Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

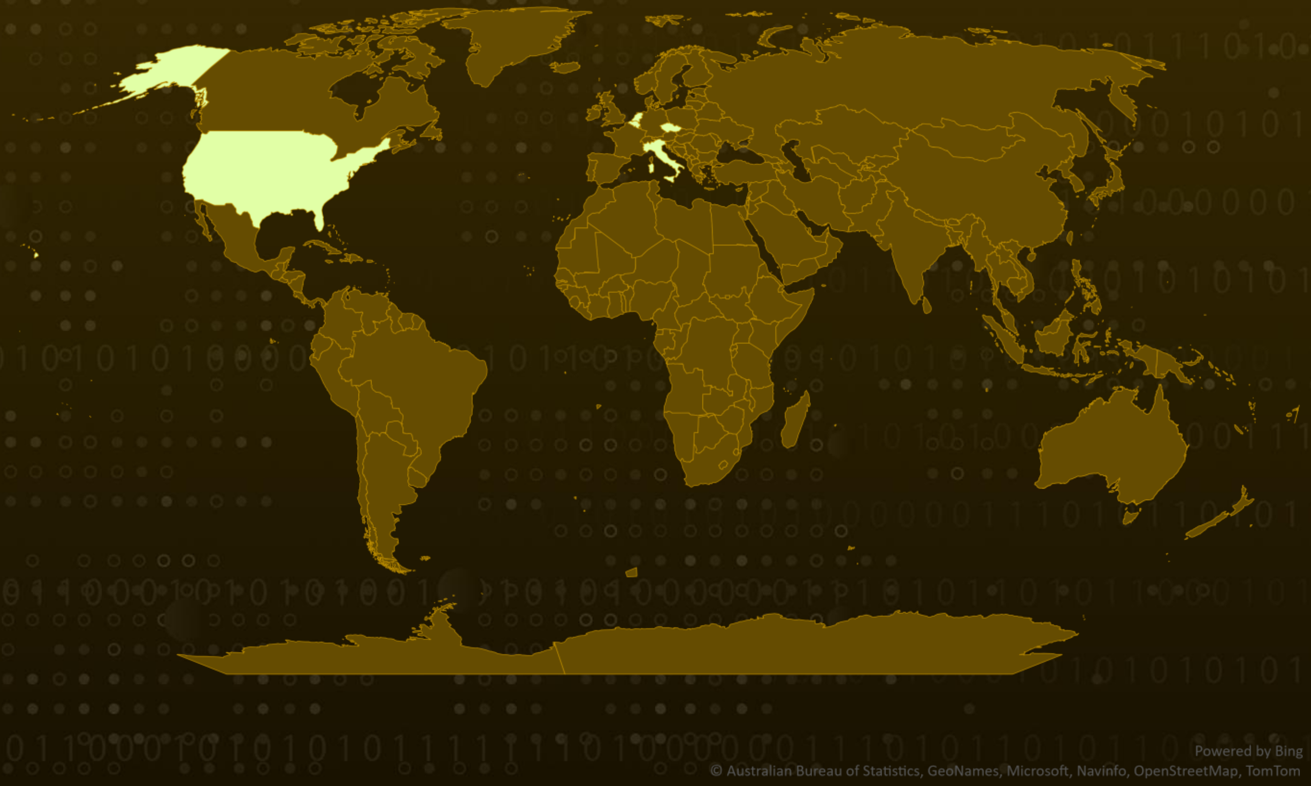
KageNoHitobito and DoNex Ransomware Plaguing Global Entities

Date of Publication	Admiralty Code	TA Number
April 26, 2024	A1	TA2024165

Summary

First Seen: March 2024
Malware: KageNoHitobito ransomware, DoNex Ransomware
Affected Platform: Microsoft Windows
Attack Region: Belgium, Czech Republic, Italy, Netherlands, United States
Attack: In March 2024, two distinct ransomware strains emerged: KageNoHitobito and DoNex. The entities purportedly impacted by these ransomware attacks are situated in parts of Europe and North America.

Attack Regions



Attack Details

#1 In March 2024, the KageNoHitobito ransomware surfaced, its initial infiltration method veiled in secrecy. Originating from Japanese, "KageNoHitobito" translates to "shadow people."

#2 Operating in line with typical ransomware tactics, this malicious software encrypts files on victims' systems, compelling them to pay a ransom for decryption, as conveyed through dropped ransom notes named "KageNoHitobito_ReadMe.txt." The encrypted files carry the distinct ".hitobito" extension, with the ransomware specifically targeting files within the local drive.

#3 A recently emerged ransomware group motivated by financial gain, identified as DoNex, has emerged. Unlike its forerunner, DoNex boasts a wider scope, encrypting files on local drives and network shares.

#4 It attaches a unique victim ID as a file extension to the compromised files and alters their icons. Additionally, DoNex is programmed to eliminate shadow copies before issuing a ransom demand, typically communicated through a ransom note prompting contact via TOR sites, TOX chat, or email.

#5 Significantly, DoNex ransomware shares striking similarities with DarkRace, employing a parallel ransom note format and utilizing identical configuration files.

Recommendations

Robust Backup Strategies: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Disable Unnecessary Services: Review and disable unnecessary services and features on systems to minimize potential attack vectors. Restrict user privileges to limit the impact of potential breaches.

Continuous Monitoring and Analysis: Implement continuous monitoring and analysis of network traffic and system logs. This proactive approach can help identify anomalies and potential threats before they escalate.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0040 Impact
TA0010 Exfiltration	T1059 Command and Scripting Interpreter	T1056 Input Capture	T1055 Process Injection
T1010 Application Window Discovery	T1018 Remote System Discovery	T1057 Process Discovery	T1082 System Information Discovery
T1083 File and Directory Discovery	T1041 Exfiltration Over C2 Channel	T1518.001 Security Software Discovery	T1486 Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	8939bfe20bc6476806d22c8edfcaba5c36f936b893b3de1c847558502654c82f, 1940fcdb2561c2f7b82f6c44d22a9906e5ffec2438d5dadfe88d1608f5f03c33,

TYPE	VALUE
SHA256	506e8753dd5ca1c8387be32f26367e26f242b7c65e61203f7f926506c04163aa, 8a10e0dc4994268ea33baecd5e89d1e2ddabef30afa099612557a4329669e857a, bec9d2dcd9565bb245f5c8beca4db627390bcb4699dd5da192cc8aba895e0e6a, 0adde4246aaa9fb3964d1d6cf3c29b1b13074015b250eb8e5591339f92e1e3ca, 6d6134adfdf16c8ed9513aba40845b15bd314e085ef1d6bd20040afd42e36e40, b32ae94b32bcc5724d706421f915b7f7730c4fb20b04f5ab0ca830dc88dcce4e, 74b5e2d90daaf96657e4d3d800bb20bf189bb2cf487479ea0facaf6182e0d1d3, 0e60d49a967599fab179f8c885d91db25016be996d66a4e00cbb197e5085efa4

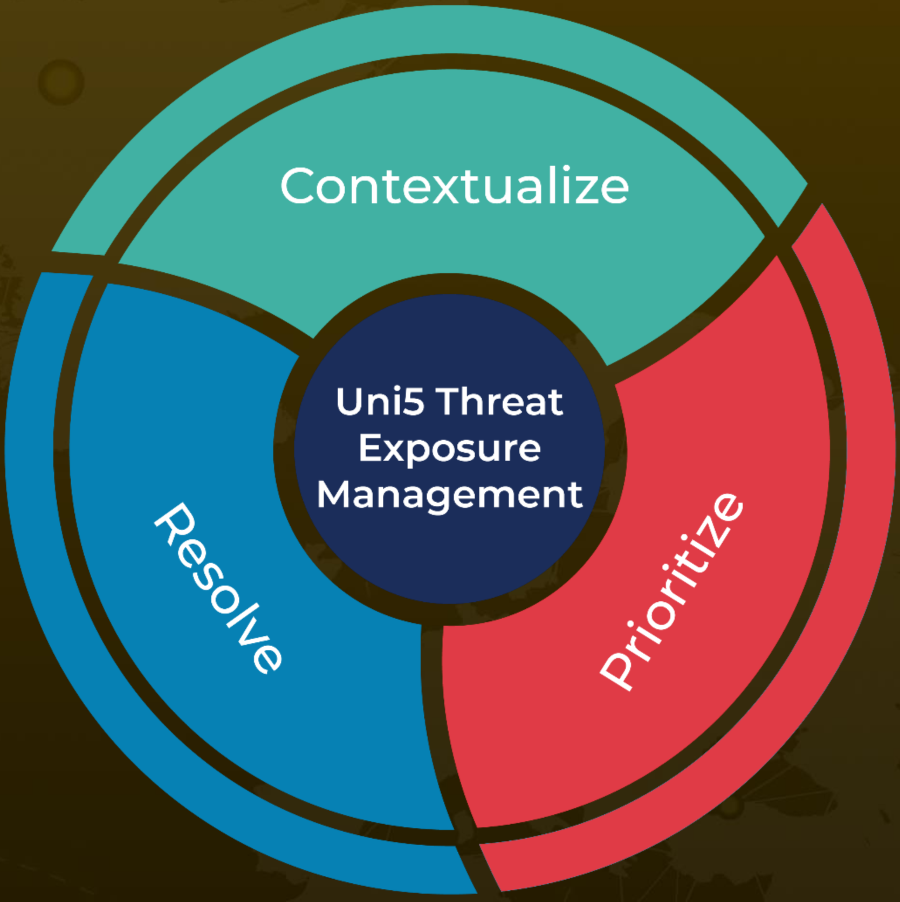
References

https://www.fortinet.com/blog/threat-research/ransomware-roundup-keganohitobito-and-donex

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

April 26, 2024 • 6:00 AM

More at www.hivepro.com