Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

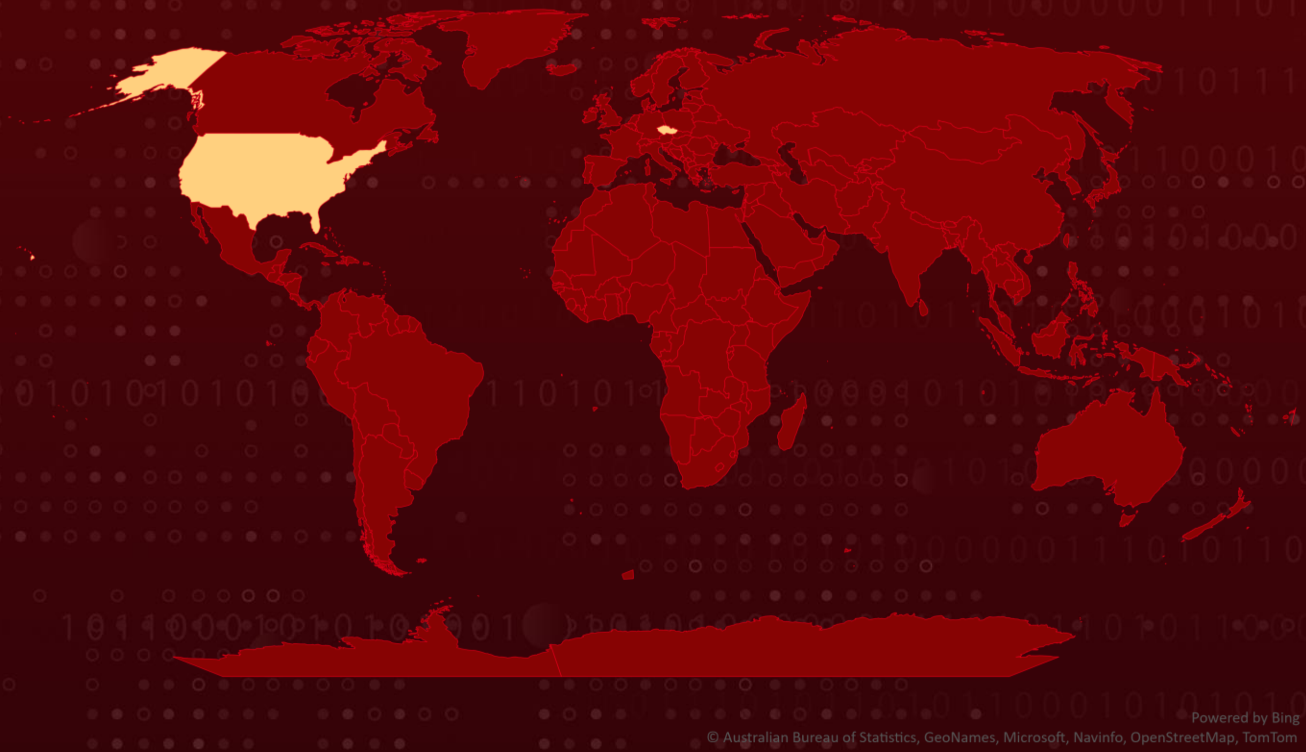
Unveiling New Windows Ransomware Named Trash Panda

Date of Publication	Admiralty Code	TA Number
August 29, 2023	A1	TA2023349

Summary

First Appearance: August, 2023
Attack Region: United States and the Czech Republic
Affected Platform: Windows
Malware: Trash Panda ransomware
Attack: Trash Panda is a ransomware that encrypts files on Windows machines, replaces the desktop wallpaper, and drops a ransom note with political messages. It adds a '.monochrome' extension to the encrypted files and demands payment for decryption.

Attack Regions


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

Attack Details

#1

Trash Panda is a ransomware strain that emerged in early August, specifically targeting Windows platforms. Upon infection, Trash Panda encrypts files on compromised machines and changes the desktop wallpaper. It appends a ".monochromebear" extension to the encrypted files. The ransomware displays a politically themed ransom note that demands payment for file decryption. The note hints at potential motives behind the attack and the targeted country.

#2

Trash Panda ransomware samples have been observed in the United States and the Czech Republic. The ransomware avoids encrypting files with certain extensions, likely to maintain system functionality. The attack prompts victims to check the provided readme file for further instructions. The ransom note demands payment in exchange for the decryption key, suggesting a potential political agenda.

Recommendations

Keep your systems and software up to date: Regularly install updates for your operating system, applications, and security software. This helps patch vulnerabilities that adversaries can exploit.

Conduct Regular Data Backups: Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.

Install Antivirus and Antimalware Software: Use reputable security software that can detect and prevent ransomware infections. Keep the software definitions updated regularly.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0005 Defense Evasion	TA0001 Initial Access	TA0002 Execution
T1486 Data Encrypted for Impact	T1036 Masquerading	T1059 Command and Scripting Interpreter	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	D5d37ae269008e9bfddc171c3b05bd3d43a5cd4d
SHA256	ce5cf3b964e636d546bf2c52423296bda06b7fe47e6f8a757f165a3be93c88db
MD5	A0fea954561663f60059420e6c78fa5c

References

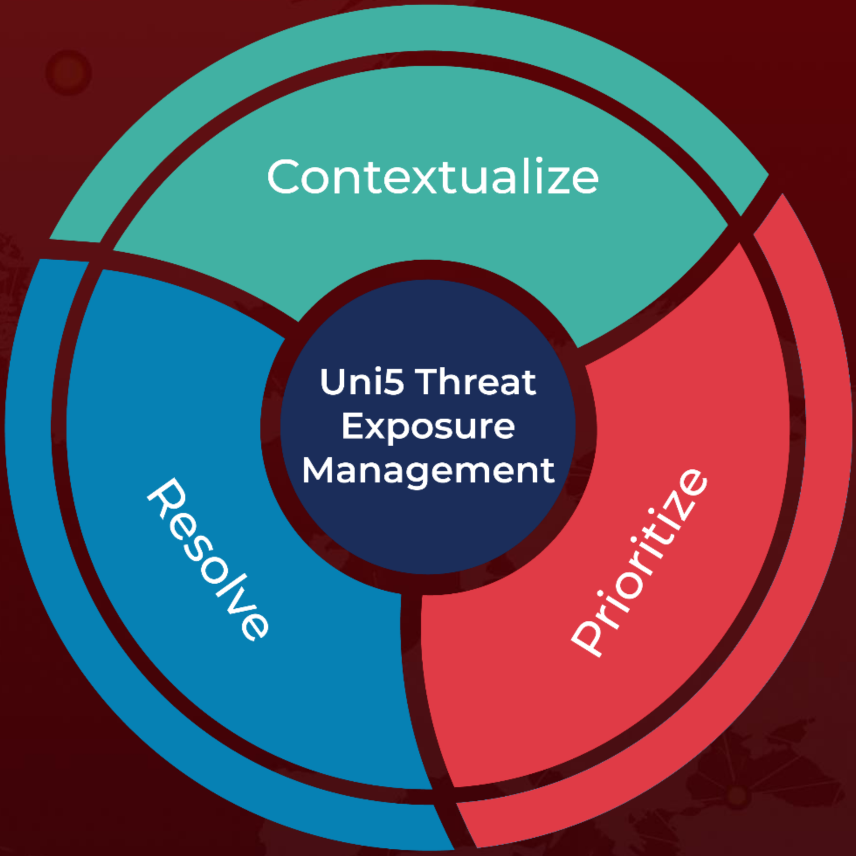
https://www.fortinet.com/blog/threat-research/ransomware-roundup-trash-panda-and-nocry-variant

https://howtofix.guide/trash-panda-virus/

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

August 29, 2023 • 7:30 AM

More at www.hivepro.com