



THREAT BULLETINS

Joint Cybersecurity Advisory: Destructive Malware Targeting Organizations in Ukraine



TLP:WHITE

Feb 28, 2022

On February 26, 2022, the United States Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released a joint cybersecurity advisory (CSA), AA22-057A, discussing the destructive malware deployed by threat actors against Ukraine organizations to destroy computer systems and render them inoperable prior to Russia invading Ukraine.

On January 15, 2022, the Microsoft Threat Intelligence Center (MSTIC) disclosed that malware, known as WhisperGate, was being used to target organizations in Ukraine. According to Microsoft, WhisperGate is intended to be destructive and is designed to render targeted devices inoperable.

On February 23, 2022, several cybersecurity researchers disclosed that malware known as HermeticWiper was being used against

organizations in Ukraine. According to SentinelLabs, the malware targets Windows devices, manipulating the master boot record, which results in subsequent boot failure.

Destructive malware can present a direct threat to an organization's daily operations, impacting the availability of critical assets and data. Further disruptive cyberattacks against organizations in Ukraine are likely to occur and may unintentionally spill over to organizations in other countries. Organizations should increase vigilance and evaluate their capabilities encompassing planning, preparation, detection, and response for such an event.

Health-ISAC is releasing this intelligence report for your increased geopolitical and security awareness. This joint Cybersecurity Advisory (CSA) provides information on WhisperGate and HermeticWiper malware as well as open-source indicators of compromise (IOCs) for organizations to detect and prevent the malware. Additionally, this joint CSA provides recommended guidance and considerations for organizations to address as part of network architecture, security baseline, continuous monitoring, and incident response practices.

Indicators of Compromise have been entered into Health-ISAC's automated sharing platform for those members ingesting automated threat indicators. For posterity, the full PDF report is attached to this alert, and can also be accessed [here](#).

Threat actors have deployed destructive malware, including both WhisperGate and HermeticWiper, against organizations in Ukraine to destroy computer systems and render them inoperable. Listed below are high-level summaries of campaigns employing the malware. CISA recommends organizations review the resources listed below for more in-depth analysis and see the Mitigation section for best practices on handling destructive malware.

On January 15, 2022, Microsoft announced the identification of a sophisticated malware operation targeting multiple organizations in Ukraine. The malware, known as WhisperGate, has two stages that corrupts a system's master boot record, displays a fake ransomware note, and encrypts files based on certain file extensions. Although a ransomware message is displayed during the attack, Microsoft highlighted that the targeted data is destroyed, and is not recoverable even if a ransom is paid. For additional information on Microsoft's

blog regarding destructive malware targeting Ukrainian organizations, please see the report [here](#).

On February 23, 2022, cybersecurity researchers disclosed that malware known as HermeticWiper was being used against organizations in Ukraine. According to SentinelLabs, the malware targets Windows devices, manipulating the master boot record and resulting in subsequent boot failure. HermeticWiper was discovered to have similarities to the earlier WhisperGate attacks against Ukraine in which the wiper was disguised as ransomware, according to Broadcom.

Reference(s)

[cisa](#), [Microsoft](#), [Sentinel One](#), [cisa](#), [cisa](#)

Recommendations

Best Practices for Handling Destructive Malware

As previously noted above, destructive malware 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 section is focused on the threat of malware using enterprise-scale distributed propagation methods 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.

CISA and the FBI urge all organizations to implement the following recommendations to increase their cyber resilience against this threat.

Potential Distribution Vectors

Destructive malware may use popular communication tools to spread, including worms sent through email and instant messages, Trojan horses dropped from websites, and virus-infected files downloaded from peer-to-peer connections. Malware seeks to exploit existing vulnerabilities on systems for quiet and easy access.

The malware has the capability to target a large scope of systems and can execute across multiple systems throughout a network. As a result, it is important for organizations to assess their environment for atypical channels for malware delivery and/or propagation throughout their 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 used by the corporate help desk)
- Antivirus (AV) software
- Systems assigned to system and network administrative personnel
- Centralized backup servers
- Centralized file shares

While not only applicable to malware, 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, remove/modify, configuration attributes, or destroy firmware or system binaries—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.
- 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.
 - Communications flow paths should be fully defined, documented, and authorized.
- Increase awareness of systems that can be used as a gateway to pivot (lateral movement) or directly connect to additional endpoints throughout the enterprise.
 - Ensure that these systems are contained within restrictive Virtual Local Area Networks (VLANs), with additional segmentation and network access controls.
- Ensure that centralized network and storage devices' management interfaces reside on restrictive VLANs.
 - Layered access control, and
 - Device-level access control enforcement – restricting access from only pre-defined VLANs and trusted IP ranges.

Access Control

- For enterprise systems that can directly interface with multiple endpoints:
 - Require multifactor 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 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 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 ACLs 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, including:
 - Connections using ports that do not correlate to the standard communications flow associated with an application
 - Activity correlating to port scanning or enumeration
 - Repeated connections using ports that can be used 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 communications 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 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 that 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 robust vulnerability management and patching practices are in place.
 - CISA maintains a living catalog of known exploited vulnerabilities that carry significant risk to federal agencies as well as public and private sectors entities. In addition to thoroughly testing and implementing vendor patches in a timely—and, if possible, automated— manner, organizations should ensure patching of the vulnerabilities CISA includes in this catalog.
- Ensure that the underlying operating system (OS) and dependencies (e.g., Internet Information Services [IIS], Apache, Structured Query Language [SQL]) supporting an application are configured and hardened based upon industry-standard best practice recommendations. Implement application-level security controls based on best practice guidance provided by the vendor. Common recommendations include:
 - Use role-based access control
 - Prevent end-user capabilities to bypass application-level security controls
 - For example, do not allow users to disable AV on local workstations.
 - Remove, or disable unnecessary or unused features or packages
 - Implement robust application logging and auditing.

Recovery and Reconstitution Planning

A business impact analysis (BIA) 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
- 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 destructive malware, 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
- 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
- Optical disc image (ISO)/image files for baseline restoration of critical systems and applications:
 - OS installation media
 - Service packs/patches
 - Firmware
 - Application software installation packages.
- Licensing/activation keys for 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, and
- System and application integrity test and acceptance checklists.

Incident Response

Victims of a destructive malware attacks should immediately focus on containment to reduce the scope of affected systems. 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, and
 - Common Domain Name System (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 ACLs 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, and
 - Be prepared to, if necessary, reset all passwords and tickets within directories (e.g., changing golden/silver tickets).

Sources

[CISA AA22-057A: Destructive Malware Targeting Organizations in Ukraine](#)

- See Attached

Alert ID a7975b7b

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

[View Alert](#)

Tags HermeticWiper, WhisperGate, Russian APT, CISA Advisory, CISA Alert, FBI Alert, FBI-LIR, CISA, Russia, FBI, Ukraine, Russian

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

CISA CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

FBI The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts may be identified at www.fbi.gov/contact-us/field. Contact CyWatch by telephone at 855-292-3937 or by email at CyWatch@fbi.gov.

Download Health-ISAC's Information Sharing App.



For more update and alerts, visit: <https://health-isac.cyware.com>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.

Powered by [Cyware](#)