Homeland Security

Best Practices for Continuity of Operations (Handling Destructive Malware)

by National Protections and Programs Directorate
Department of Homeland Security

June 26, 2018

Overview

While infrequent in occurrence, destructive malware[1] can present a direct threat to an organization's daily operations impacting the availability of critical assets and data. Organizations should increase vigilance and evaluate their capabilities encompassing planning, preparation, detection, and response for such an event. This publication is focused on the threat of enterprise-scale distributed propagation methods for malware and provides recommended guidance and considerations for an organization to address as part of their network architecture, security baseline, continuous monitoring, and Incident Response practices. This paper provides recommendations and strategies that organizations can employ to actively prepare for and respond to a disruptive event such as destructive malware. These recommendations have also been posted on the US-CERT web site and are available at https://www.us-cert.gov/ncas.tips/ST13-003.

Potential Distribution Vectors

Destructive malware has the capability to target a large scope of systems and can potentially execute across multiple systems throughout a network. As a result, it is important for an organization to assess its environment for atypical channels for potential malware delivery and/or propagation throughout its systems. Systems to assess include:

- Enterprise Applications-particularly those that have the capability to directly interface with and impact multiple hosts and endpoints. Common examples include:
    - Patch Management Systems
    - Asset Management Systems
    - Remote Assistance Software (typically utilized by the corporate Help Desk)
    - Antivirus (AV)
    - Systems assigned to system and network administrative personnel
    - Centralized Backup Servers
    - Centralized File Shares

While not applicable to malware specifically, threat actors could compromise additional resources to impact the availability of critical data and applications. Common examples include:

- Centralized storage device
    - Potential Risk-direct access to partitions and data warehouses;
- Network Devices
    - Potential Risk-capability in inject false routes within the routing table, delete specific routes from the routing table, or remove/modify configuration attributes, which could isolate or degrade availability of critical network resources.

Best Practices and Planning Strategies

Common strategies can be followed to strengthen an organization's resilience against destructive malware. Targeted assessment and enforcement of best practices should be employed for enterprise components susceptible to destructive malware.

- Communication Flow
    - Ensure proper network segmentation[2].
    - Ensure that network-based access control lists (ACLs) are configured to permit server-to-host and host-to-host connectivity via the minimum scope of ports and protocols and that directional flows for connectivity are represented appropriately.

---

[1] https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B, web site last accessed January 22, 2015.

[2] http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/De..., web site last accessed January 22, 2015.

        - Communication flow paths should be fully defined, documented, and authorized
    - Increase awareness of systems that can be utilized as a gateway to pivot (lateral movement) or directly connect to additional endpoints throughout the enterprise.
        - Ensure that these systems are contained within restrictive VLANs, with additional segmentation and network access-controls.
    - Ensure the centralized network and storage devices' management interfaces are resident on restrictive VLANs.
        - Layered access-control, and
        - Device-level access control enforcement, restricting access from only predefined VLANs and trusted IP ranges.
- Access Control
    - For Enterprise systems that can directly interface with multiple endpoints:
        - Require two factor authentication for interactive logons.
        - Ensure that authorized users are mapped to a specific subset of enterprise personnel.
            - If possible, the "Everyone," "Domain Users," or the "Authenticated Users" groups should not be permitted the capability to directly access or authenticate to these systems.
        - Ensure that unique domain accounts are used and documented for each Enterprise application service.
            - Context of permission assigned to these accounts should be fully documented and configured based on the concept of least privilege.
            - Provides an enterprise with the capability to track and monitor specific actions correlating to an application's assigned service account.
        - If possible, do not grant a service account with local or interactive logon permissions.
            - Service accounts should be explicitly denied permissions to access network shares and critical data locations.
        - Accounts that are used to authenticate to centralized enterprise application servers or devices should not contain elevated permissions on downstream systems and resources throughout the enterprise
    - Continuously review centralized file share access-control lists and assigned permission.
        - Restrict Write/Modify/Full Control permissions when possible.
- Monitoring
    - Audit and review security logs for anomalous references to enterprise-level administrative (privileged) and service accounts.
        - Failed logon attempts,
        - File share access, and
        - Interactive logons via a remote session.
    - Review network flow data for signs of anomalous activity.
        - Connections utilizing ports that do not correlate to the standard communication flow with an application,
        - Activity correlating to port scanning or enumeration, and
        - Repeated connections using ports that can be utilized for command and control purposes.
    - Ensure that network devices log and audit all configuration changes.
        - Continually review network device configurations and rule sets, to ensure

communication flows are restricted to the authorized subset of rules.

- File Distribution
    - When deploying patches or AV signatures throughout and enterprise, stage the distributions to include a specific grouping of systems (staggered over a predefined time period).
        - This action can minimize the overall impact in the event that an enterprise patch management or AV system is leveraged as a distribution vector for a malicious payload.
    - Monitor and assess the integrity of patches and AV signatures, which are distributed throughout the enterprise.
        - Ensure updates are received only from trusted sources.
        - Perform file and data integrity checks.
        - Monitor and audit as related to the data that is distributed from an enterprise application.
- System and Application Hardening
    - Ensure that the underlying Operating System (OS) and dependencies (ex: IIS, Apache, SQL) supporting an application are configured and hardened based on industry standard best practice recommendations[3]. Implement application-level security controls based on best practice guidance provided by the vendor. Common recommendations include:
        - Utilize role-based access control.
        - Prevent end-user capabilities to bypass application-level security controls,
        - Example: disabling AV on a local workstation.
        - Disable unnecessary or un-utilized features or packages.
        - Implement robust application logging and auditing.
    - Thoroughly test and implement vendor patches in a timely manner.

Recovery and Reconstitution Planning

A Business Impact Analysis (BIA)[4] is a key component of contingency planning and preparation. The overall output of a BIA will provide an organization with two key components (as related to critical mission/business operations):

- Characterization and classification of system components, and
- Interdependences.

Based on the identification of an organization's mission critical assets (and their associated interdependencies), in the event that an organization is impacted by a potentially destructive condition, recovery, and reconstitution efforts should be considered.

To plan for this scenario, an organization should address the availability and accessibility for the following resources (and should include the scope of these items within Incident Response exercises and scenarios):

- Comprehensive inventory of all mission critical systems and applications:
    - Versioning information,
    - System/application dependencies,
    - System partitioning/storage configuration and connectivity, and
    - Asset Owners/Points of Contact.
- Comprehensive inventory of all mission critical systems and applications:

[3] http://web.nvd.nist.gov/view/ncp/repository, web site last accessed January 22, 2015.

[4] http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_err..., web site last accessed January 22, 2015.

    - Versioning information,
    - System/application dependencies,
    - System partitioning/storage configuration and connectivity, and
    - Asset Owners/Points of Contact.
- Contact information for all essential personnel within the organization,
- Secure communications channel for recovery teams,
- Contact information for external organizational-dependent resources:
    - Communication Providers,
    - Vendors (hardware/software), and
    - Outreach partners/External Stakeholders
- Service Contract Numbers for engaging vendor support,
- Organizational Procurement Points of Contact,
- ISO/image files for baseline restoration of critical systems and applications:
    - Operating Systems installation media,
    - Service Packs/Patches,
    - Firmware, and
    - Application software installation packages.
- Licensing/activation keys for Operating Systems (Oss) and dependent applications,
- Enterprise Network Topology and Architecture diagrams,
- System and application documentation,
- Hard copies of operational checklists and playbooks,
- System and application configuration backup files,
- Data backup files (full/differential),
- System and application security baseline and hardening checklists/guidelines, and
- System and application integrity test and acceptance checklist.

Containment

In the event that an organization observes a large-scale outbreak that may be reflective of a destructive malware attack[5], in accordance with Incident Response best practices, the immediate focus should be to contain the outbreak and reduce the scope of additional systems that could be further impacted. Strategies a containment include:

- Determining a vector common to all systems experiencing anomalous behavior (or having been rendered unavailable) from which a malicious payload could have been delivered:
    - Centralized Enterprise Application,
    - Centralized File Share (for which the identified systems were mapped or had access),
    - Privileged User Account common to the identified systems,
    - Network Segment or Boundary, and
    - Common DNS Server for name resolution.
- Based on the determination of a likely distribution vector, additional mitigation controls can be enforced to further minimize impact:
    - Implement network-based access-control lists to deny the identified application(s) the capability to directly communication with additional systems,
        - Provides an immediate capability to isolate and sandbox specific systems or resources.
    - Implement null network routes for specific IP addresses (or IP ranges) from which the

[5] http://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B, web site last accessed January 22, 2015.

payload may be distributed,
    - An organization's internal DNS can also be leveraged for this task just as a null pointer record could be added within DNS zone for an identified server or application.
  - Readily disable access for suspected user or service account(s), and
  - For suspect file shares (which may be hosting the infection vector), remove access or disable the share path from being accessed by additional systems.

Additional Recommended Practices

NCCIC/ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT web page at: http://ics-cert.us-cert.gov/content/recommended-practices. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies, that is available for download from the ICS-CERT web site (http://ics-cert.us-cert.gov/).

Organizations may wish to read the Defensive Best Practices for Destructive Malware, Version 1.0, MIT-001R-2015, dated January 16, 2015, available at:
https://www.nsa.gov/ia/_files/factsheets/Defending_Against_Destructive_Malware.pdf

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in email messages.
2. Refer to Recognizing and Avoiding Email Scams[6] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[7] for more information on social engineering attacks.

---

[6] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, web site last accessed January 22, 2015.

[7] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, web site last accessed January 22, 2015.

Contacting and Reporting to ICS-CERT

ICS-CERT recommends that organizations report cyber incidents for tracking and correlation. This enables ICS-CERT to create a big picture view of malicious cyber activity and report back to the community to further situational awareness.

ICS-CERT can also provide assistance to companies with the analysis of hard drives, malware, log files, and other artifacts. Indicators derived from analysis of that data are sanitized of company attribution and provided back to the industrial control system community for detection. Reporting of incidents enables more actionable information to flow to the industrial control system community and ultimately, raises awareness of cyber threats and helps to secure CIKR.

For any questions related to this report, please contact ICS-CERT at:

ICS-CERT Operations Center
Toll Free: 1-877-776-7585
International: 1-208-526-0900
Email: ics-cert@hq.dhs.gov

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov/

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://www.us-cert.gov/forms/feedback.