U.S. Department of Health & Human Services

ASPR Administration for Strategic Preparedness & Response

From the Office of Critical Infrastructure Protection within the Office of Preparedness

Healthcare and Public Health Sector Cybersecurity Notification

June 16, 2023

This email notification was produced by the Division of Critical Infrastructure Protection (CIP) within the U.S. Department of Health and Human Services' (HHS) Office of the Administration for Strategic Preparedness and Response (ASPR) and the Office of Information Security's Health Sector Cybersecurity Coordination Center (HC3).

#TimisoaraHackerTeam Analysis

Executive Summary

A ransomware variant and threat group called TimisoaraHackerTeam has resurfaced in a recent ransomware attack on a medical facility. Little is know about the obscure group of hackers, but when its ransomware is deployed, their rarely used and very effective technique of encrypting data in a target environment has paralyzed the health and public health (HPH) sector. An examination of the ransomware strain and the group's tactics provides insight into how and why they target the healthcare sector, possible ties to other threat groups, and recommendations for how HPH organizations can better protect themselves.

Overview

Discovered by researchers in July 2018, TimisoaraHackerTeam (THT) is a relatively unknown threat actor that has previously attacked healthcare organizations around the world. Rather than use custom built tools to encrypt the files of the victims like many ransomware groups, THT's characteristic tactic of abusing legitimate tools like Microsoft Bitlocker and Jetico's BestCrypt makes them unique among threat actors. While rare, the use of these tools and other tactics, techniques, and procedures (TTPs) have additionally been linked to other attacks orchestrated by threat group, DeepBlueMagic, and also to Chinese hackers, prompting speculation of a potential relationship between THT and these groups.

Name	TimisoaraHackerTeam

Type	Threat Actor and Ransomware
Short Description	The ransomware encrypts files on your computer system and demands a ransom to be paid to allegedly recover them.
Symptoms	The ransomware will encrypt your files and leave a ransom note with payment instructions.
Distribution Method	Spam Emails, Email Attachments
Ransom Note Contact Information	▪ m4xroothackerteam@protonmail.com ▪ timisoarahackerteam@protonmail.com ▪ vitaly.vermakov@protonmail.com ▪ vitalyyermankov@cock.li

Impact to HPH Sector

Even among hackers, there is often a code of conduct not to attack hospitals or other HPH organizations that could cause physical harm. However, in their purposeful targeting of the healthcare sector, groups like THT abstain from that moral code. The June 2023 attack on a U.S. cancer center significantly reduced patient treatment capability, rendered digital services unavailable, and also threatened exposure of patient personal health information (PHI) and personal identifiable information (PII).

A previous April 2021 attack against a French hospital was also loosely attributed to THT based on the historical use of their TTPs. While both aforementioned attacks were attributed to THT by name, attacks by other groups with a potential nexus to THT are similarly examined below. Healthcare is particularly vulnerable to cyberattacks owing to their high propensity to pay a ransom, the value of patient records, and often inadequate security.

Leadership and Key Individuals

Named after a Romanian town, its ransomware seems to have been produced by Romanian speakers, judging from its source code. The text instructions that THT ransomware creates for its victims provide instructions in grammatically incorrect English, suggesting that the threat actors are not native speakers of the language. However, whether operating in Romania or using the implication of a false lead, the overarching family that THT ransomware belong to has yet to be defined by analysts.

Motivations

THT appears to be financially motivated in their targeting of the health sector, often demanding ransom in the form of Bitcoin to unlock infected servers. One cybersecurity company noted that THT ransomware targets only big corporations with more than 30 terminals.

For purposes of this product, THT is identified as a unique Ransomware as a Service (RaaS) group and ransomware. However, similar TTPs (i.e. encryption tools, ransom notes, and/or nonencryption of system drive (C:/)) have created speculations that THT may have ties to or be an offshoot of other threat groups.

Nomenclature and Associations

For purposes of this product, THT is identified as a unique Ransomware as a Service (RaaS) group and ransomware. However, similar TTPs (i.e. encryption tools, ransom notes, and/or nonencryption of system drive (C:/)) have created speculations that THT may have ties to or be an offshoot of other threat groups.

DeepBlueMagic
First observed in an attack on a device running Windows Servers 2012 R2 by researchers at Heimdal Security on August 11, 2021, DeepBlueMagic is both a RaaS group and ransomware strain. It's most infamous attack was on a medical center in Israel in October 2021. The incident paralyzed the majority of the hospital's computer sytems, resulting not only in the theft of large amounts of data, including confidential pateint information, but also an inability to access patient files and the patient registry system, and nonfuctional electric doors. In a matter of days, the targeting of the medical center, which was attributed to DeepBlueMagic, spurred an additional nine attacks on other hospitals and health organizations in the country, resulting in the largest cyber attack ever launched on the Israeli health sector.

DeepBlueMagic shares common behaviors with THT, prompting some cybersecurity experts to speculate that DeepBlueMagic may be an evolution of the group, or has simply adopted the same TTPs at THT. Nevertheless, both share a focus for targeting the healthcare sector.

- Usage of legitimate third-party disk encryption tool – Jetico BestCrypt
- Similar ransom notes

Hello. Your company's server hard drive was encrypted by us.

We use the most complex encryption algorithm (AES256). Only we can decrypt.

Please contact us: [email address 1]

(Please check spam, Avoid missing mail)

*Identification code: ******** (Please tell us the identification code)*

Please contact us and we will tell you the amount of ransom and how to pay.

(If the contact is fast, we will give you a discount.)

After the payment is successful, we will tell the decrypt password.

In order for you to believe in us, we have prepared the test server. Please contact us and we will tell the test server and decrypt the password.

Please do not scan encrypted hard drives or attempt to recover data. Prevent data corruption. [redacted]

In its August 2021 inception attack, researchers determined that DeepBlueMagic ransomware disabled security solutions installed on devices to prevent detection, then proceeded to encrypt entire hard drives using a third-party disk encryption tool rather than files. All drives on the targeted server were encryped with the exception of the system drive ("C:\" partition). Heimdal was not able to determine how the attackers might have gained initial access to the compromised system. It was also unable to obtain a sample of the original executable file because the ransomware deleted iself from the system.

The ransomware also used BestCrypt Volume Encryption software from Jetico. In the attack, the D:\ drive was turned into a RAW partition rather than New Technology File System (NTFS), which rendered it inaccessible. Following an attack, any attempt to access the encryped drive would result in the Windows OS interfact prompting the user to accept formatting of the disk, since the drive would be unreadable.

Further analysis of the attack revealed the ransomware stopped all third-party Windows services on the targeted device, thus disabling all security solutions. Then, DeepBlueMagic ransomware deleted the Volume Shadow Copy of Windows to ensure the drive could not be restored. An attempt was also made to activate Bitlocker on all endpoints in the Active Directory.

In this attack, the disk encryption process was started but was not completed; only the volume headers were encrypted. This meant that the encryption process could be continued, or the rescue file created by Jetico's BestCrypt Volume Encryption could be used to restore the drive; however, the rescue file was also encrypted by the ransomware. In order to access the rescue file, a password must be provided.

Heimdal Security said the ransomware itself was self-deleted in the attack, so it could not be recovered and analyzed on this occasion. The researchers were not able to determine how the ransomware was installed on the server but said there were no failed login attempts so it was not delivered as a result of a brute force attack. The server only had a Microsoft Dynamics AAX installed with a Microsoft SQL Server. The ransomware note saved to the desktop advised the victim to make contain via email to find out how much must be paid for the password to recover the encrypted drives.

Heimdal Security researchers said because the encryption process was only partially completed, recovery without paying the ransom is possible. They simulated the DeepBlueMagic process and attempted to use several decryption tools and were able to successfully restore the files on the inaccessible partition using the free TestDisk tool from CGSecurity.org.

In the ransom note itself, similar verbiage and sentence structure makes it look like DeepBlueMagic all but recycled the same message. With the only difference being the account details, this suggests a possible linkage between the groups.

APT41 (People's Republic of China)
Following the attack on the Israeli HPH sector, some cybersecurity experts in the country attributed the ransomware to a group of criminals working out of China. Israeli authorities shared the IOCs from their own investigation, and, as confirmed by independent cybersecurity firms, determined that the threat actors used the "BestCrypt" hard drive encryption tool to encrypt devices. Early indications suggest that DeepBlueMagic, which claimed attribution, gained initial access by exploiting a known Pulse Secure VPN vulnerability. Israel's Natonal Cyber Directorate released the IOCs in the form of file hashes that have been seen in related attacks.

Soon after, the cybersecurity chief for the Israeli Health Ministry announced that the attack was likely carried out by "a Chinese hacker group that broke away from another group and started working in August…who motives were purely financial." However, a source in the cybersecurity industry told a leading publication that the attribution to China is weak and that the attacks may have simply been port scans or probes into a network's defenses.

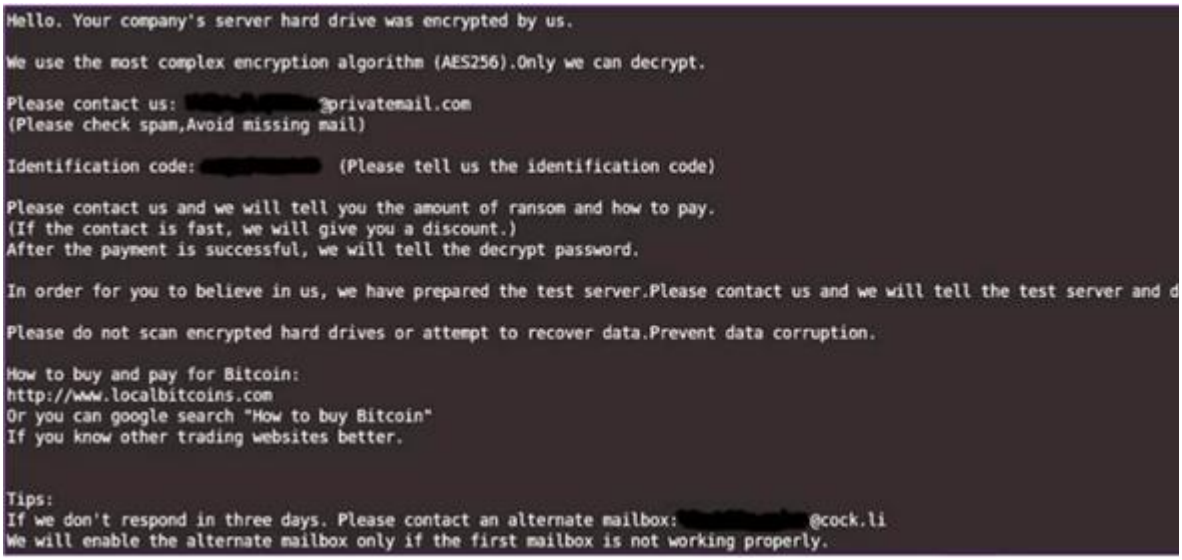
Conversely, one cybersecurity reseacher noted similarities between DeepBlueMagic and the Chinese state-sponsored threat actor, APT41. Examining an August 2021 report on DeepBlueMagic by Heimdal security experts and an April 2020 report on APT41 by LIFARS security researchers, he noted that both publications likely refer to the same ransomware variant

and observed notable common behaviors from the two groups in both publications:

- Usage of legitimate third-party disk encryption tool – Jetico BestCrypt
- System drive (C:/) is not encrypted
- Similar ransom notes

Similar to THT and DeepBlueMagic, APT41's ransom note contains similar verbiage and sentence structure. With the only difference being the account details, this also suggests a possible linkage between the groups.

Whereas LIFARS provided indicators of compromise (IOCs), Heimdal did not, making a comparative analysis of the malware all but impossible. Nevertheless, the possible Chinese connection to this group could explain the high level of sophistication and innovation behind DeepBlueMagic's recent activity.



Common Tactics, Techniques, and Procedures (TTPs)
THT encrypts files with a virus and places a .txt file, with instructions inside about the compromised system. It's ransomware variant, like the many ransomware Trojans, will take a victim's files hostage, encrypting them with a strong encryption algorithm. THT ransomware attacks seem to be carried out by taking advantage of poorly protected Remote Desktop access and targeted medium to large servers.

THT has been known to utilize various exploits to gain initial remote access into a victim's network. Most commonly, THT will employ Common Vulnerability Exploitations (CVEs) against vulnerable VPNs to gain initial access into a network and deploy a ransomware attack.

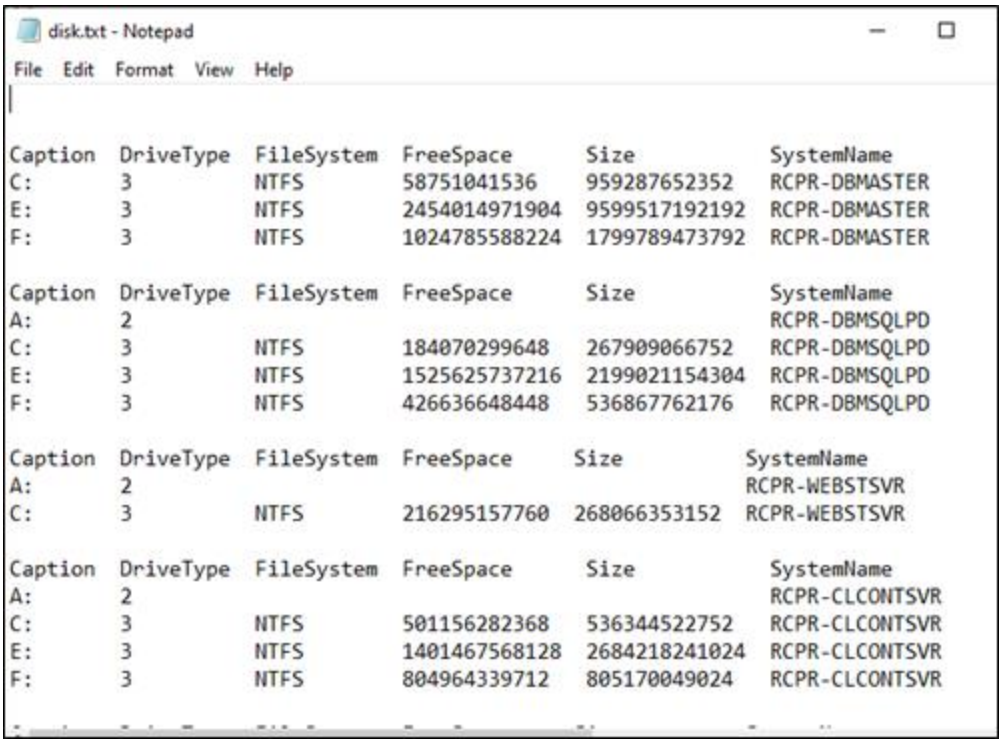
The threat group also utilizes zero-day vulnerability found in Microsoft Exchange servers found in early 2021 and recent vulnerabilities in Fortinet firewalls. THT usually uses "The Onion Router" (TOR) and/or other anonymizing services to make connections. THT will usually authenticate into the network using administrative level credentials obtained via vulnerabilities exploitation. Once THT gains initial access into a victim's network, they will look to move laterally around the network.

THT has found success on flat networks with little to no segregation/compartmentalization. THT will sometimes drop files using shared network folders/drives.

TTPs utilized by THT include Living off the Land (LotL) tools, which are less likely to be detected by traditional security solutions. These include the use of legitimate tools such as Microsoft BitLocker (if there is only a "C:\" drive) and BestCrypt for all other logical volumes. For the most recent incident against an American healthcare organization, the following attack vectors were captured:

Targeted Service	▪ FortiOS SSL VPN ▪ It is highly likely that CVE-2022-42475 was exploited in this incident
Threat Movement	Remote Desktop Protocol (RDP) utilized to move laterally throughout networks
Encryption Tools Used	▪ Bitlocker - Native Windows Tools (No Unique Indicators) ▪ BestCrypt - Commercial Software ("crypt" folder dropped onto root directory of "C:" drive that contains commercial BestCrypt files "license.txt" in "C:/crypt" folder contains trial license key for BestCrypt (MD5: 4c7d7ce7ae0b2db8ae0b809c35811b59)
IP Addresses Used to Remotely Access Victim Network	▪ 89.185.85.140 (TOR/Onion Routing) ▪ 185.220.101.60 (TOR/Onion Routing)

Indicators of Compromise (IOCs)
IOCs from the domain controller PRCCR-DC01
The file "address.txt" has a total of 22 IPs all from subnet 10.4.0.x or 10.4.1.x. targeting PRCCR site.



Subscribe to HPH Sector Cyber Notifications

Did a colleague forward you this HPH Sector Cyber Notification? Receive these cyber notifications directly by subscribing to the HPH Sector bulletins. HPH Sector bulletins inform stakeholders about the most significant issues facing the sector including cybersecurity, medical supply chains, COVID-19, and more. If you are interested in receiving cyber notifications or other HPH Sector bulletins, visit the CIP bulletins subscription webpage.

Comments and Questions

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov or ASPR CIP at CIP@hhs.gov

Traffic Light Protocol (TLP) Designation: CLEAR

TLP: CLEAR information may be distributed without restriction.

. Disclaimer: ASPR provides the above sources of information for the convenience of the HPH Sector community and is not responsible for the availability or content of the information or tools provided, nor does ASPR endorse, warrant or guarantee the products, services or information described or offered. It is the responsibility of the user to determine the usefulness and applicability of the information provided.

U.S. Department of Health & Human Services, Office of the Administration for Strategic Preparedness & Response
200 C Street, SW
Washington, DC 20024