THREAT BULLETINS

UPDATE - Joint Cybersecurity Advisory: Destructive Malware Targeting Organizations in Ukraine

TLP:WHITE

Apr 29, 2022

On April 28, 2022, an update to the Joint Cybersecurity Advisory (CSA), AA22-057A, by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) was released 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.

Additionally, specific malware analysis reports (MAR) are provided within the report for the various malware groups below:

- HermeticWiper
- IsaacWiper and HermeticWizard
- CaddyWiper

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.

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.

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.

UPDATE: Additional IOCs Associated with WhisperGate

The additional IOCs associated with WhisperGate 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.

Reference(s)	CISA, Microsoft, Sentinel One, CISA, CISA, us-cert, us-cert, us-cert, CISA, 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

Threat Indicator(s)

Domain(s):
Lxkdjr[.]com
Nxoaa[.]com

SHA1:
7c77b1c72a2228936e4989de2dfab95bfbbbc737
b6793fc62b27ee3cce24e9e63e3108a777f71904
9496494756ab4276cf4e4aeb4988e781f0db031a
e7917df9feabfedae47d8b905136d52cb5cb7f37

```
5ab518686fcd3879dd8c02d74b97caa333ea51ab
f71f0289d99aa1334e7e74b68320cbabbd37fbc1
8fbc7565af01b4a53c72fede3678f4aeba40c5f4
4a434c738e402242ecca92182312f04ce336ff86
71daf7af9480743f9e20254946521d6b648b0fe8
ba9a811915c3134bfde4414b051a8e6d7949080c
0eccc0aa674fd9fc27023c70067e630fd5d21cd6
88750f0e1f488656ef0aeb3c40a5785d6c72eb3f
e68dc7a106dab7186fc3ff3f7c70ab280b89d17d
cd8ef5a2543a2535416655f861c574c63e9008ea
3bbb84206f0c81f7fd57148f913db448a8172e92
9b9374a5e376492184a368fcc6723a7012132eae
59b03cfb7f2d672f66eb6d027244cb1d9f39f30a
bddb6994656659d098d6040dc895e90877fb1266
6e11c3e119499f11b83787cc4bb5f2751bd90219
ac672a07c62d48c0a7f98554038913770efaef11
fdc6bf0a4154d79115ddfac02134580ac4685222
88e5bf24bd0f01778217c4fcdb37b76929c2d32b
09650cb7a5ed0f43cf67985d03182ca608591a7c
1e3497ac435936be06ba665a4acd06b850cf56b4
76152dc6243ae29d8315f24f6e9449d620f672cd
2ecbb11218f3a24a6c1f33ea7027ab714fad2c3f
572acb2baea77c5ba8e9fe668fd81a817e695d73
b19d5f0d8696271aff5af616b91a4cdc73981934
50df153f513b3be09e474b23553b3610625fbb41
ca00849b308d48daaea7d86e0d7c7af580a2e856
9e96114159d458597ed2fdc8603a97c9cd2c1e90
27a6e76209de03e55136dd72533f3c81d3e715e4
c4f8d6354ef3ee4e437aa7312df0121446d3a71f
6c216522d2a1211399fb08567fcdec1d341340e3
f24c3237a1612888c8b5526e557a963f3b73e984
db370ee79d9b4bd44e07f425d7b06beffc8bdded
37f54f121bcae65b4b3dd680694a11c5a5dfc406
f9b6fff55fef34fc49432c8338eb3e9c0c44286e
981319f00b654d0142430082f2e636ef69a377d9
d599f16e60a916f38f201f1a4e6d73cb92822502
2e113050a81bbd0774db7e86fad4abd44e5b6ec2
24f71409bde9d01e3519236e66f3452236302e46
3bb75935fc79205dffccb6102a19f0b96300ab70
4c2a0f44b176ba83347062df1d56919a25445568
034c0d73b21cf17c25c086d19a6ef3bb8a06bab7
bd5116865bcf066758f817ba9385cc7d001ecad9
fa8a373e837d7be2fce0bfe073a6fdeaefc56ca1
5096ca0de8b6ca27dcdcf5790a2cb99566f03e04
647ebdca2ef6b74b17bb126df19bf0ed88341650
```

```
d92e315f3c290a7e71950480f074af5b59e8bd3d
1f731bef9777cd4531de39b98a881d83506bb5d9
8a93bfd9e70611547a420971662d113b6b3c6234
c96fc59fbe8495dbb50e5ba73b53496614ef8a8a
d2d475d2df5b0ec1e97ea45e499f55e45d2aac17
13ca079770f6f9bdddfea5f9d829889dc1fbc4ed
965e4bae8d753efc695c3b1705f43ea7333a1688
b589574d1ca3438929b8051329552d8e62a7a128
d3ff54b679922ff9296bfb1b4c379d361f44afd9
e0770b79e372f2cab86ae2ec33b5160708059eee
c99c982d1515ade3da81268e79f5e5f7d550aabd
ba6f3e474174bcb97c365b4d6365c71ca294aa16
1d543a67ea0fcbc5cdc3d698af0d285356d2001b
c4740eec9528e1a205326c8a7b7e8d44c8a5b6b1
052825569c880212e1e39898d387ef50238aaf35
d6594fda649e3e4f15ea35e8ed29ac5c8c14760a
e5828387cd6f596932d6caebfd76de1df5ba9ee2
ac618c4ece55eca2b067bedd2ce963b8ada30b40
98ab3ae46358a66c480810d1e4f24ef730e4dc7e
cdcccb2a011cd22f49d7a96ffb06df3fe334f960
4fabb94902244f60fd2359c61c1c79434095a2ba
69e4efc8000a473d2b2c0067f317b22664453205
424f7a756f72f1da9012859bf86ad7651bafa937
cdf858add61db5c44503f78cda67915ddb0f77d6
1125b2c3c91491aa71e0536bb9a8a1b86ff8f641
d8d875f31c4d7c40cfd6483d6b250943d4f5e437
88c76d31b046227d82f94db87697b25e482eb398
d2a697fc1b61888c49a48ce094e400b62a71201d
90fa56e79765d27d35706d028d32dc5be7efb623
b5e3e65cd6b09b17d4819a1379dde7db3e33813b
d51214461fc694a218a01591c72fe89af0353bc1
988f07a4094a4a93b76a165ea9f7e251bbbf340f
c4ebbfcb3dc47a1260a0af9b3eb9b125f48d22cc
f5c769d2a27877e56cc0c540490b26c7c0ff25dd
fa62e7df0cc1ece81ba2228cc22be01214cab2ab
6c64e1f2ba11ecff5e899f880d14da42acf3f699
f831bb0148a8f9d34f914d9560be062c821a7d83
10bc94cdefb8ed8d305d087ca868b8fe963c69d4
95cf3c261178388c850a777ffe981bbeb287afcb
aa124ef17e870e6cd291cb371cde52ca4ffc94d2
f7ab3996edf81551fdd867fdd28a616491445c38
00d6c66ab2fd1810628d13980cc73275884933b1
86bd95db7b514ea0185dba7876fa612fae42b715
e53c3b7726cb36b3e898d48ad0f25dbd032e8a8b
f7cf30c68989c4a3852397f59fda5d8d1f67f396
```

```
2ee451947da9efdee0e9f39c9623f388297db6b4
50566fdea2f4b8a3466427f9c6798dabe2587823
c5e57aa3e027f1ae4d3216a5b652b11a63314534
fb83899dc633c59a8473a3048c9aacce7e1bf8d8
6d11b5e4fce9c580b06298ca3dd4a6134fe4b520
e52cea59499060b8d0e84a7594a687448599f386
d9c2ce9c53f10cd12844a98270b4559e9fbfde44
ff71f9defc2dd27b488d961ce0fbc6ece56b2962
c0cd6f8567df73e9851dbca4f7c4fbfe4813a2e1
d85e1614cf4a1e9ec632580b62b0ecb5f8664352
c681f91c80673deff9f6efa61060f597fc0c1cd0
3ac2d185c28548d43ea47b8fa3795b4308a4c39d
1ae21693ce6060059a1284a1e3166f735c339687
12f50a97955497c49f9603ea2531384e430f0df5
594fad1593de55df36f294a32330f7b6f487a3e8
d08d894023b16b8374466e6e9ede97f56f7cd4c7
0ba64c284dc0e13bc3f7adfee084ed25844da3d2
72a45d6bfde93eb92a7b7a1ea284f35e1d24203a
4ac3c035909101ebddcb78573723d4d48b293a6e
1aa120fe90d053060fb4e741bcde1f41d6d33303
d6830184a413628db9946faaae8b08099c0593a0
376a2339cbbb94d33f82dea2ea78bb011485e0d9
1fc463b2f53ba0889c90cc2b7866afae45a511de
3e50a761cd4bbd9eeaf8f6b9629f9ce871d6f2dd
2277461ac707766f5bb694235b7edfd78af26ff1
fbc4d60042c69bf2b5fec701201b24ceb22a43fe
39e7abe29f4a574d80b438233e4d2099b99000bb
e0dbe49c9398a954095ee68186f391c288b9fcc5
d083da96134924273a7cbc8b6c51c1e92de4f9e1
5fbd9bd73040d7a2cac0fc21d2fe29ebe57fb597
312b8526b3e961887104e80f6447f5bb33ed06df
c3181fd7cb463893fc73974acc0016605d90ef6c
d6ffa42548ff12703e38c5db6c9c39c34fe3d82a
305d215c36d2a7fd9913007059a93e140503870d
f79829972bc0ace5c498df3a840acf7d41c56056
93cecf50d645ff633ef57e014c49a3ae967140c6
08f0b0d66d370151fd8a265b1f9be8be61cc1aa9
d503b4818a36f7eae9fbee0d8468b811bca87e83
31ef83a2032cdcc2412991a8fbfe75ed1eed11e8
27c176bbd3e254d5e46ccb865d29c8c166ba4a9f
d665b0cfd313d8a72586b0515b92496dd7dc4bb0
9d0d4de1d09624de659ce39f449ce5a17f1bef50
efa60e42ff1f5c5b57b9fb15a5b04baded2c4c82
d57100a6d734be30a8a92734175a67983c7b0c32
a0074dbb3316eb570c08219609921a33052d7356
```

```
b2d863fc444b99c479859ad7f012b840f896172e
c9600ba9e63500b2fe345ff190042ef11d4ce88e
5ec9d35b41ee59d109370b257603aa804ecb7c15
87a36b87bade46d0b0614b104152db7814808b21
6b8eab6713abb7c1c51701f12f23cdff2ff3a243
4facd9a973505bb00eb1fd9687cbab906742df73
731dab83ef1d02203db64fbefbe59f3791db1e21
5dbd68dd3bab6f3a06e303d68bb23e37994084eb
8b9e47457a645d41b98ba07249e8cc3406831cb5
f990e9c85cd196f9380930e951fbc2085fdf76b7
4212472d84ab9f36402bcc12193b9c63901a21d2
b91ede2fa35ea3d4031fb51c32bc8211ab5f1e75
5ac592332a406d5b2dcfc81b131d261da7e791d2
f6acdc16c695c3c219116aea3d585efedcafdab5
b48cbc3ba518c9db5840169e1e21b3ca66cd8177
512510a1a5c20ecbcc96781366edaaac58ae4608
8998c076c21930b8fb223882fd9d82899544a902
4de3118370c2720d60df566684b8b3b7ebf6dfa2
e8623063485c61d7411fab8f72cfdbab08f29131
42a28a4fa6bdb674be63001cd5efff6f7c1b11fc
```

Alert ID ea81a81a

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

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.

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**.

##
##

Health-ISAC (H-ISAC)
www.h-isac.org
twitter.com/HealthISAC