Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

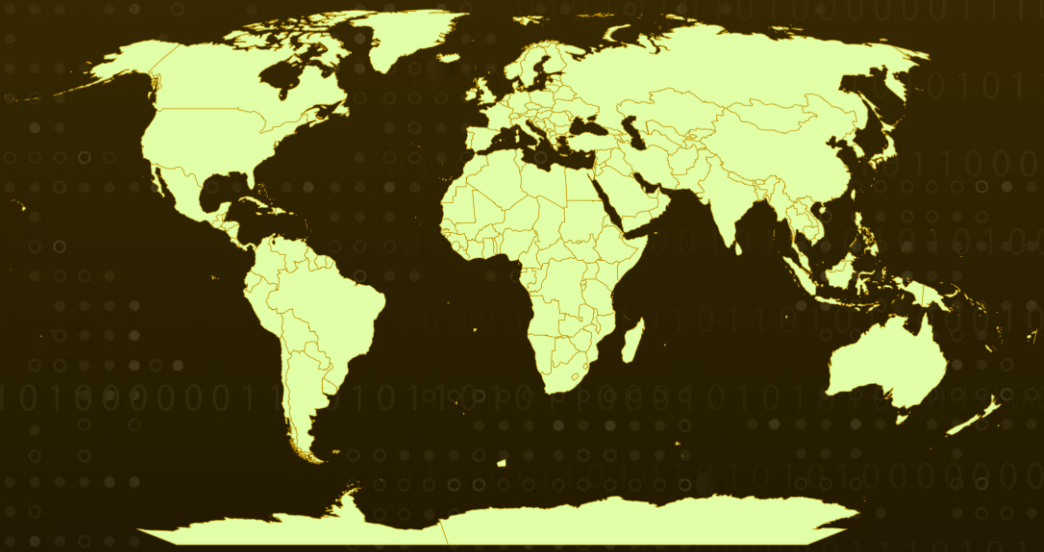
Rancoz Ransomware Employs Advanced Techniques to Encrypt Victims' Files

Date of Publication	Admiralty Code	TA Number
May 17, 2023	A1	TA2023232

Summary

Date: May 11, 2023
Attack Country: Worldwide
Malware: Rancoz ransomware
Attack: Rancoz ransomware demonstrates the growing danger of tailored ransomware strains, leveraging advanced encryption techniques, double extortion tactics, and destructive actions to coerce victims into paying the ransom and increasing the difficulty of mitigation and analysis.

⚔ Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 Rancoz ransomware is a newly discovered variant that exhibits similarities to Vice Society ransomware. It employs advanced techniques to encrypt victims' files and extract ransom payments. By modifying existing code from leaked source codes, threat actors tailor the ransomware to target specific industries, organizations, or geographic regions, enabling them to evade detection and increase the effectiveness of their attacks.

#2 Once executed, Rancoz ransomware inspects command line arguments and proceeds with its default execution if no valid arguments are provided. It employs a double extortion technique, encrypting the victim's data and threatening to leak stolen information on a designated site, thereby pressuring victims to pay the ransom.

#3 Rancoz ransomware carries out destructive actions, such as deleting Shadow Copies, removing Remote Desktop Connection values from the Windows Registry, deleting the default Remote Desktop Protocol configuration file, and erasing Windows event logs. These actions hinder recovery and analysis efforts.

#4 Using multi-threading, Rancoz encrypts files using the ChaCha20-Poly algorithm for symmetric encryption and the NTRUEncrypt algorithm for asymmetric encryption. Certain folders and file extensions are excluded from encryption to preserve critical system files.

#5 The ransomware modifies the victim's desktop background and drops a ransom note titled "HOW_TO_RECOVERY_FILES.txt" in encrypted directories. The note provides instructions for contacting the threat actors and paying the ransom for file recovery. The discovery of Rancoz ransomware highlights the ongoing threat of customized ransomware variants.

Recommendations

Implement Strong Cybersecurity Measures: To protect against Rancoz ransomware and similar threats, it is crucial to have robust cybersecurity measures in place. This includes using reliable and up-to-date antivirus and anti-malware software, conducting regular system updates and patching, and employing intrusion detection and prevention systems.

Regularly Backup Data: Implement a comprehensive data backup strategy that includes regular and secure backups of critical files and systems. This ensures that even if Rancoz ransomware or any other malware infects your system, you can restore your data without paying the ransom. Backups should be stored offline or in secure, isolated environments to prevent unauthorized access.

Educate and Train Employees: Human error is often a weak point in cybersecurity defenses. It is essential to educate and train employees on best practices for cybersecurity, including how to identify and avoid phishing emails, suspicious websites, and malicious attachments. Regular security awareness training helps create a security-conscious culture and reduces the likelihood of employees inadvertently triggering ransomware infections.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0007** Discovery	**TA0005** Defense Evasion	**TA0040** Impact
T1059 Command and Scripting Interpreter	**T1204** User Execution	**T1082** System Information Discovery	**T1135** Network Share Discovery
T1083 File and Directory Discovery	**T1070** Indicator Removal	**T1486** Data Encrypted for Impact	**T1490** Inhibit System Recovery

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	8d9f3e223f8d5e350b87dc0908fee0a5
SHA1	9fe3060e5cbe3a9ab6c3fb3dee40bd6cd385a6f6
SHA256	b95a4443bb8bff80d927ac551a9a5a5cfac3e3e03a5b5737c0e05c75f33ad61e

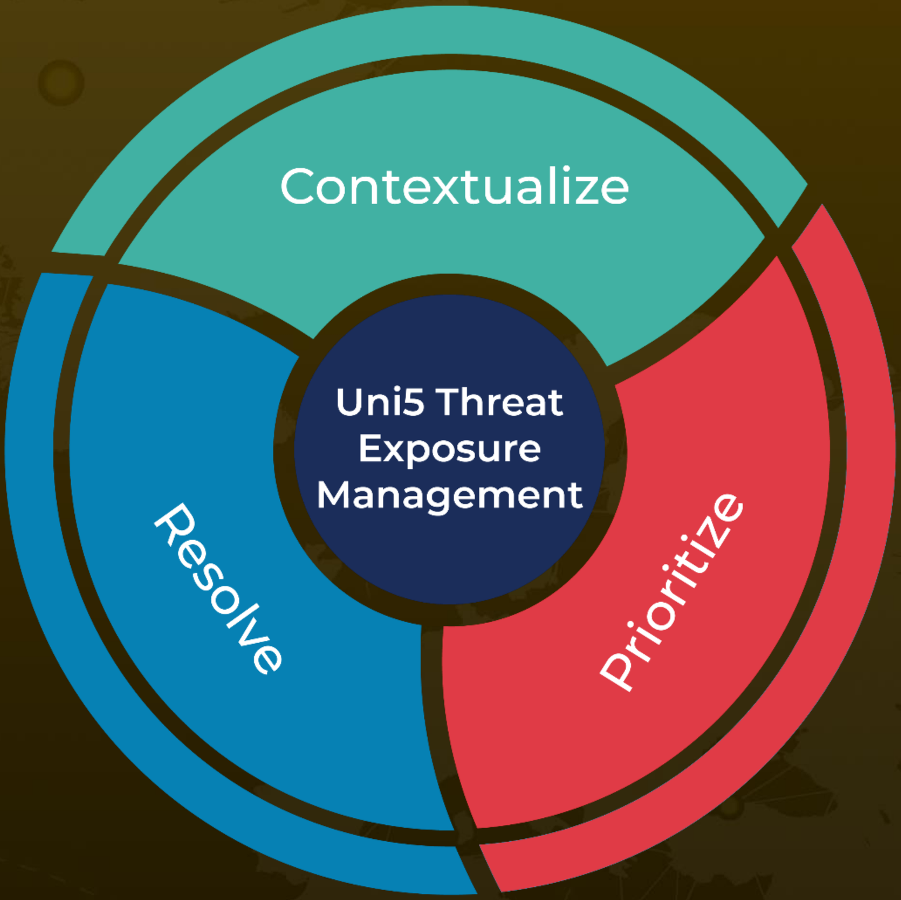
References

https://blog.cyble.com/2023/05/11/dissecting-rancoz-ransomware/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 17, 2023 • 1:30 AM

More at www.hivepro.com