TLP:WHITE

JOINT CYBERSECURITY ADVISORY

Ransomware Activity Targeting the Healthcare and Public Health Sector

AA20-302A

October 28, 2020

Updated October 29, 2020

TLP:WHITE

TLP:WHITE

Note: This advisory was updated on October 29, 2020 to include information on Conti, TrickBot, and BazarLoader, including new IOCs and Yara Rules for detection.

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 7 framework. See the ATT&CK for Enterprise version 7 for all referenced threat actor tactics and techniques.

SUMMARY

This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). This advisory describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health Sector (HPH) to infect systems with ransomware, notably Ryuk and Conti, for financial gain.

CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers. CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.

Key Findings

- CISA, FBI, and HHS assess malicious cyber actors are targeting the HPH Sector with TrickBot and BazarLoader malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services.
- These issues will be particularly challenging for organizations within the COVID-19 pandemic; therefore, administrators will need to balance this risk when determining their cybersecurity investments.

TECHNICAL DETAILS

Threat Details

The cybercriminal enterprise behind TrickBot, which is likely also the creator of BazarLoader malware, has continued to develop new functionality and tools, increasing the ease, speed, and profitability of victimization. These threat actors increasingly use loaders—like TrickBot and BazarLoader (or BazarBackdoor)—as part of their malicious cyber campaigns. Cybercriminals disseminate TrickBot and BazarLoader via phishing campaigns that contain either links to malicious websites that host the malware or attachments with the malware. Loaders start the infection chain by distributing the payload; they deploy and execute the backdoor from the C2 server and install it on the victim's machine.

TrickBot

What began as a banking trojan and descendant of Dyre malware, TrickBot now provides its operators a full suite of tools to conduct a myriad of illegal cyber activities. These activities include credential harvesting, mail exfiltration, cryptomining, point-of-sale data exfiltration, and the deployment of ransomware, such as Ryuk and Conti.

In early 2019, FBI began to observe new TrickBot modules named Anchor, which cyber actors typically used in attacks targeting high-profile victims—such as large corporations. These attacks often involved data exfiltration from networks and point-of-sale devices. As part of the new Anchor toolset, TrickBot developers created `anchor_dns`, a tool for sending and receiving data from victim machines using Domain Name System (DNS) tunneling.

`anchor_dns` is a backdoor that allows victim machines to communicate with command and control (C2) servers over DNS to evade typical network defense products and make their malicious communications blend in with legitimate DNS traffic. `anchor_dns` uses a single-byte `XOR` cipher to encrypt its communications, which have been observed using key `0xB9`. Once decrypted, the string `anchor_dns` can be found in the DNS request traffic.

TrickBot Indicators of Compromise

After successful execution of the malware, TrickBot copies itself as an executable file with a 12-character (includes `.exe`), randomly generated file name (e.g. `mfjdieks.exe`) and places this file in one of the following directories.

- C:\Windows\
- C:\Windows\SysWOW64\
- C:\Users\[Username]\AppData\Roaming\

Once the executable is running and successful in establishing communication with C2s, the executable places appropriate modules downloaded from C2s for the infected processor architecture type (32 or 64 bit instruction set), to the infected host's `%APPDATA%` or `%PROGRAMDATA%` directory, such as `%AppData\Roaming\winapp`. Some commonly named plugins that are created in a `Modules` subdirectory are (the detected architecture is appended to the module filename, e.g., `importDll32` or `importDll64`):

- `Systeminfo`
- `importDll`
- `outlookDll`
- `injectDll` with a directory (ex. `injectDLL64_configs`) containing configuration files:
  - `dinj`
  - `sinj`
  - `dpost`
- `mailsearcher` with a directory (ex. `mailsearcher64_configs`) containing configuration file:
  - `mailconf`
- `networkDll` with a directory (ex. `networkDll64_configs`) containing configuration file:

    - dpost
- wormDll
- tabDll
- shareDll

Filename client_id or data or FAQ with the assigned bot ID of the compromised system is created in the malware directory. Filename group_tag or Readme.md containing the TrickBot campaign IDs is created in the malware directory.

The malware may also drop a file named anchorDiag.txt in one of the directories listed above.

Part of the initial network communications with the C2 server involves sending information about the victim machine such as its computer name/hostname, operating system version, and build via a base64-encoded GUID. The GUID is composed of /GroupID/ClientID/ with the following naming convention:

/anchor_dns/[COMPUTERNAME]_[WindowsVersionBuildNo].[32CharacterString]/.

The malware uses scheduled tasks that run every 15 minutes to ensure persistence on the victim machine. The scheduled task typically uses the following naming convention.

[random_folder_name_in_%APPDATA%_excluding_Microsoft] autoupdate#[5_random_numbers] (e.g., Task autoupdate#16876).

After successful execution, anchor_dns further deploys malicious batch scripts (.bat) using PowerShell commands.

The malware deploys self-deletion techniques by executing the following commands.

- cmd.exe /c timeout 3 && del C:\Users\[username]\[malware_sample]
- cmd.exe /C PowerShell \"Start-Sleep 3; Remove-Item C:\Users\[username]\[malware_sample_location]\"

The following domains found in outbound DNS records are associated with anchor_dns.

- kostunivo[.]com
- chishir[.]com
- mangoclone[.]com
- onixcellent[.]com

This malware used the following legitimate domains to test internet connectivity.

- ipecho[.]net
- api[.]ipify[.]org
- checkip[.]amazonaws[.]com
- ip[.]anysrc[.]net
- wtfismyip[.]com
- ipinfo[.]io

- icanhazip[.]com
- myexternalip[.]com
- ident[.]me

Currently, there is an open source tracker for Trickbot C2 servers located at https://feodotracker.abuse.ch/browse/trickbot/.

The anchor_dns malware historically used the following C2 servers.

- 23[.]95[.]97[.]59
- 51[.]254[.]25[.]115
- 193[.]183[.]98[.]66
- 91[.]217[.]137[.]37
- 87[.]98[.]175[.]85

TrickBot YARA Rules

```
rule anchor_dns_strings_filenames {
    meta:
        description = "Rule to detect AnchorDNS samples based off strings or
filenames used in malware"
        author = "NCSC"
        hash1 = "fc0efd612ad528795472e99cae5944b68b8e26dc"
        hash2 = "794eb3a9ce8b7e5092bb1b93341a54097f5b78a9"
        hash3 = "9dfce70fded4f3bc2aa50ca772b0f9094b7b1fb2"
        hash4 = "24d4bbc982a6a561f0426a683b9617de1a96a74a"
    strings:
        $ = ",Control_RunDLL \x00"
        $ = ":$GUID" ascii wide
        $ = ":$DATA" ascii wide
        $ = "/1001/"
        $ = /(\x00|\xCC)qwertyuiopasdfghjklzxcvbnm(\x00|\xCC)/
        $ = /(\x00|\xCC)QWERTYUIOPASDFGHJKLZXCVBNM(\x00|\xCC)/
        $ = "start program with cmdline \"%s\""
        $ = "Global\\fde345tyhoVGYHUJKIOuy"
        $ = "ChardWorker::thExecute: error registry me"
        $ = "get command: incode %s, cmdid \"%s\", cmd \"%s\""
```

```
        $ = "anchorDNS"
        $ = "Anchor_x86"
        $ = "Anchor_x64"
    condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and 3 of them
}

rule anchor_dns_icmp_transport {
    meta:
        description = "Rule to detect AnchorDNS samples based off ICMP transport
strings"
        author = "NCSC"
        hash1 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
    strings:
        $ = "reset_connection <- %s"
        $ = "server_ok <- %s (packets on server %s)"
        $ = "erase successfully transmitted packet (count: %d)"
        $ = "Packet sended with crc %s -> %s"
        $ = "send data confimation to server(%s)"
        $ = "data recived from <- %s"
        $ = "Rearmost packed recived (id: %s)"
        $ = "send poll to server -> : %s"
    condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and 3 of them
}

rule anchor_dns_config_dexor {
    meta:
        description = "Rule to detect AnchorDNS samples based off configuration
deobfuscation (XOR 0x23 countup)"
```

```
        author = "NCSC"
        hash1 = "d0278ec015e10ada000915a1943ddbb3a0b6b3db"
        hash2 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
    strings:
        $x86 = {75 1F 56 6A 40 B2 23 33 C9 5E 8A 81 ?? ?? ?? ?? 32 C2 FE C2 88 81
?? ?? ?? ?? 41 83 EE 01 75 EA 5E B8 ?? ?? ?? ?? C3}
        $x64 = {41 B0 23 41 B9 80 00 00 00 8A 84 3A ?? ?? ?? 00 41 32 C0 41 FE C0
88 04 32 48 FF C2 49 83 E9 01 75 E7}
    condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}


rule anchor_dns_installer {
    meta:
        description = "Rule to detect AnchorDNS installer samples based off MZ
magic under one-time pad or deobfuscation loop code"
        author = "NCSC"
        hash1 = "fa98074dc18ad7e2d357b5d168c00a91256d87d1"
        hash2 = "78f0737d2b1e605aad62af252b246ef390521f02"
    strings:
        $pre = {43 00 4F 00 4E 00 4F 00 55 00 54 00 24 00 00 00} //CONOUT$
        $pst = {6B 65 72 6E 65 6C 33 32 2E 64 6C 6C 00 00 00 00} //kernel32.dll
        $deob_x86 = {8B C8 89 4D F8 83 F9 FF 74 52 46 89 5D F4 88 5D FF 85 F6 74
34 8A 83 ?? ?? ?? ?? 32 83 ?? ?? ?? ?? 6A 00 88 45 FF 8D 45 F4 50 6A 01 8D 45 FF
50 51 FF 15 34 80 41 00 8B 4D F8 43 8B F0 81 FB 00 ?? ?? ?? 72 CC 85 F6 75 08}
        $deob_x64 = {42 0F B6 84 3F ?? ?? ?? ?? 4C 8D 8C 24 80 00 00 00 42 32 84
3F ?? ?? ?? ?? 48 8D 54 24 78 41 B8 01 00 00 00 88 44 24 78 48 8B CE 48 89 6C 24
20 FF 15 ?? ?? ?? ?? 48 FF C7 8B D8 48 81 FF ?? ?? ?? ?? 72 B8}
    condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550)
        and
            (   uint16(@pre+16) ^ uint16(@pre+16+((@pst-(@pre+16))\2)) == 0x5A4D
```

```
                or
                $deob_x86 or $deob_x64
            )
}

import "pe"
rule anchor_dns_string_1001_with_pe_section_dll_export_resolve_ip_domains {
    meta:
        description = "Rule to detect AnchorDNS samples based off /1001/ string
in combination with DLL export name string, PE section .addr or IP resolution
domains"
        author = "NCSC"
        hash1 = "ff8237252d53200c132dd742edc77a6c67565eee"
        hash2 = "c8299aadf886da55cb47e5cbafe8c5a482b47fc8"
    strings:
        $str1001 = {2F 31 30 30 31 2F 00} // /1001/
        $strCtrl = {2C 43 6F 6E 74 72 6F 6C 5F 52 75 6E 44 4C 4C 20 00} //
,Control_RunDLL
        $ip1 = "checkip.amazonaws.com" ascii wide
        $ip2 = "ipecho.net" ascii wide
        $ip3 = "ipinfo.io" ascii wide
        $ip4 = "api.ipify.org" ascii wide
        $ip5 = "icanhazip.com" ascii wide
        $ip6 = "myexternalip.com" ascii wide
        $ip7 = "wtfismyip.com" ascii wide
        $ip8 = "ip.anysrc.net" ascii wide
    condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550)
        and $str1001
        and (
                for any i in (0..pe.number_of_sections): (
```

```
                    pe.sections[i].name == ".addr"
                )
            or
                $strCtrl
            or
                6 of ($ip*)
            )
}


rule anchor_dns_check_random_string_in_dns_response {
    meta:
        description = "Rule to detect AnchorDNS samples based off checking random
string in DNS response"
        author = "NCSC"
        hash1 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
        hash2 = "14e9d68bba7a184863667c680a8d5a757149aa36"
    strings:
        $x86 = {8A D8 83 C4 10 84 DB 75 08 8B 7D BC E9 84 00 00 00 8B 7D BC 32 DB
8B C7 33 F6 0F 1F 00 85 C0 74 71 40 6A 2F 50 E8 ?? ?? ?? ?? 46 83 C4 08 83 FE 03
72 EA 85 C0 74 5B 83 7D D4 10 8D 4D C0 8B 75 D0 8D 50 01 0F 43 4D C0 83 EE 04 72
11 8B 02 3B 01 75 10 83 C2 04 83 C1 04 83 EE 04 73 EF 83 FE FC 74 2D 8A 02 3A 01
75 29 83 FE FD 74 22 8A 42 01 3A 41 01 75 1C 83 FE FE 74 15 8A 42 02 3A 41 02 75
0F 83 FE FF 74 08 8A 42 03 3A 41 03 75 02 B3 01 8B 75 B8}
        $x64 = {4C 39 75 EF 74 56 48 8D 45 DF 48 83 7D F7 10 48 0F 43 45 DF 49 8B
FE 48 85 C0 74 40 48 8D 48 01 BA 2F 00 00 00 E8 ?? ?? ?? ?? 49 03 FF 48 83 FF 03
72 E4 48 85 C0 74 24 48 8D 55 1F 48 83 7D 37 10 48 0F 43 55 1F 48 8D 48 01 4C 8B
45 2F E8 ?? ?? ?? ?? 0F B6 DB 85 C0 41 0F 44 DF 49 03 F7 48 8B 55 F7 48 83 FE 05
0F 82 6A FF FF FF}
    condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}


rule anchor_dns_default_result_execute_command {
```

```
    meta:
        description = "Rule to detect AnchorDNS samples based off default result
value and executing command"
        author = "NCSC"
        hash1 = "056f326d9ab960ed02356b34a6dcd72d7180fc83"
        hash2 = "14e9d68bba7a184863667c680a8d5a757149aa36"
    strings:
        $x86 = {83 C4 04 3D 80 00 00 00 73 15 8B 04 85 ?? ?? ?? ?? 85 C0 74 0A 8D
4D D8 51 8B CF FF D0 8A D8 84 DB C7 45 A4 0F 00 00 00}
        $x64 = {48 98 B9 E7 03 00 00 48 3D 80 00 00 00 73 1B 48 8D 15 ?? ?? ?? ??
48 8B 04 C2 48 85 C0 74 0B 48 8D 55 90 48 8B CE FF D0 8B C8}
    condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}


rule anchor_dns_pdbs {
    meta:
        description = "Rule to detect AnchorDNS samples based off partial PDB
paths"
        author = "NCSC"
        hash1 = "f0e575475f33600aede6a1b9a5c14f671cb93b7b"
        hash2 = "1304372bd4cdd877778621aea715f45face93d68"
        hash3 = "e5dc7c8bfa285b61dda1618f0ade9c256be75d1a"
        hash4 = "f96613ac6687f5dbbed13c727fa5d427e94d6128"
        hash5 = "46750d34a3a11dd16727dc622d127717beda4fa2"
    strings:
        $ = ":\\MyProjects\\secondWork\\Anchor\\"
        $ = ":\\simsim\\anchorDNS"
        $ = ":\\[JOB]\\Anchor\\"
        $ = ":\\Anchor\\Win32\\Release\\Anchor_"
        $ = ":\\Users\\ProFi\\Desktop\\data\\Win32\\anchor"
```

```
    condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}
```

BazarLoader/BazarBackdoor

Beginning in approximately early 2020, actors believed to be associated with Trickbot began using BazarLoader and BazarBackdoor to infect victim networks. The loader and backdoor work closely together to achieve infection and communicate with the same C2 infrastructure. Campaigns using Bazar represent a new technique for cybercriminals to infect and monetize networks and have increasingly led to the deployment of ransomware, including Ryuk. BazarLoader has become one of the most commonly used vectors for ransomware deployment.

Deployment of the BazarLoader malware typically comes from phishing email and contains the following:

- Phishing emails are typically delivered by commercial mass email delivery services. Email received by a victim will contain a link to an actor-controlled Google Drive document or other free online filehosting solutions, typically purporting to be a PDF file.
- This document usually references a failure to create a preview of the document and contains a link to a URL hosting a malware payload in the form of a misnamed or multiple extension file.
- Emails can appear as routine, legitimate business correspondence about customer complaints, hiring decision, or other important tasks that require the attention of the recipient.
- Some email communications have included the recipient's name or employer name in the subject line and/or email body.

Through phishing emails linking users to Google Documents, actors used the below identified file names to install BazarLoader:

- `Report-Review26-10.exe`
- `Review_Report15-10.exe`
- `Document_Print.exe`
- `Report10-13.exe`
- `Text_Report.exe`

Bazar activity can be identified by searching the system startup folders and Userinit values under the `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` registry key:

`%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\adobe.lnk`

For a comprehensive list of indicators of compromise regarding the BazarLocker malware, see https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html.

Indicators

In addition to TrickBot and BazarLoader, threat actors are using malware, such as KEGTAP, BEERBOT, SINGLEMALT, and others as they continue to change tactics, techniques, and procedures in their highly dynamic campaign.[1] The following C2 servers are known to be associated with this malicious activity.

- 45[.]148[.]10[.]92
- 170[.]238[.]117[.]187
- 177[.]74[.]232[.]124
- 185[.]68[.]93[.]17
- 203[.]176[.]135[.]102
- 96[.]9[.]73[.]73
- 96[.]9[.]77[.]142
- 37[.]187[.]3[.]176
- 45[.]89[.]127[.]92
- 62[.]108[.]35[.]103
- 91[.]200[.]103[.]242
- 103[.]84[.]238[.]3
- 36[.]89[.]106[.]69
- 103[.]76[.]169[.]213
- 36[.]91[.]87[.]227
- 105[.]163[.]17[.]83
- 185[.]117[.]73[.]163
- 5[.]2[.]78[.]118
- 185[.]90[.]61[.]69
- 185[.]90[.]61[.]62
- 86[.]104[.]194[.]30
- 31[.]131[.]21[.]184
- 46[.]28[.]64[.]8
- 104[.]161[.]32[.]111
- 107[.]172[.]140[.]171
- 131[.]153[.]22[.]148
- 195[.]123[.]240[.]219
- 195[.]123[.]242[.]119
- 195[.]123[.]242[.]120
- 51[.]81[.]113[.]25

[1] FireEye: Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser

- `74[.]222[.]14[.]27`

Ryuk Ransomware

Typically Ryuk has been deployed as a payload from banking Trojans such as TrickBot.[2] Ryuk first appeared in August 2018 as a derivative of Hermes 2.1 ransomware, which first emerged in late 2017 and was available for sale on the open market as of August 2018. Ryuk still retains some aspects of the Hermes code. For example, all of the files encrypted by Ryuk contain the `HERMES` tag but, in some infections, the files have `.ryk` added to the filename, while others do not. In other parts of the ransomware code, Ryuk has removed or replaced features of Hermes, such as the restriction against targeting specific Eurasia-based systems.

While negotiating the victim network, Ryuk actors will commonly use commercial off-the-shelf products—such as Cobalt Strike and PowerShell Empire—in order to steal credentials. Both frameworks are very robust and are highly effective dual-purpose tools, allowing actors to dump clear text passwords or hash values from memory with the use of Mimikatz. This allows the actors to inject malicious dynamic-link library into memory with read, write, and execute permissions. In order to maintain persistence in the victim environment, Ryuk actors have been known to use scheduled tasks and service creation.

Ryuk actors will quickly map the network in order to enumerate the environment to understand the scope of the infection. In order to limit suspicious activity and possible detection, the actors choose to live off the land and, if possible, use native tools—such as net view, net computers, and ping—to locate mapped network shares, domain controllers, and active directory. In order to move laterally throughout the network, the group relies on native tools, such as PowerShell, Windows Management Instrumentation (WMI), Windows Remote Management , and Remote Desktop Protocol (RDP). The group also uses third-party tools, such as Bloodhound.

Once dropped, Ryuk uses AES-256 to encrypt files and an RSA public key to encrypt the AES key. The Ryuk dropper drops a `.bat` file that attempts to delete all backup files and Volume Shadow Copies (automatic backup snapshots made by Windows), preventing the victim from recovering encrypted files without the decryption program.

In addition, the attackers will attempt to shut down or uninstall security applications on the victim systems that might prevent the ransomware from executing. Normally this is done via a script, but if that fails, the attackers are capable of manually removing the applications that could stop the attack. The `RyukReadMe` file placed on the system after encryption provides either one or two email addresses, using the end-to-end encrypted email provider Protonmail, through which the victim can

[2] See the United Kingdom (UK) National Cyber Security Centre (NCSC) advisory, Ryuk Ransomware Targeting Organisations Globally, on their ongoing investigation into global Ryuk ransomware campaigns and associated Emotet and TrickBot malware.

contact the attacker(s). While earlier versions provide a ransom amount in the initial notifications, Ryuk users are now designating a ransom amount only after the victim makes contact.

The victim is told how much to pay to a specified Bitcoin wallet for the decryptor and is provided a sample decryption of two files.

Initial testing indicates that the `RyukReadMe` file does not need to be present for the decryption script to run successfully but other reporting advises some files will not decrypt properly without it. Even if run correctly, there is no guarantee the decryptor will be effective. This is further complicated because the `RyukReadMe` file is deleted when the script is finished. This may affect the decryption script unless it is saved and stored in a different location before running.

According to MITRE, Ryuk uses the ATT&CK techniques listed in table 1.

Table 1: Ryuk ATT&CK techniques

Technique	Use
System Network Configuration Discovery [T1016]	Ryuk has called `GetIpNetTable` in attempt to identify all mounted drives and hosts that have Address Resolution Protocol entries.
Masquerading: Match Legitimate Name or Location [T1036.005]	Ryuk has constructed legitimate appearing installation folder paths by calling `GetWindowsDirectoryW` and then inserting a null byte at the fourth character of the path. For Windows Vista or higher, the path would appear as `C:\Users\Public`.
Process Injection [T1055]	Ryuk has injected itself into remote processes to encrypt files using a combination of `VirtualAlloc`, `WriteProcessMemory`, and `CreateRemoteThread`.
Process Discovery [T1057]	Ryuk has called `CreateToolhelp32Snapshot` to enumerate all running processes.
Command and Scripting Interpreter: Windows Command Shell [T1059.003]	Ryuk has used `cmd.exe` to create a Registry entry to establish persistence.
File and Directory Discovery [T1083]	Ryuk has called `GetLogicalDrives` to enumerate all mounted drives, and `GetDriveTypeW` to determine the drive type.
Native API [T1106]	Ryuk has used multiple native APIs including `ShellExecuteW` to run executables,

Technique	Use
	`GetWindowsDirectoryW` to create folders, and `VirtualAlloc`, `WriteProcessMemory`, and `CreateRemoteThread` for process injection.
Access Token Manipulation [T1134]	Ryuk has attempted to adjust its token privileges to have the `SeDebugPrivilege`.
Data Encrypted for Impact [T1486]	Ryuk has used a combination of symmetric and asymmetric encryption to encrypt files. Files have been encrypted with their own AES key and given a file extension of `.RYK`. Encrypted directories have had a ransom note of `RyukReadMe.txt` written to the directory.
Service Stop [T1489]	Ryuk has called `kill.bat` for stopping services, disabling services and killing processes.
Inhibit System Recovery [T1490]	Ryuk has used `vssadmin Delete Shadows /all /quiet` to delete volume shadow copies and `vssadmin resize shadowstorage` to force deletion of shadow copies created by third-party applications.
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]	Ryuk has used the Windows command line to create a Registry entry under `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` to establish persistence.
Impair Defenses: Disable or Modify Tools [T1562.001]	Ryuk has stopped services related to anti-virus.

MITIGATIONS

For a downloadable copy of IOCs, see AA20-302A.stix. For additional IOCs detailing this activity, see https://gist.github.com/aaronst/6aa7f61246f53a8dd4befea86e832456.

Plans and Policies

CISA, FBI, and HHS encourage HPH Sector organizations to maintain business continuity plans—the practice of executing essential functions through emergencies (e.g., cyberattacks)—to minimize service interruptions. Without planning, provision, and implementation of continuity principles, organizations may be unable to continue operations. Evaluating continuity and capability will help identify continuity gaps. Through identifying and addressing these gaps, organizations can establish a viable continuity program that will help keep them functioning during cyberattacks or other

emergencies. CISA, FBI, and HHS suggest HPH Sector organizations review or establish patching plans, security policies, user agreements, and business continuity plans to ensure they address current threats posed by malicious cyber actors.

Network Best Practices

- Patch operating systems, software, and firmware as soon as manufacturers release updates.
- Check configurations for every operating system version for HPH organization-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled.
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Audit logs to ensure new accounts are legitimate.
- Scan for open or listening ports and mediate those that are not needed.
- Identify critical assets such as patient database servers, medical records, and teleheatlh and telework infrastructure; create backups of these systems and house the backups offline from the network.
- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment.
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans.

Ransomware Best Practices

CISA, FBI and HHS do not recommend paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. In addition to implementing the above network best practices, the FBI, CISA and HHS also recommend the following:

- Regularly back up data, air gap, and password protect backup copies offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location.

User Awareness Best Practices

- Focus on awareness and training. Because end users are targeted, make employees and stakeholders aware of the threats—such as ransomware and phishing scams—and how they

are delivered. Additionally, provide users training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities.
- Ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyberattack. This will ensure that the proper established mitigation strategy can be employed quickly and efficiently.

Recommended Mitigation Measures

System administrators who have indicators of a TrickBot network compromise should immediately take steps to back up and secure sensitive or proprietary data. TrickBot infections may be indicators of an imminent ransomware attack; system administrators should take steps to secure network devices accordingly. Upon evidence of a TrickBot infection, review DNS logs and use the `XOR` key of `0xB9` to decode `XOR` encoded DNS requests to reveal the presence of `anchor_dns`, and maintain and provide relevant logs.

GENERAL RANSOMWARE MITIGATIONS — HPH SECTOR

This section is based on CISA and Multi-State Information Sharing and Analysis Center (MS-ISAC)'s Joint Ransomware Guide, which can be found at https://www.cisa.gov/publication/ransomware-guide.

CISA, FBI, and HHS recommend that healthcare organizations implement both ransomware prevention and ransomware response meaures immediately.

Ransomware Prevention

Join and Engage with Cybersecurity Organizations

CISA, FBI, and HHS recommend that healthcare organizations take the following initial steps:

- Join a healthcare information sharing organization, H-ISAC:
  - Health Information Sharing and Analysis Center (H-ISAC): https://h-isac.org/membership-account/join-h-isac/
  - Sector-based ISACs - National Council of ISACs: https://www.nationalisacs.org/member-isacs
  - Information Sharing and Analysis Organization (ISAO) Standards Organization: https://www.isao.org/information-sharing-groups/
- Engage with CISA and FBI, as well as HHS—through the HHS Health Sector Cybersecurity Coordination Center (HC3)—to build a lasting partnership and collaborate on information sharing, best practices, assessments, and exercises.
  - CISA: cisa.gov, https://us-cert.cisa.gov/mailing-lists-and-feeds,
  - FBI: ic3.gov, www.fbi.gov/contact-us/field-offices
  - HHS/HC3: http://www.hhs.gov/hc3,

Engaging with the H-ISAC, ISAO, CISA, FBI, and HHS/HC3 will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

Follow Ransomware Best Practices

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline or in separated networks as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
    - Use the 3-2-1 rule as a guideline for backup practices. The rule states that three copies of all critical data are retained on at least two different types of media and at least one of them is stored offline.
    - Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
    - Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
        - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
        - Ensure all backup hardware is properly patched.
- In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
    - Review available incident response guidance, such as CISA's Technical Approaches to Uncovering and Remediating Malicious Activity https://us-cert.cisa.gov/ncas/alerts/aa20-245a.
- Help your organization better organize around cyber incident response.
- Develop a cyber incident response plan.
- The Ransomware Response Checklist, available in the CISA and MS-ISAC Joint Ransomware Guide, serves as an adaptable, ransomware- specific annex to organizational cyber incident response or disruption plans.
- Review and implement as applicable MITRE's Medical Device Cybersecurity: Regional Incident Preparedness and Response Playbook (https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf).

- Develop a risk management plan that maps critical health services and care to the necessary information systems; this will ensure that the incident response plan will contain the proper triage procedures.
- Plan for the possibility of critical information systems being inaccessible for an extended period of time. This should include but not be limited to the following:
    - Print and properly store/protect hard copies of digital information that would be required for critical patient healthcare.
    - Plan for and periodically train staff to handle the re-routing of incoming/existing patients in an expedient manner if information systems were to abruptly and unexpectedly become unavailable.
    - Coordinate the potential for surge support with other healthcare facilities in the greater local area. This should include organizational leadership periodically meeting and collaborating with counterparts in the greater local area to create/update plans for their facilities to both abruptly send and receive a significant amount of critical patients for immediate care. This may include the opportunity to re-route healthcare employees (and possibly some equipment) to provide care along with additional patients.
- Consider the development of a second, air-gapped communications network that can provide a minimum standard of backup support for hospital operations if the primary network becomes unavailable if/when needed.
- Predefine network segments, IT capabilities and other functionality that can either be quickly separated from the greater network or shut down entirely without impacting operations of the rest of the IT infrastructure.
- Legacy devices should be identified and inventoried with highest priority and given special consideration during a ransomware event.
- See CISA and MS-ISAC's Joint Ransomware Guide for infection vectors including internet-facing vulnerabilities and misconfigurations; phishing; precursor malware infection; and third parties and managed service providers.
- HHS/HC3 tracks ransomware that is targeting the HPH Sector; this information can be found at http://www.hhs.gov/hc3.

Hardening Guidance

- The Food and Drug Administration provides multiple guidance documents regarding the hardening of healthcare and specifically medical devices found here: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.
- See CISA and MS-ISAC's Joint Ransomware Guide for additional in-depth hardening guidance.

Contact CISA for These No-Cost Resources

- Information sharing with CISA and MS-ISAC (for SLTT organizations) includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware.

- Policy-oriented or technical assessments help organizations understand how they can improve their defenses to avoid ransomware infection: https://www.cisa.gov/cyber-resource-hub.
    - Assessments include Vulnerability Scanning and Phishing Campaign Assessment.
- Cyber exercises evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario.
- CISA Cybersecurity Advisors (CSAs) advise on best practices and connect you with CISA resources to manage cyber risk.

Ransomware Quick References

- *Ransomware: What It Is and What to Do About It* (CISA): General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf
- *Ransomware* (CISA): Introduction to ransomware, notable links to CISA products on protecting networks, specific ransomware threats, and other resources: https://www.us-cert.cisa.gov/Ransomware
- HHS/HC3: Ransomware that impacts HPH is tracked by the HC3 and can be found at www.hhs.gov/hc3
- *Security Primer* – Ransomware (MS-ISAC): Outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations: https://www.cisecurity.org/white-papers/security-primer-ransomware/
- *Ransomware: Facts, Threats, and Countermeasures* (MS- ISAC): Facts about ransomware, infection vectors, ransomware capabilities, and how to mitigate the risk of ransomware infection: https://www.cisecurity.org/blog/ransomware- facts-threats-and-countermeasures/
- HHS Ransomware Fact Sheet: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- NIST Securing Data Integrity White Paper: https://csrc.nist.gov/publications/detail/white-paper/2020/10/01/securing-data-integrity-against-ransomware-attacks/draft

Ransomware Response Checklist

Remember: Paying the ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised. CISA, FBI, and HHS do not recommend paying ransom.

Should your organization be a victim of ransomware, CISA strongly recommends responding by using the Ransomware Response Checklist located in CISA and MS-ISAC's Joint Ransomware Guide, which contains steps for detection and analysis as well as containment and eradication.

Consider the Need For Extended Identification or Analysis

If extended identification or analysis is needed, CISA, HHS/HC3, or federal law enforcement may be interested in any of the following information that your organization determines it can legally share:

□ Recovered executable file

□ Copies of the readme file – DO NOT REMOVE the file or decryption may not be possible

□ Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)

□ Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)

□ Malware samples

□ Names of any other malware identified on your system

□ Encrypted file samples

□ Log files (Windows Event Logs from compromised systems, Firewall logs, etc.)

□ Any PowerShell scripts found having executed on the systems

□ Any user accounts created in Active Directory or machines added to the network during the exploitation

□ Email addresses used by the attackers and any associated phishing emails

□ A copy of the ransom note

□ Ransom amount and whether or not the ransom was paid

□ Bitcoin wallets used by the attackers

□ Bitcoin wallets used to pay the ransom (if applicable)

□ Copies of any communications with attackers

Upon voluntary request, CISA can assist with analysis (e.g., phishing emails, storage media, logs, malware) at no cost to support your organization in understanding the root cause of an incident, even in the event additional remote assistance is not requested.

- CISA – Advanced Malware Analysis Center: https://www.malware.us-cert.gov/MalwareSubmission/pages/submission.jsf

CONTACT INFORMATION

CISA, FBI, and HHS recommend identifying and having on hand the following contact information for ready use should your organization become a victim of a ransomware incident. Consider contacting these organizations for mitigation and response assistance or for purpose of notification.

- State and Local Response Contacts
- IT/IT Security Team – Centralized Cyber Incident Reporting
- State and Local Law Enforcement
- Fusion Center
- Managed/Security Service Providers

- Cyber Insurance

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Additionally, see CISA and MS-ISAC's Joint Ransomware Guide for information on contacting—and what to expect from contacting—federal asset response and federal threat response contacts.

RESOURCES

- CISA Emergency Services Sector Continuity Planning Suite
- CISA MS-ISAC Joint Ransomware Guide
- CISA Tip: Avoiding Social Engineering and Phishing Attacks
- FBI PSA: High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations
- Health Industry Cybersecurity Tactical Crisis Response
- Health Industry Cybersecurity Practices (HICP)
- HHS - Ransomware Spotlight Webinar
- HHS - Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
- HHS - Ransomware Briefing
- HHS - Aggressive Ransomware Impacts
- HHS - Ransomware Fact Sheet
- HHS - Cyber Attack Checklist
- HHS - Cyber-Attack Response Infographic
- NIST - Data Integrity Publication
- NIST - Guide for Cybersecurity Event Recovery
- NIST - Identifying and Protecting Assets Against Ransomware and Other Destructive Events
- NIST - Detecting and Responding to Ransomware and Other Destructive Events
- NIST - Recovering from Ransomware and Other Destructive Events
- FireEye - Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser
- Github list of IOCs