National Cybersecurity and Communications Integration Center

05 November 2013

Planning and Recommended Guidance – Destructive Malware

Overview

As related to malware which may exhibit a potentially destructive capability[1], organizations should increase vigilance and evaluate their capabilities encompassing planning, preparation, detection, and response for such an event. Destructive malware presents a direct threat to an organization's daily operations, directly impacting the availability of critical assets and data. In addition, the response required for such an event can be extremely resource intensive.

This publication provides recommended guidance and considerations for an organization to address as part of their network architecture, security baseline, continuous monitoring, and Incident Response practices.

While specific indicators and modules related to destructive malware may evolve over time, it is critical that an organization assess their capability to actively prepare for and respond to such an event.

Potential Distribution Vectors

As actual methods for initial compromise may vary[2], this publication is focused on the threat of enterprise-scale distributed propagation methods for malware, the potential impact to critical resources within an organization, and countermeasures for mitigation.

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 that an organization assess their environment for atypical channels from which malware could potentially be delivered and/or propagate throughout the environment.

- Enterprise Applications – particularly those which 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)
    - Anti-Virus
    - 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 devices
    - Potential Risk – direct access to partitions and data warehouses
- Network devices
    - Potential Risk – capability to 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. As related to enterprise components which could be leveraged to mass distribute a malicious payload throughout the enterprise, targeted assessments and enforcement of best practices should be considered.

Communication Flow

- Ensure proper network segmentation[3]
- 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.
    - Communication flow paths should be fully defined, documented, and authorized
- Increase awareness of systems which 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 that centralized network and storage devices' management interfaces are resident on restrictive VLANs
    - Layered access-control
    - Device-level access-control enforcement – restricting access from only pre-defined VLANs and trusted IP ranges

Access Control

- For Enterprise systems which 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 utilized and documented for each Enterprise application service
        - Context of permissions assigned to these accounts should be fully documented and configured based upon 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 which are utilized 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 permissions
    - 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
    - Interactive logons via a remote session
- Review network flow data for signs of anomalous activity
    - Connections utilizing ports which do not correlate to the standard communication flow associated with an application
    - Activity correlating to port scanning or enumeration
    - Repeated connections utilizing ports which 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 that communication flows are restricted to the authorized subset of rules

File Distribution

- When deploying patches or AV signatures throughout an enterprise, stage the distributions to include a specific grouping of systems (staggered over a pre-defined 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 upon industry-standard best practice recommendations[4]
- Implement application-level security controls based upon 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 Antivirus on a local workstation
    - Disable un-necessary 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)[5] 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
- Interdependencies

Based upon 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
    - Asset Owners / Points of Contact
- Comprehensive inventory of all mission critical systems and applications
    - Versioning information
    - System / application dependencies
    - System partitioning/ storage configuration and connectivity
    - 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)
    - 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 System installation media
    - Service Packs / Patches
    - Firmware
    - Application software installation packages
- Licensing/activation keys for Operating Systems (OS) 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
- System and application integrity test and acceptance checklists

Containment

In the event that an organization observes a large-scale outbreak that may be reflective of a destructive malware attack[6], in accordance with Incident Response best practices, the immediate focus should be to contain the outbreak, and reduce the scope of additional systems which could be further impacted.

Strategies for 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
    - Common DNS Server for name resolution

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

As related to incident response and incident handling[7], organizations are reminded to:

- Report the incident to US-CERT and/or ICS-CERT for tracking and correlation purposes[8,9]
- Preserve forensic data for use in internal investigation of the incident or for possible law enforcement purposes[10]

ICS-CERT Contact

For questions or to report an incident impacting critical infrastructure, please contact ICS-CERT.

ICS-CERT Operations Center
(877) 776-7585
ics-cert@dhs.gov

For additional information concerning best practices, alerts and advisories, visit: www.ics-cert.org

US-CERT Contact

For general inquiries or to report an incident, please contact US-CERT.

US-CERT Operations Center
(888) 282-0870
soc@us-cert.gov | nccic@us-cert.gov

For more information about general threats or to subscribe to the National Cyber Awareness System, visit www.us-cert.gov

References

[1] http://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B-0
[2] http://www.us-cert.gov/security-publications
[3] http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf
[4] http://web.nvd.nist.gov/view/ncp/repository
[5] http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
[6] http://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B-0
[7] http://ics-cert.us-cert.gov/sites/default/files/DHS_CyberSecurity_CSSP-Incident_Handling-v10.pdf
[8] http://www.us-cert.gov/contact-us
[9] http://ics-cert.us-cert.gov/
[10] http://ics-cert.us-cert.gov/sites/default/files/Incident_Handling_Brochure_Nov_2010.pdf