Published on *The National Law Review* https://natlawreview.com

Federal Agencies Partner to Warn Healthcare Systems of Imminent Cyber Threat

Article By:

Privacy and Data Protection Practice Group

US hospitals and healthcare systems should be on high alert after a rare joint advisory issued by the Federal Bureau of Investigation (FBI), the Cybersecurity Infrastructure Security Agency (CISA) and the Department of Health and Human Services (HHS) warning all US hospitals and healthcare providers of an "increased and imminent cybercrime threat to US hospitals and healthcare providers." The joint advisory can be found here.

In Depth

In the advisory released late in the evening of October 28, 2020, the FBI, CISA and HHS warned against the threat of Ryuk ransomware, which is often deployed using Trickbot malware or other exploitation tools, and can spread quickly across an affected organization's networks, disabling their systems. These agencies received credible intelligence of malicious threat actors targeting approximately 400 healthcare providers in the United States with Ryuk attacks.

Large-scale ransomware attacks during an upsurge of COVID-19 cases and hospitalizations would present a significant challenge to an already burdened healthcare system, as is noted in the advisory. The agencies' warning is intended to provide hospitals and healthcare providers with information they need to take steps to protect their network before infection and to provide guidance on responding to ransomware attacks to those entities which have already been compromised. The advisory explains how Ryuk and Trickbot are deployed and spread, and provides indicators of compromise (IOCs) associated with such attacks, along with key tips on network protection and ransomware response best practices. If your organization is targeted by a ransomware attack, note that US law enforcement agencies do not recommend paying the ransom. The Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory earlier this month reminding victim entities that paying a ransom to a threat actor that is either a sanctioned entity or covered by comprehensive country or region sanctions is a violation of OFAC regulations and may result in civil penalties.

If your organization is the target of a cyberattack, we encourage you to consult with legal counsel immediately. Forensic vendors are reporting a spike in cybersecurity incidents and may be at capacity and unable to provide immediate service. Consider lining up third-party resources ahead of time to be on standby.

Indicators of Compromise

Below is the list of IOCs CISA, FBI and HHS identified in their advisory. Separately, cybersecurity incident response firm Mandiant also released a list of domains and Internet Protocol (IP) addresses used by Ryuk in previous attacks this year. Please review your systems for these IOCs, and if found, take immediate steps to protect your network and data.

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***

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

Prior to initiating communications with the C2 server, the malware uses an infection marker of ***Global\fde345tyhoVGYHUJKIOuy****, typically found in the running memory of the victim machine.*

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***

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***

National Law Review, Volume X, Number 303

Source URL:https://natlawreview.com/article/federal-agencies-partner-to-warn-healthcare-systems-imminent-cyber-threat