharing**:
    - Organization-wide, disable or limit access to open Windows shares temporarily via group policy or network configuration until the infection is resolved.
    - For critical shared resources, restrict access to authenticated users or specific systems.
- **Disabling Email Features:**
    - Block outgoing emails containing attachments from infected systems, if feasible.
- **Implement Temporary Access Controls**:
    - Restrict non-essential ports (e.g., port 445 for SMB traffic) at the firewall and host-based firewalls.
- **Monitor and Block Malicious Communication**:
    - Use IDS/IPS systems to block connections from known or suspected command-and-control (C2) servers.
    - Employ rate-limiting to minimize DDoS agent impact.

4. ERADICATION

Goals: The organization should attempt to remove the worm and DDoS agent from all infected hosts as comprehensive patching of all vulnerable machines is critical.

- Identify the vulnerability: Once the worm's method of propagation is understood (e.g., exploiting an SMB vulnerability or relying on a known email client bug), apply vendor-supplied patches.
- Prioritize Critical Systems: Focus on patching high-risk systems first, such as domain controllers, file servers, or systems housing sensitive data.
- Use the organization's patch management system to push critical OS and application patches to all machines.
- **Antivirus Updates:**
    - As soon as the AV vendor releases new signatures, test them on a non-critical infected machine.
    - Once validated, push the updated signatures enterprise-wide via your endpoint management system.
    - Perform a full scan on all endpoints, starting with those known or suspected to be infected.
- **Manual Removal (If needed):**
    - If some endpoints are heavily infected or if the AV cannot remove the worm automatically, consider a manual cleanup. This may involve:
        - Booting into Safe Mode or using a bootable antivirus scanner.
        - Removing malicious registry entries and files identified during the IOC gathering phase.
        - Reimaging machines that are severely compromised, if this is faster and more reliable.
- Apply patches in a phased manner, starting with critical servers and high-risk endpoints, and then moving to the broader workstation population.
- **Rollback Plan:** Ensure there is a contingency for systems that break post-patch (e.g., verify the patch in a test environment before widespread deployment).
- **Risk Management:**
    - Assess the feasibility of patching systems in real time based on criticality and risk level.

- For systems that cannot be patched immediately, apply compensating controls such as virtual patching and endpoint hardening measures, such as disabling unneeded vulnerable services or applying restrictive permissions, until patching is complete.

5. RECOVERY

Goals: Restore systems to normal operation and ensure that no backdoors or residual worm components remain.

- **System Restoration:**
  - Restore critical systems from clean, verified backups if necessary.
  - Reconnect previously isolated hosts to the network once verified clean.
  - Reset credentials if the worm may have harvested them.
  - Restore necessary SMB shares slowly and with strict controls. Consider requiring user authentication for previously open shares and implement least-privilege permissions.
  - Review email gateway rules and revert them once it is confirmed the threat is mitigated but maintain stricter attachment filtering policies going forward.
- **Validate DDoS Removal**:
  - Verify that no residual DDoS agents remain by monitoring network traffic for anomalies.
- **Monitoring:**
  - Enhance monitoring for abnormal network traffic, suspicious emails, and SMB usage.
  - Use IDS/IPS, SIEM, and endpoint logs to detect any lingering infection attempts.
- **Communication:**
  - **Internal Reporting**:
    - Notify leadership and IT teams about the infection and steps taken.
  - **User Notification**:
    - Alert employees to avoid opening suspicious emails and attachments.
    - Provide guidance on identifying and reporting phishing attempts.

6. LESSONS LEARNED

Goals: After resolving the incident, document the entire incident and conduct a post-incident review with all stakeholders to improve future defenses.

- **Root Cause Analysis:**
  - Determine how the worm entered initially—was it a lack of attachment filtering, a missed patch, or user error (social engineering)?
  - Identify what enabled its lateral spread—open shares with weak permissions, no network segmentation?
- **Policy and Control Improvements:**
  - Update the email security policy to block or closely scrutinize risky file types for faster detection of email-based malware.
  - Improve endpoint security controls (e.g., HIDS/HIPS, EDR) to detect unusual file or network behavior.
  - Strengthen Windows share security Enforce stricter access controls and network segmentation to reduce worm spread potential.
  - Consider implementing application whitelisting and.
  - Update the incident response plan and playbooks based on lessons learned.
  - Provide enhanced user training or tools to address gaps identified during the incident.
- **Documentation:**
  - Write a thorough incident report covering the timeline, actions taken, and lessons learned.
  - Present findings to leadership and relevant stakeholders to justify security improvements and potential increased budget for advanced detection and prevention tools.
  - Share sanitized findings with external partners or threat intelligence networks (if appropriate).