America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

Update: Destructive Malware Targeting Organizations in Ukraine

Last Revised: April 28, 2022 **Alert Code:** AA22-057A

Summary

Actions to Take Today:

- Set antivirus and antimalware programs to conduct regular scans.
- Enable strong spam filters to prevent phishing emails from reaching end users.
- Filter network traffic.
- Update software.
- Require multifactor authentication.

(Updated April 28, 2022) This advisory has been updated to include additional Indicators of Compromise (IOCs) for WhisperGate and technical details for HermeticWiper, IsaacWiper, HermeticWizard, and CaddyWiper destructive malware, all of which have been deployed against Ukraine since January 2022. Additional IOCs associated with WhisperGate are in the Appendix, and specific malware analysis reports (MAR) are hyperlinked below.

- Refer to MAR-10375867.r1.v1 for technical details on HermeticWiper. </ncas/analysis-reports/ar22-115a>
- Refer to MAR-10376640.r1.v1 for technical details on IsaacWiper and HermeticWizard. </ncas/analysis-reports/ar22-115b>
- Refer to MAR-10376640.r2.v1 for technical details on CaddyWiper. </ncas/analysis-reports/ar22-115c>

(end of update)

Leading up to Russia's unprovoked attack against Ukraine <https://www.cisa.gov/shields-up>, threat actors deployed destructive malware against organizations in Ukraine to destroy computer systems and render them inoperable.

- 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 <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>, WhisperGate is intended to be destructive and is designed render targeted devices inoperable.
- On February 23, 2022, several cybersecurity researchers disclosed that malware known as HermeticWiper <https://twitter.com/esetresearch/status/1496581903205511181> was being used against organizations in Ukraine. According to SentinelLabs <https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/>, 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.

This joint Cybersecurity Advisory (CSA) between the Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) 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.

Download the Joint Cybersecurity Advisory: Update: Destructive Malware Targeting Organizations in Ukraine (pdf, 559kb) </sites/default/files/publications/aa22-057a_destructive_malware_targeting_organizations_in_ukraine.pdf>.
Click here </sites/default/files/publications/aa22-057a.stix.xml> for STIX.

Technical Details

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. **Note:** 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. See Microsoft's blog on Destructive malware targeting Ukrainian organizations <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/> for more information and see the IOCs in table 1.

Table 1: IOCs associated with WhisperGate

Name	File Category	File Hash	Source
WhisperGate	stage1.exe	a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 <https://www.virustotal.com/gui/file/a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92>	Microsoft MSTIC <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>
WhisperGate	stage2.exe	dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78 <https://www.virustotal.com/gui/file/dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78>	Microsoft MSTIC <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>

(Updated April 28, 2022) *See Appendix: Additional IOCs associated with WhisperGate.*

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. **Note:** according to Broadcom Software, "[HermeticWiper] has some

similarities to the earlier WhisperGate wiper attacks against Ukraine, where the wiper was disguised as ransomware." See the following resources for more information and see the IOCs in table 2 below.

- ESET Research Tweet: Breaking. #ESETResearch discovered a new data wiper malware used in Ukraine today. ESET telemetry shows that it was installed on hundreds of machines in the country <https://twitter.com/esetresearch/status/1496581903205511181>.
- SentinelLabs: HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine <https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/>
- Broadcom Software's Symantec Threat Hunter Team: Ukraine: Disk-wiping Attacks Precede Russian Invasion <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia>

Table 2: IOCs associated with HermeticWiper

Name	File Category	File Hash	Source
Win32/KillDisk.NCV	Trojan	912342F1C840A42F6B74132F8A7C4FFE7D40FB7761B25D11392172E587D8DA3045812A66C3385451	ESET research
HermeticWiper	Win32 EXE	912342f1c840a42f6b74132f8a7c4ffe7d40fb77	SentinelLabs <https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/>

Name	File Category	File Hash	Source
HermeticWiper	Win32 EXE	61b25d11392172e587d8da3045812a66c3385451	SentinelLabs <https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/>
RCDATA_DRV_X64	ms-compressed	a952e288a1ead66490b3275a807f52e5	SentinelLabs <https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/>
RCDATA_DRV_X86	ms-compressed	231b3385ac17e41c5bb1b1fcb59599c4	SentinelLabs <https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/>
RCDATA_DRV_XP_X64	ms-compressed	095a1678021b034903c85dd5acb447ad	SentinelLabs <https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/>
RCDATA_DRV_XP_X86	ms-compressed	eb845b7a16ed82bd248e395d9852f467	SentinelLabs <https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/>

Name	File Category	File Hash	Source
Trojan.Killdisk	Trojan.Killdisk	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591	Symantec Threat Hunter Team <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia>
Trojan.Killdisk	Trojan.Killdisk	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da	Symantec Threat Hunter Team <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia>
Trojan.Killdisk	Trojan.Killdisk	a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e	Symantec Threat Hunter Team <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia>

Name	File Category	File Hash	Source
Ransomware	Trojan.Killdisk	4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382	Symantec Threat Hunter Team <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia>

Mitigations

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, and
  - 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, and
  - 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, and
  - 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, and
  - 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 <https://cisa.gov/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, and
  - Implement robust application logging and auditing.

Recovery and Reconstitution Planning

A business impact analysis (BIA) <https://www.ready.gov/business-impact-analysis> 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, 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,
- Optical disc image (ISO)/image files for baseline restoration of critical systems and applications:
  - OS installation media,
  - Service packs/patches,
  - Firmware, and
  - 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).

As related to incident response and incident handling, organizations are encouraged to report incidents to the FBI and CISA (see the Contact section below) and to preserve forensic data for use in internal investigation of the incident or for possible law enforcement purposes. See Technical Approaches to Uncovering and Remediating Malicious Activity <https://www.cisa.gov/uscert/ncas/alerts/aa20-245a> for more information.

Contact Information

Organizations can also report anomalous cyber activity and/or cyber incidents 24/7 to SayCISA@cisa.dhs.gov or by calling 1-844-Say-CISA (1-844-729-2472) and/or to the FBI via your local FBI field office <https://www.fbi.gov/contact-us/field-offices> or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

Resources

- Joint CSA: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure <https://www.cisa.gov/uscert/ncas/alerts/aa22-011a>
- Joint CSA: NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems <https://www.cisa.gov/uscert/ncas/alerts/aa20-205a>
- Joint CSA: Ongoing Cyber Threats to U.S. Water and Wastewater Systems <https://www.cisa.gov/uscert/ncas/alerts/aa21-287a>
- CISA and MS-ISAC: Joint Ransomware Guide <https://www.cisa.gov/sites/default/files/publications/cisa_ms-isac_ransomware%20guide_s508c.pdf>
- CISA webpage: Russia Cyber Threat Overview and Advisories <https://www.cisa.gov/uscert/russia>
- NIST: Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events <https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond>
- NIST: Data Integrity: Recovering from Ransomware and Other Destructive Events <https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/recover>
- CISA Cyber hygiene services <https://www.cisa.gov/cyber-hygiene-services>: CISA offers a range of no-cost services to help critical infrastructure organizations assess, identify and reduce their exposure to threats, including ransomware. By requesting and leveraging these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

Updated April 28, 2022:

Appendix: Additional IOCS Associated with WhisperGate

The hashes in Table 3 contain malicious binaries, droppers, and macros linked to WhisperGate cyber actors activity. The binaries are predominantly `.Net` and are obfuscated. Obfuscation varies; some of the binaries contain multiple layers of obfuscation. Analysis identified multiple uses of string reversal, character replacement, base64 encoding, and packing. Additionally, the malicious binaries contain multiple defenses including VM checks, sandbox detection and evasion, and anti-debugging techniques. Finally, the sleep command was used in varying lengths via PowerShell to obfuscate execution on a victim's network.

All Microsoft `.doc` files contain a malicious macro that is base64 encoded. Upon enabling the macro, a PowerShell script runs a sleep command and then downloads a file from an external site. The script connects to the external website via HTTP to download an executable. Upon download, the executable is saved to `C:\Users\Public\Documents\` filepath on the victim host.

An identified zip file was found to contain the Microsoft Word file macro_t1smud.doc. Once the macro is enabled, a bash script runs a sleep command and the script connects to `htxxps://the.earth.li/~sgtatham/putty/latest/w32/putty.exe`. This binary is likely the legitimate Putty Secure Shell binary. Upon download the file is saved to `C:\Users\Public\Documents\` file path.

Profile of Malicious Hashes

- **Saintbot** (and related .Net loaders)
- **WhisperGate Malware and related VB files**
- **Quasar RAT**
- **.NET Infostealer malware**
- **Telegram Bot**
- **Multiple Loaders** (mostly utilizing PowerShell that pull down a jpg or bin files)
- **Jpg/PNG files** = obfuscated executables
- **antidef.bat** = likely a bat file to disable Windows Defender

Table 3: Additional IOCs associated with WhisperGate

Hash	Associated Files
647ebdca2ef6b74b17bb126df19bf0ed88341650	loader2132.exe
24f71409bde9d01e3519236e66f3452236302e46	saint.exe
1e3497ac435936be06ba665a4acd06b850cf56b4	loader.exe
981319f00b654d0142430082f2e636ef69a377d9	Yudjcfoyg.exe
e0dbe49c9398a954095ee68186f391c288b9fcc5	Project_1.exe
0ba64c284dc0e13bc3f7adfee084ed25844da3d2	Hjtiyz.jpg
6b8eab6713abb7c1c51701f12f23cdff2ff3a243	Ltfckzl.jpg
3bbb84206f0c81f7fd57148f913db448a8172e92	Vgdnggv.jpg
7c77b1c72a2228936e4989de2dfab95bfbbbc737	Pfiegomql.jpg
c0cd6f8567df73e9851dbca4f7c4fbfe4813a2e1	Fezpwij.jpg
d6830184a413628db9946faaae8b08099c0593a0	Bqpptgcal.jpg
d083da96134924273a7cbc8b6c51c1e92de4f9e1	loader.jpg
d599f16e60a916f38f201f1a4e6d73cb92822502	Debythht.jpg
9b9374a5e376492184a368fcc6723a7012132eae	Dmhdgocsp.jpg
86bd95db7b514ea0185dba7876fa612fae42b715	Zysyrokzk.jpg
e7917df9feabfedae47d8b905136d52cb5cb7f37	Baeipiyd.jpg

b2d863fc444b99c479859ad7f012b840f896172e	Tbopbh.jpg
d85e1614cf4a1e9ec632580b62b0ecb5f8664352	Lxkdjr.jpg
08f0b0d66d370151fd8a265b1f9be8be61cc1aa9	Twojt.bin
5ac592332a406d5b2dcfc81b131d261da7e791d2	Rvlxi.bin
052825569c880212e1e39898d387ef50238aaf35	Yarfe.bin
4c2a0f44b176ba83347062df1d56919a25445568	Ftvqpq.bin
d51214461fc694a218a01591c72fe89af0353bc1	Pkbsu.bin
1125b2c3c91491aa71e0536bb9a8a1b86ff8f641	Pkcxiu.bin
37f54f121bcae65b4b3dd680694a11c5a5dfc406	loader.bin
4facd9a973505bb00eb1fd9687cbab906742df73	loader.bin
376a2339cbbb94d33f82dea2ea78bb011485e0d9	Qmpnrffn.bin
b6793fc62b27ee3cce24e9e63e3108a777f71904	Vpzhote.bin
1fc463b2f53ba0889c90cc2b7866afae45a511de	Yymmdbfrb.bin
ff71f9defc2dd27b488d961ce0fbc6ece56b2962	Zlhmmwutx.bin
13ca079770f6f9bdddfea5f9d829889dc1fbc4ed	Xhlnfjeqy.bin
c99c982d1515ade3da81268e79f5e5f7d550aabd	Gpfsqm.png
d6ffa42548ff12703e38c5db6c9c39c34fe3d82a	Ktlbo.png

bd5116865bcf066758f817ba9385cc7d001ecad9	Vgdnggv.png
034c0d73b21cf17c25c086d19a6ef3bb8a06bab7	Rsscffiiu.png
69e4efc8000a473d2b2c0067f317b22664453205	loader.png
424f7a756f72f1da9012859bf86ad7651bafa937	Wmztvc.png
6c64e1f2ba11ecff5e899f880d14da42acf3f699	Ygxdlt.png
fa8a373e837d7be2fce0bfe073a6fdeaefc56ca1	Fewbfaklk.png
0eccc0aa674fd9fc27023c70067e630fd5d21cd6	www.google.png
6e11c3e119499f11b83787cc4bb5f2751bd90219	Nxoaa.com
8a93bfd9e70611547a420971662d113b6b3c6234	Lxkdjr.com
b19d5f0d8696271aff5af616b91a4cdc73981934	www.google.com
b5e3e65cd6b09b17d4819a1379dde7db3e33813b	Cpdfx.jpeg
d92e315f3c290a7e71950480f074af5b59e8bd3d	Mtubbb.jpeg
fb83899dc633c59a8473a3048c9aacce7e1bf8d8	Kzwolw.jpeg
5fbd9bd73040d7a2cac0fc21d2fe29ebe57fb597	Fczdcmep.jpeg
90fa56e79765d27d35706d028d32dc5be7efb623	Jdeiipc.jpeg
cd8ef5a2543a2535416655f861c574c63e9008ea	5415.jpeg
72a45d6bfde93eb92a7b7a1ea284f35e1d24203a	000.jpeg

d2a697fc1b61888c49a48ce094e400b62a71201d	Ofewufeiy.exe
bddb6994656659d098d6040dc895e90877fb1266	load.exe
00d6c66ab2fd1810628d13980cc73275884933b1	loader.exe
12f50a97955497c49f9603ea2531384e430f0df5	loader.exe
27c176bbd3e254d5e46ccb865d29c8c166ba4a9f	Wdlord.bin
88c76d31b046227d82f94db87697b25e482eb398	Ofewufeiy.bin
2e113050a81bbd0774db7e86fad4abd44e5b6ec2	Bdfjvu.bin
db370ee79d9b4bd44e07f425d7b06beffc8bdded	Jdnpanki.bin
88e5bf24bd0f01778217c4fcdb37b76929c2d32b	downloader.bin
f6acdc16c695c3c219116aea3d585efedcafdab5	up74987340.bin
c3181fd7cb463893fc73974acc0016605d90ef6c	Tdivhgry.png
731dab83ef1d02203db64fbefbe59f3791db1e21	Mbowytboz.png
50566fdea2f4b8a3466427f9c6798dabe2587823	Tlmbluje.png
5dbd68dd3bab6f3a06e303d68bb23e37994084eb	loader.png
ac618c4ece55eca2b067bedd2ce963b8ada30b40	antidef.bat
a0074dbb3316eb570c08219609921a33052d7356	antidef.bat
c4f8d6354ef3ee4e437aa7312df0121446d3a71f	antidef.bat

d9c2ce9c53f10cd12844a98270b4559e9fbfde44	antidef.bat
87a36b87bade46d0b0614b104152db7814808b21	antidef.bat
d3ff54b679922ff9296bfb1b4c379d361f44afd9	1631031555.doc
71daf7af9480743f9e20254946521d6b648b0fe8	1631031555.doc
1aa120fe90d053060fb4e741bcde1f41d6d33303	1631031555.doc
aa124ef17e870e6cd291cb371cde52ca4ffc94d2	1631031555.doc
f79829972bc0ace5c498df3a840acf7d41c56056	1631031555.doc
efa60e42ff1f5c5b57b9fb15a5b04baded2c4c82	1631031555.doc
c96fc59fbe8495dbb50e5ba73b53496614ef8a8a	1631031555.doc
09650cb7a5ed0f43cf67985d03182ca608591a7c	1631031555.doc
c9600ba9e63500b2fe345ff190042ef11d4ce88e	1631031555.doc
ba6f3e474174bcb97c365b4d6365c71ca294aa16	1631031555.doc
f71f0289d99aa1334e7e74b68320cbabbd37fbc1	1631031555.doc
50df153f513b3be09e474b23553b3610625fbb41	1631031555.doc
9496494756ab4276cf4e4aeb4988e781f0db031a	1631031555.doc
4de3118370c2720d60df566684b8b3b7ebf6dfa2	1631031555.doc
d2d475d2df5b0ec1e97ea45e499f55e45d2aac17	1631031555.doc

cdf858add61db5c44503f78cda67915ddb0f77d6	1631031555.doc
39e7abe29f4a574d80b438233e4d2099b99000bb	1631031555.doc
4212472d84ab9f36402bcc12193b9c63901a21d2	1631031555.doc
2277461ac707766f5bb694235b7edfd78af26ff1	1631031555.doc
d57100a6d734be30a8a92734175a67983c7b0c32	1631031555.doc
ba9a811915c3134bfde4414b051a8e6d7949080c	1631031555.doc
1d543a67ea0fcbc5cdc3d698af0d285356d2001b	1631031555.doc
965e4bae8d753efc695c3b1705f43ea7333a1688	1631031555.doc
594fad1593de55df36f294a32330f7b6f487a3e8	1631031555.doc
ac672a07c62d48c0a7f98554038913770efaef11	1631031555.doc
fa62e7df0cc1ece81ba2228cc22be01214cab2ab	1631031555.doc
fdc6bf0a4154d79115ddfac02134580ac4685222	1631031555.doc
e5828387cd6f596932d6caebfd76de1df5ba9ee2	1631031555.doc
f5c769d2a27877e56cc0c540490b26c7c0ff25dd	1631031555.doc
b589574d1ca3438929b8051329552d8e62a7a128	1631031555.doc
1f731bef9777cd4531de39b98a881d83506bb5d9	1631031555.doc
e68dc7a106dab7186fc3ff3f7c70ab280b89d17d	1631031555.doc

572acb2baea77c5ba8e9fe668fd81a817e695d73	1631031555.doc
27a6e76209de03e55136dd72533f3c81d3e715e4	1631031555.doc
1ae21693ce6060059a1284a1e3166f735c339687	1631031555.doc
9e96114159d458597ed2fdc8603a97c9cd2c1e90	1631031555.doc
ca00849b308d48daaea7d86e0d7c7af580a2e856	1631031555.doc
305d215c36d2a7fd9913007059a93e140503870d	1631031555.doc
d503b4818a36f7eae9fbee0d8468b811bca87e83	1631031555.doc
512510a1a5c20ecbcc96781366edaaac58ae4608	1631031555.doc
e53c3b7726cb36b3e898d48ad0f25dbd032e8a8b	1631031555.doc
2ecbb11218f3a24a6c1f33ea7027ab714fad2c3f	1631031555.doc
93cecf50d645ff633ef57e014c49a3ae967140c6	1631031555.doc
10bc94cdefb8ed8d305d087ca868b8fe963c69d4	1631031555.doc
c4740eec9528e1a205326c8a7b7e8d44c8a5b6b1	1631031555.doc
312b8526b3e961887104e80f6447f5bb33ed06df	1631031555.doc
88750f0e1f488656ef0aeb3c40a5785d6c72eb3f	1631031555.doc
c5e57aa3e027f1ae4d3216a5b652b11a63314534	1631031555.doc
d6594fda649e3e4f15ea35e8ed29ac5c8c14760a	1631031555.doc

f831bb0148a8f9d34f914d9560be062c821a7d83	1631031555.doc
b48cbc3ba518c9db5840169e1e21b3ca66cd8177	1631031555.doc
3bb75935fc79205dffccb6102a19f0b96300ab70	1631031555.doc
9d0d4de1d09624de659ce39f449ce5a17f1bef50	1631031555.doc
5ab518686fcd3879dd8c02d74b97caa333ea51ab	1631031555.doc
8fbc7565af01b4a53c72fede3678f4aeba40c5f4	1631031555.doc
8998c076c21930b8fb223882fd9d82899544a902	1621031555.doc
988f07a4094a4a93b76a165ea9f7e251bbbf340f	1621031555.doc
95cf3c261178388c850a777ffe981bbeb287afcb	1621031555.doc
e52cea59499060b8d0e84a7594a687448599f386	1621031555.doc
cdcccb2a011cd22f49d7a96ffb06df3fe334f960	1621031555.doc
5ec9d35b41ee59d109370b257603aa804ecb7c15	1621031555.doc
42a28a4fa6bdb674be63001cd5efff6f7c1b11fc	1621031555.doc
4fabb94902244f60fd2359c61c1c79434095a2ba	1621031555.doc
fbc4d60042c69bf2b5fec701201b24ceb22a43fe	1621031555.doc
5096ca0de8b6ca27dcdcf5790a2cb99566f03e04	1622031555.doc
f7cf30c68989c4a3852397f59fda5d8d1f67f396	1622031555.doc

c4ebbfcb3dc47a1260a0af9b3eb9b125f48d22cc	1622031555.doc
59b03cfb7f2d672f66eb6d027244cb1d9f39f30a	16.09.2021.pdf.js
4ac3c035909101ebddcb78573723d4d48b293a6e	loader_exe_64_97975_1.exe
f990e9c85cd196f9380930e951fbc2085fdf76b7	api_signed_3.exe
e8623063485c61d7411fab8f72cfdbab08f29131	api_crypted_2.exe
e0770b79e372f2cab86ae2ec33b5160708059eee	payload.exe
2ee451947da9efdee0e9f39c9623f388297db6b4	test2.exe 21312d.exe
c681f91c80673deff9f6efa61060f597fc0c1cd0	payload.exe
d8d875f31c4d7c40cfd6483d6b250943d4f5e437	api177_crypted.exe
f24c3237a1612888c8b5526e557a963f3b73e984	api177_signed.exe
76152dc6243ae29d8315f24f6e9449d620f672cd	Fearsomely.exe
d08d894023b16b8374466e6e9ede97f56f7cd4c7	firstgoon.exe
f7ab3996edf81551fdd867fdd28a616491445c38	test4.exe
31ef83a2032cdcc2412991a8fbfe75ed1eed11e8	documents.exe
d08d894023b16b8374466e6e9ede97f56f7cd4c7	firstgoon1.exe
8b9e47457a645d41b98ba07249e8cc3406831cb5	7.exe

f9b6fff55fef34fc49432c8338eb3e9c0c44286e	Matrix_MAX.exe
b91ede2fa35ea3d4031fb51c32bc8211ab5f1e75	crypted.exe
d665b0cfd313d8a72586b0515b92496dd7dc4bb0	crypted_2.exe
4a434c738e402242ecca92182312f04ce336ff86	work.exe
3e50a761cd4bbd9eeaf8f6b9629f9ce871d6f2dd	SLP.exe
6c216522d2a1211399fb08567fcdec1d341340e3	Downloader.exe
6d11b5e4fce9c580b06298ca3dd4a6134fe4b520	Xhlnfjeqy.exe
3ac2d185c28548d43ea47b8fa3795b4308a4c39d	Jdnpanki.exe
e0770b79e372f2cab86ae2ec33b5160708059eee	payload.vbs payload_2.vbs
98ab3ae46358a66c480810d1e4f24ef730e4dc7e	1.rar

Revisions

February 26, 2022: Initial Revision |March 1, 2022: Added STIX version.|April 28, 2022: Updated IOCs.

Tags

Nation-State Actor: Russia

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

Give Feedback

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov