TRIAL_RECOVERY RANSOMWARE

Vairav Advisory Report

26th September 2024

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairav.net

EXECUTIVE SUMMARY

Ransomware is a type of malicious software designed to encrypt files on a victim's system and demand a ransom for their decryption. It often targets a wide range of industries, causing significant disruption by locking crucial data behind complex encryption algorithms. Victims are presented with a ransom note, typically instructing them to pay in cryptocurrency in exchange for a decryption key. However, paying the ransom does not guarantee file recovery, and it supports further criminal activity. The report provides a finding on Trial_recovery ransomware, a malicious program that encrypts files on infected systems, appending a unique name and the extension ".-encrypted." The attack process typically involves phishing emails, downloading malicious files, executing those files, encrypting data, and displaying a ransom note. Common distribution methods include infected email attachments, torrent websites, and malicious ads. The report outlines the ransomware's detection names, symptoms, damage, and prevention strategies. Recommendations emphasize the importance of not engaging with scam emails, utilizing updated antivirus software, reporting scams, and educating users about safe online practices.

INTRODUCTION OF CYBER ADVERSARY

Recent ransomware infections involving the Trial_recovery ransomware have surfaced, notably using file extensions like ".-encrypted" following random characters. Trial_recovery ransomware is a malicious program designed to encrypt files appending a unique name to each locked file on the victim's system and demanding a ransom for their decryption. It also exfiltrates sensitive data, threatening to sell the stolen information unless the victim pays the ransom. In most ransomware cases, decryption is only possible with the attackers' help, and flawed ransomware is a rare exception. Victims often fail to receive decryption keys even after paying the ransom, so it's best to avoid compliance, as recovery isn't guaranteed, and it fuels criminal activity. Removing Trial_recovery ransomware will stop further encryption, but it won't restore compromised files. The only recovery option is to restore from a pre-existing backup stored separately. This ransomware operates similarly to a variant known as "Available_for_trial".

The key characteristics of the trial_recovery ransomware include:

File Renaming: It appends a specific pattern to encrypted files, such as "[random_string].[random_string].-encrypted". For example, a file named "1.jpg" might become "084k0ij61jeb49pxqd.639xzbe.-encrypted."

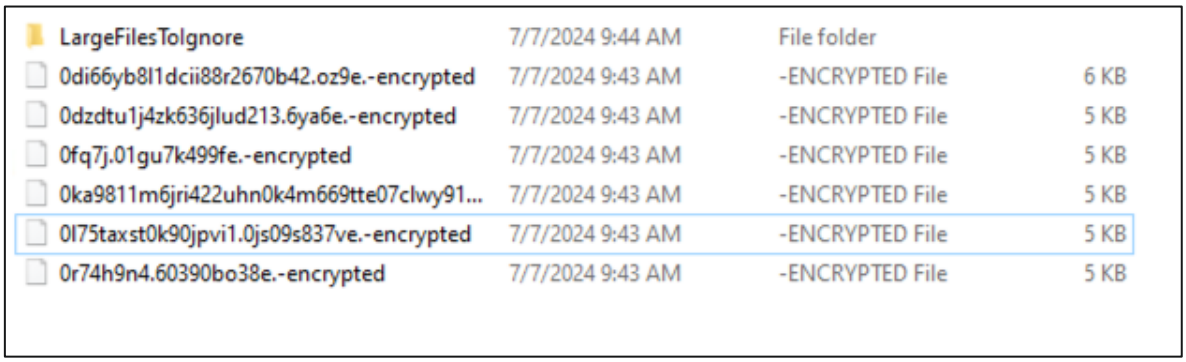
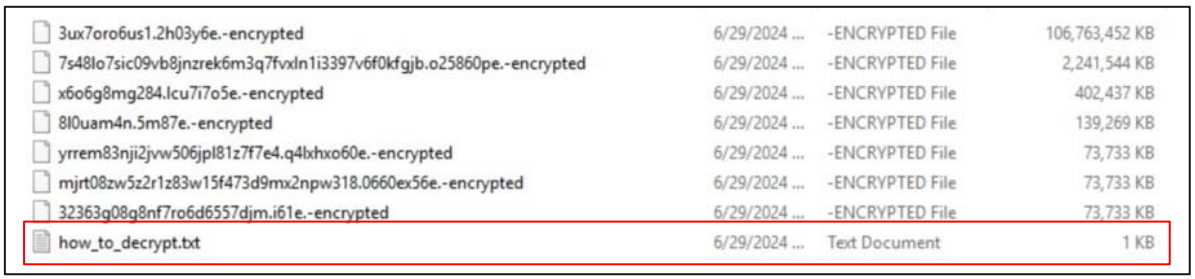


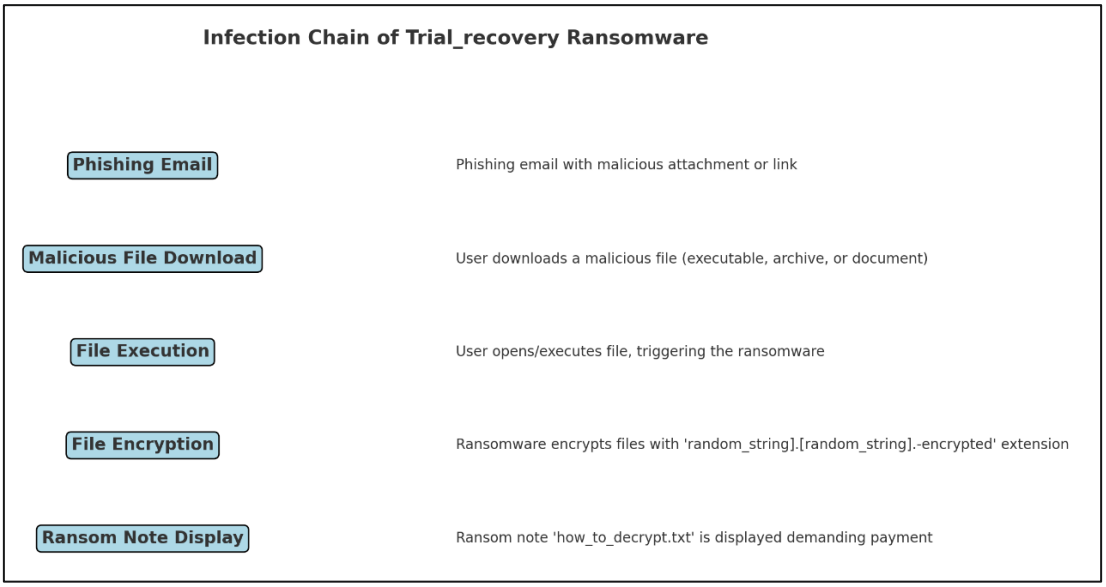
Figure 1: Example of encrypted files.

Ransom Note: A text file titled "how_to_decrypt.txt" is dropped, containing instructions on how to contact the attackers and the ransom demand.



Threats: The ransomware claims to have exfiltrated sensitive data and threatens to sell it unless the victim complies with the payment demand.

ATTACK PROCESS



Trial_recovery ransomware may also pose as legitimate tools, tricking users into installation through fake alerts. It can infect computers through several methods, including spam emails with suspicious links, free hosting resources, hidden installations bundled with freeware, illegal peer-to-peer (P2P) downloads of pirated software, or Trojans disguised as legitimate files. The process that outlines how this ransomware infection spreads is given below:

1. **Initial Access - Phishing Emails:**
   - The attack begins with a phishing email that contains either a malicious attachment (often in the form of a file, such as an executable, a PDF, or a Word document with embedded macros) or a link to a malicious website.
   - These emails are designed to trick the user into believing that the content is legitimate, often using urgent or alarming messages.
2. **Malware Delivery - Downloading Malicious File:**
   - The user downloads the malicious file attached to the email or clicks the embedded link, which redirects to a webpage that initiates the download of a payload.
   - The file could be executable (.exe), a compressed archive (.zip), or a document (.docx) that contains malicious macros.
3. **Execution - File Execution:**
   - The user opens the downloaded file, which executes the malicious code hidden inside.
   - If it's a document, the macros are triggered once the user enables them, leading to the ransomware installation.
   - At this point, Trial_recovery ransomware installs itself in the background.
4. **Ransomware Actions - File Encryption:**
   - Once the ransomware is executed, it begins its primary function: encrypting user files.
   - It appends a unique extension, such as [random_string].[random_string].-encrypted, to all affected files, making them inaccessible to the user.
5. **Extortion - Ransom Note Display:**
   - After file encryption, Trial_recovery ransomware drops a ransom note, usually named something like "how_to_decrypt.txt".
   - The note contains instructions for the victim, demanding a ransom (typically in cryptocurrency) in exchange for the decryption key to restore the locked files.

```
 ATTENTION!!!!

Your computer ID: -

ATTENTION to representatives MASS!!!!

Your system has been tested for security and unfortunately your system was
vulnerable.

We specialize in file encryption and industrial (economic or corporate) espionage.

We don't care about your files or what you do, nothing personal - it's just
business.

We recommend contacting us as your confidential files have been stolen and will be
sold to interested parties unless you pay to remove them from our clouds and
auction,

or decrypt your files.

For more detailed information write to us: varentsujikyuke@mail.com

Telegram: hxxps://t.me/BlackNevas

Reserve Email: widemoucerpco@mail.com

Your computer ID: -
```

Figure 2: Ransom note content

THREAT SUMMARY

Attribute	Details
Name	Trial_recovery
Threat Type	Ransomware, Crypto Virus, Files locker
Detection Names	Avast: Win32:Evo-gen [Trj] Combo Cleaner: Gen:Variant.Cerbu.196226 ESET-NOD32: A Variant of Win32/Filecoder.Trigona.B Kaspersky: HEUR:Trojan-Ransom.Win32.Generic Microsoft: Ransom:Win32/Trigona.ATR!MTB
Symptoms	Inability to open files on your computer.
	Files have a modified extension (e.g., "084k0ij61jeb49pxqd.639xzbe.-encrypted").
	A ransom demand message displayed on the desktop.
	Payment is requested in Bitcoin to unlock files.
Distribution Methods	Infected email attachments (with macros).
	Torrent websites.
	Malicious advertisements.
Damage	All files are encrypted and inaccessible without ransom payment.
	Potential installation of additional malware, including password-stealing trojans
Prevention and Response	Do not respond to scam emails.
	Use updated antivirus software to detect and block ransomware.
	Report scams to law enforcement and cybercrime units.
	Educate users on safe browsing practices and the risks of downloading from untrusted sites.
	Implement and update security measures.
	Avoid clicking on suspicious links or downloading attachments from unknown sources.

VAIRAV RECOMMENDATIONS

We strongly recommend implementing the following comprehensive procedures to effectively mitigate and prevent ransomware attacks:

Conduct Regular Data Backups: Regular data backups are crucial as they provide a reliable means of restoring data in the event of a ransomware attack. By consistently backing up important information, you ensure that even if files are encrypted by ransomware, they can be restored from a secure backup source. It is advisable to use offline or isolated network storage solutions to keep backups protected during an attack.

Establish an Incident Response Plan: Having a clearly defined incident response strategy in place before facing a ransomware attack is essential. This plan should detail specific procedures and responsibilities for isolating compromised systems, notifying key stakeholders, and initiating the recovery process. Organizations with a pre-established and practiced response plan can minimize downtime, contain the attack, and quickly resume normal operations.

Limit Execution of Files from Untrusted Sources: Ransomware often infiltrates organizations through malicious email attachments, dubious website downloads, or pirated software. Enforcing strict security measures, such as application whitelisting or sandboxing, to prevent the execution of files from untrusted sources adds a layer of protection and reduces the risk of harmful code execution.

Keep Systems and Software Updated: Regularly updating operating systems, software applications, and firmware is vital to address security vulnerabilities that ransomware attackers may exploit. Software vendors release updates and patches to resolve known issues, so staying current is essential for maintaining a secure computing environment.

Adopt the Least Privilege Principle: The least privilege principle ensures that employees receive only the access rights necessary to perform their job functions. By restricting access to critical systems and sensitive data, organizations can reduce the attack surface for ransomware. Limiting user permissions can minimize damage and prevent lateral movement across the network in the event of a successful ransomware attack.

Utilize Strong Antivirus and Anti-Malware Solutions: Deploying reputable antivirus and anti-malware software provides an additional layer of protection against ransomware. These tools help detect and prevent harmful files and actions, including known ransomware

threats. Regular updates ensure that you have the latest virus definitions to identify and thwart emerging threats.

Implement Multi-Factor Authentication (MFA): Multi-factor authentication enhances the security of organizational systems and accounts. By requiring multiple authentication factors, such as a password and a unique verification code, MFA helps prevent unauthorized access even if a user's credentials are compromised. This significantly reduces the likelihood of attackers gaining control over critical systems and data.

Activate Firewalls and Intrusion Detection/Prevention Systems: Firewalls act as a barrier between the internal network and external threats. Configuring firewalls to monitor and filter incoming and outgoing network traffic helps prevent unauthorized access and suspicious connections. They track network activity for indicators of malicious behavior and respond promptly to thwart potential ransomware attacks.

It is important to recognize that cyber adversaries involved in ransomware operations continually evolve their methods, tools, and techniques to evade detection and maintain successful attacks. Therefore, organizations and individuals must stay informed about the latest tactics, techniques, and procedures (TTPs) used by ransomware groups like 8Base and take proactive measures to safeguard themselves.

CONCLUSION

Stay vigilant and informed about potential scams. Vairav SOC prioritizes delivering timely and accurate information to protect your digital security. Our commitment ensures that you receive the necessary support to safeguard your digital assets. Should you have any concerns or require assistance, please do not hesitate to reach out to our dedicated support team. Your proactive approach and timely reporting play a crucial role in mitigating these malicious activities and enhancing overall cybersecurity measures.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairav.net

Website: https://vairav.net