HC3: Threat Actor Profile

October 4, 2024 TLP:CLEAR Report: 202410041500

Trinity Ransomware

Executive Summary

Trinity ransomware is a relatively new threat actor, known for employing a double extortion strategy. This method involves exfiltrating sensitive data before encrypting files, thereby increasing pressure on victims to pay the ransom. This ransomware uses the ChaCha20 encryption algorithm, and encrypted files are tagged with the ".trinitylock" file extension. Trinity operates a victim support site for decryption assistance and a leak site that displays their victims. It also shares similarities with two other ransomware groups—2023Lock and Venus—suggesting possible connections or collaborations among these threat actors. The group's tactics and techniques are sophisticated, making them a significant threat to the U.S. HPH. HC3 is aware of at least one healthcare entity in the United States that has fallen victim to Trinity ransomware recently.

Report

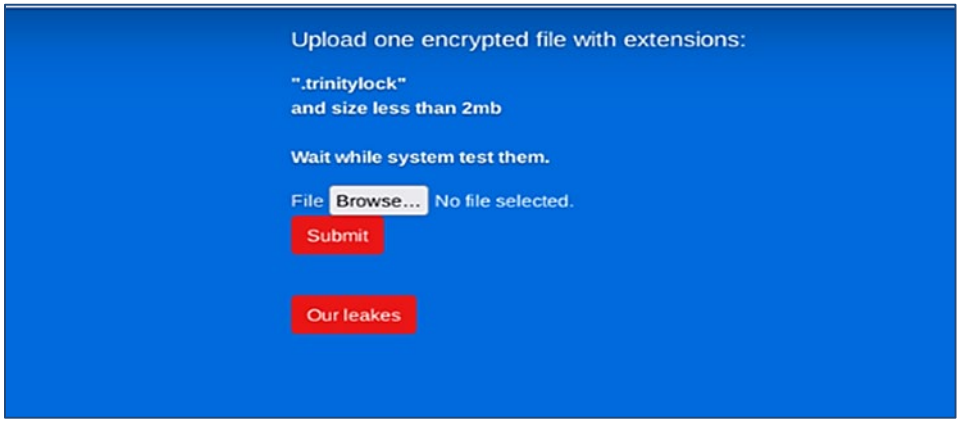
Trinity ransomware was first seen around May 2024. It is a type of malicious software that infiltrates systems through several attack vectors, including phishing emails, malicious websites, and exploitation of software vulnerabilities. Upon installation, Trinity ransomware begins gathering system details such as the number of processors, available threads, and connected drives to optimize its multi-threaded encryption operations. Next, Trinity ransomware will attempt to escalate its privileges by impersonating the token of a legitimate process. This allows it to evade security protocols and protections. Additionally, Trinity ransomware performs network scanning and lateral movement, indicating its ability to spread and carry out attacks across multiple systems in a targeted network.

Once inside the system, Trinity ransomware employs a double extortion strategy to target its victims. It seems to exfiltrate the victim's data before initiating encryption. It encrypts the victim's files using a robust encryption algorithm, rendering them unusable without the correct decryption key. The ransomware typically appends the ".trinitylock" file extension to the affected files, making it clear which ones have been compromised.

Researchers have discovered that Trinity ransomware may share ties with both the Venus and 2023Lock ransomware. Both Trinity and Venus ransomware strains have similarities in their codebase and tactics, including their use of the ChaCha20 encryption algorithm and similar registry values and mutex naming conventions. Researchers have also observed similarities between Trinity ransomware and the 2023Lock ransomware, which has been active since early 2024. The deep similarities between the two variants, like identical ransom notes and code, suggest that Trinity might also be a newer variant of the 2023Lock ransomware. ChaCha20 is a symmetric encryption algorithm that utilizes a 256-bit key for both encrypting and decrypting data. After the encryption process is complete, Trinity ransomware generates a ransom note, in both text and .hta formats, and adjusts the desktop wallpaper via a registry modification. The ransom note is often placed on the desktop or within directories containing the encrypted files. This note contains instructions provided by the threat actor (TA), their onion site URL, and the email address for communication. Trinity's ransom note informs victims that their files have been encrypted and that personal data and databases have been extracted. The attacker then demands a ransom payment in cryptocurrency in exchange for the decryption key. Victims have 24 hours to contact the cybercriminals, and failure to do so will result in the stolen data being leaked or sold. Unfortunately, no known decryption tools are currently available for Trinity ransomware, leaving victims with few options. Some victims,

however, have had limited success by using data recovery tools or consulting cybersecurity professionals to attempt file restoration.

Trinity ransomware uses both a support and data leak site in their operations. The support site allows victims to upload a sample file that is less than 2MB in size for decryption.

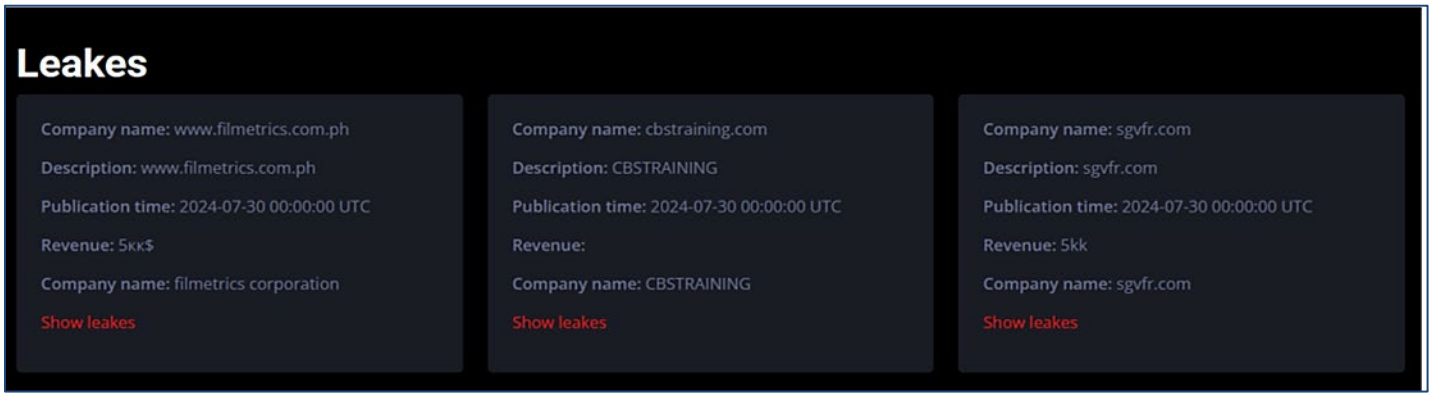


Trinity ransomware victim support site. *Source: CYBLE.COM*

As previously stated, Trinity ransomware employs a double extortion strategy. This involves exfiltrating sensitive data from victims before encrypting it, and then threatening to publish the data if the ransom is not paid. This is a tactic increasingly seen across newer ransomware strains targeting critical industries, particularly healthcare. There has been a total of seven Trinity ransomware victims identified to date. Of these, two victims have been identified as healthcare providers, one based in the United Kingdom, and the other a United States-based gastroenterology services provider, where Trinity claims to have access to 330 GB of the organization's data.

Ransomware Group Data Leak Sites

Data leak sites are websites or portals operated by ransomware groups as part of their double extortion strategy. In this approach, attackers not only encrypt the victim's files, but also steal sensitive data and threaten to publish it on these leak sites if the ransom is not paid. These sites are hosted on the dark web, making them difficult to track and shut down by law enforcement.



Trinity ransomware leak site. *Source: CYJAX.COM*

Key Characteristics of Data Leak Sites:

- **Data Listings:** These sites typically list the names of companies or individuals that have been breached and failed to pay the ransom. They serve as "name-and-shame" platforms, where attackers threaten to release sensitive information, including personal data, financial records, or proprietary business information.
- **Downloadable Data:** Once a victim refuses to pay the ransom, their stolen data is often made available for download on the leak site, either in part or in full, which may include employee records, customer databases, and confidential documents.
- **Tactical Leaks:** In some cases, ransomware groups may leak small portions of data initially to prove they have access to the files. If the victim still refuses to pay, the full set of stolen data may be released.
- **Ransom Negotiation Pages:** Some data leak sites also offer negotiation portals where victims can engage with attackers to discuss the ransom terms or seek extensions.

These data leak sites are an essential part of modern ransomware attacks, leveraging the threat of public exposure to increase pressure on victims to pay the ransom.

Likely TTPs for Trinity Ransomware:

- **Initial Access:**
  - Exploiting vulnerabilities in unpatched software or systems.
  - Phishing attacks with malicious attachments or links.
  - Compromising remote desktop protocol (RDP) endpoints with weak or stolen credentials.
- **Execution:**
  - Running malicious code to infect the system after initial access is gained, often through PowerShell scripts, batch files, or downloaded executable files.
- **Persistence:**
  - Establishing persistence on the infected system by creating registry keys, scheduled tasks, or other mechanisms to survive reboots and ensure long-term access.
- **Privilege Escalation:**
  - Exploiting vulnerabilities or misconfigurations to gain elevated privileges on the system, allowing for broader access and control.
- **Defense Evasion:**
  - Using obfuscation techniques to hide the ransomware payload from security solutions.
  - Disabling security software or tampering with antivirus programs to avoid detection.
- **Credential Access:**
  - Dumping passwords or using keyloggers to gain access to administrator accounts or other sensitive credentials.
- **Discovery:**
  - Scanning the local network to identify other systems to spread the ransomware to, increasing the impact of the attack.
  - Identifying backup solutions and other key data repositories to ensure maximum damage.
- **Lateral Movement:**
  - Spreading the ransomware laterally through the organization’s network to infect as many systems as possible.
- **Data Encryption:**

- Encrypting files using robust encryption algorithms (often RSA or AES).
- Encrypting backup files or network shares to maximize the effect.

- **Double Extortion Exfiltration:**
  - Extracting sensitive data before encryption, threatening to leak it unless a ransom is paid.
- **Impact:**
  - Rendering systems inoperable by encrypting critical files, halting business operations.
  - Demanding ransom payment, typically in cryptocurrency, in exchange for the decryption key.

Trinity Threat Actor Communications

Typed	Indicator
Email Address	wehaveyourdata (@) onionmail.org
TOR URL	hxxp://xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx[.]onion

Trinity MITRE ATT&CK® Tactics, Techniques, Procedures

TACTIC	TECHNIQUE	PROCEDURE
Execution	T1204.002 (User Execution)	Malicious file
Defense Evasion	T1134 (Access Token Manipulation)	Impersonates tokens
Defense Evasion	T1140 (Deobfuscate/Decode Files or Information)	The binary contains encrypted strings
Discovery	T1083 (File and Directory Discovery)	Ransomware enumerates folders for file encryption
Lateral Movement	T1570 (Lateral Tool Transfer)	Enumerates network shares and scans the network
Impact	T1486 (Data Encrypted for Impact)	Ransomware encrypts the data for extortion
Impact	T1491.001 (Defacement: Internal Defacement)	Changes desktop wallpaper
Impact	T1490 (Inhibit System Recovery)	Removes shadow copies

Trinity Indicators of Compromise (IOCs)

WHAT	IOC
MD5	949c438e4ed541877dce02b38bf593ad
SHA1	4c58d2d624d9bdf6b14a6f8563788785074947a7
SHA256	36696ba25bdc8df0612b638430a70e5ff6c5f9e75517ad401727be03b26d8ec4

HC3: Threat Actor Profile

October 4, 2024 TLP:CLEAR Report: 202410041500

YARA Rule

```
rule Trinity {
meta:
author = "Cyble Research and Intelligence Labs"
description = "Detects Trinity Ransomware"
date = "2024-05-10"
os = "Windows"
strings:
$a1 = "pbsecGOOD" ascii fullword
$a2 = "secpbGOOD" ascii fullword
$b1 = "Wallaper" fullword ascii
$b2 = "wehaveyourdata@onionmail.org" fullword nocase ascii wide condition:
                all of them
}
```

Mitigations

HC3 recommends the following mitigations for ransomware:

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location.
- Implement network segmentation and maintain offline backups of data to ensure limited interruption to the organization.
- Regularly back up data and password-protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Install and regularly update antivirus software on all hosts and enable real time detection.
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails; Disable unused ports.
- Enforce multi-factor authentication (MFA) and consider MFA for securing RDP access while placing RDP behind a Virtual Private Network (VPN).
- Use National Institute for Standards and Technology (NIST) standards for developing and managing password policies. Require administrator credentials to install software.
- Consider implementing rate limiting to slow down the speed that attackers can guess logins.

Analyst Comment

Multiple ransomware variants have adopted a double extortion strategy, escalating ransomware tactics. By threatening to release sensitive data in addition to encrypting files, threat actors exponentially increase the pressure on victims to pay ransom demands. Furthermore, the identification of Trinity's similarities with other ransomware variants, such as 2023Lock and Venus, suggests a potential link or collaboration among threat actor groups. This collaboration could lead to the exchange of techniques, tools, and infrastructure, amplifying the scale and sophistication of future ransomware campaigns.

Relevant HC3 Products

Venus Ransomware Targets Publicly Exposed Remote Desktop Services
https://www.hhs.gov/sites/default/files/venus-ransomware-analyst-note.pdf

HC3: Threat Actor Profile

October 4, 2024 TLP:CLEAR Report: 202410041500

References

Trinity Ransomware Strikes with the Dual Extortion Strategy
https://hivepro.com/threat-advisory/trinity-ransomware-strikes-with-the-dual-extortion-strategy/

In the Shadow of Venus: Trinity Ransomware's Covert Ties
https://cyble.com/blog/in-the-shadow-of-venus-trinity-ransomwares-covert-ties/

Trinity Ransomware
https://jp.broadcom.com/support/security-center/protection-bulletin/trinity-ransomware

Researchers Observe Potential Ties between Trinity and Venus Ransomware Strains
https://thecyberexpress.com/researchers-note-ties-trinity-ransomware-venus/

Ransomware - TrinityLock
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/trinitylock

In the Shadow of Venus: Trinity Ransomware's Covert Ties
https://www.trukno.com/blog/66431a96d7d7d2084ffdd136

The Menace of Trinity Ransomware: What You Need to Know
https://www.cyclonis.com/remove-trinity-ransomware/

Data-leak site emergence continues to increase
https://www.cyjax.com/data-leak-site-emergence-continues-to-increase/

Trinity Ransomware Hits Cosmetic Dental Group: 3.63 TB Data at Risk
https://ransomwareattacks.halcyon.ai/attacks/trinity-ransomware-hits-cosmetic-dental-group-3-63-tb-data-at-risk

Contact Information

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

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback