Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Kadavro Vector Ransomware spread as a fake Tor browser installer

Date of Publication	Admiralty Code	TA Number
April 17, 2023	A1	TA2023189

Summary

First appeared: 2023
Malware: Kadavro Vector Ransomware
Affected Product: Microsoft Windows
Attack Region: Worldwide
Attack: Kadavro Vector is a specific variation of NoCry ransomware that utilizes encryption to lock files on machines that have been compromised. The attackers then demand payment in Monero (XMR) cryptocurrency in exchange for the decryption of the files.

Attack Regions

Attack Details

#1

Recent Kadavro Vector ransomware strains are disseminated as a fake Tor browser installer. Once launched, the Kadavro Vector ransomware encrypts files on compromised PCs and appends them a “.vector_” extension. The Kadavro Vector ransomware then places an interactive ransom message on the victim's desktop, demanding $250 in Monero to decrypt the victim's files. The ransom note from Kadavro Vector is available in three languages: English, Russian, and Norwegian. Victims are given four chances to enter a decryption key that is allegedly delivered once the ransom is paid.

#2

The decryption screen cautions that after four attempts, the encrypted files would be lost. The older Kadavro Vector variant encrypts files on compromised machines, and the ".tor" extension is appended to this older variant. Additionally, one of the most current Kadavro Vector samples refers to a Pastebin page for a ngrok address. "Ngrok" is a valid and user-friendly reverse proxy tool that allows developers to expose local services to the internet. Threat actors frequently exploit ngrok's tunneling features for C2 communication.

Recommendations

To protect against such attacks, it is recommended that businesses remain vigilant and take necessary precautions. Routine education and awareness training may not fully account for MFA fatigue and web browser hygiene, so it is important to integrate and communicate all lessons learned. Additionally, verifying the authenticity of email attachments and untrusted links before opening them is crucial.

To minimize the risk of ransomware infection, it is recommended to download software only from official and trusted sources, while avoiding third-party downloaders, suspicious websites, and similar sources. To ensure the safety of important data, conduct regular offline backups and install reputable anti-virus and Internet security software on all connected devices. It is also advised to turn on automatic software updates whenever possible and practical. Moreover, consider implementing proactive security measures like blocking indicators of compromise (IoCs) to stay ahead of potential threats.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**TA0008** Lateral Movement	**TA0009** Collection	**TA0040** Impact
T1047 Windows Management Instrumentation	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1036** Masquerading
T1027 Obfuscated Files or Information	**T1027.002** Software Packing	**T1140** Deobfuscate/Decode Files or Information	**T1497** Virtualization/Sandbox Evasion
T1562 Impair Defenses	**T1562.001** Disable or Modify Tools	**T1497.001** System Checks	**T1056** Input Capture
T1005 Data from Local System	**T1082** System Information Discovery	**T1071** Application Layer Protocol	**T1486** Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	8dc6ff90357e8e2d598bebe3240cefabe22054036ec2e2e91377c7125f8f8b89,39308dee3ad1f5ce7ccc3d52b3783db204d12694d6c00ec7ec301ecb73e7c8b6,b30ef4dbcc89cd4bf0da3e7787f43e42023ddc2b5f0bb4f24937538e10e17533,b7ca2dde7789da13d1b8729cc2ef3d5dc596cbd710a06c17ff6eb4ef2d9d1182,124c17b099d8c09db4bd82b5ef3d41cea61727a480abfd56a943208d858ea8cf,e6e62b3fd2be817c41537b9e3244a40b052e78e826b87c77d1bfdfa1644be199,af19fd4147c2253070e345cfcef86b1236c759911ff6b1ef90955d2e86cb8aa4,8ea5398c46a9a53f15d94a6c627ac591aa13bd2f2ac2cd35c9022c8e4dfa43fe,7694bfd321345364659539de8b4664e5d0cba8bc137b007089c63ec12e32f4d9,a076adcf9a2c8298549c22e5059cc5cd90ddc65abadaec417c3dcc74d9ce484b,2ed272aaa05d80a8504772192d5fc99035e5634e8fc306d0a3e09593c466e969

TYPE	VALUE
Pastebin Address	124c17b099d8c09db4bd82b5ef3d41cea61727a480abfd56a943208d858ea8cf,e6e62b3fd2be817c41537b9e3244a40b052e78e826b87c77d1bfdfa1644be199,af19fd4147c2253070e345cfcef86b1236c759911ff6b1ef90955d2e86cb8aa4,8ea5398c46a9a53f15d94a6c627ac591aa13bd2f2ac2cd35c9022c8e4dfa43fe,7694bfd321345364659539de8b4664e5d0cba8bc137b007089c63ec12e32f4d9,a076adcf9a2c8298549c22e5059cc5cd90ddc65abadaec417c3dcc74d9ce484b,2ed272aaa05d80a8504772192d5fc99035e5634e8fc306d0a3e09593c466e969

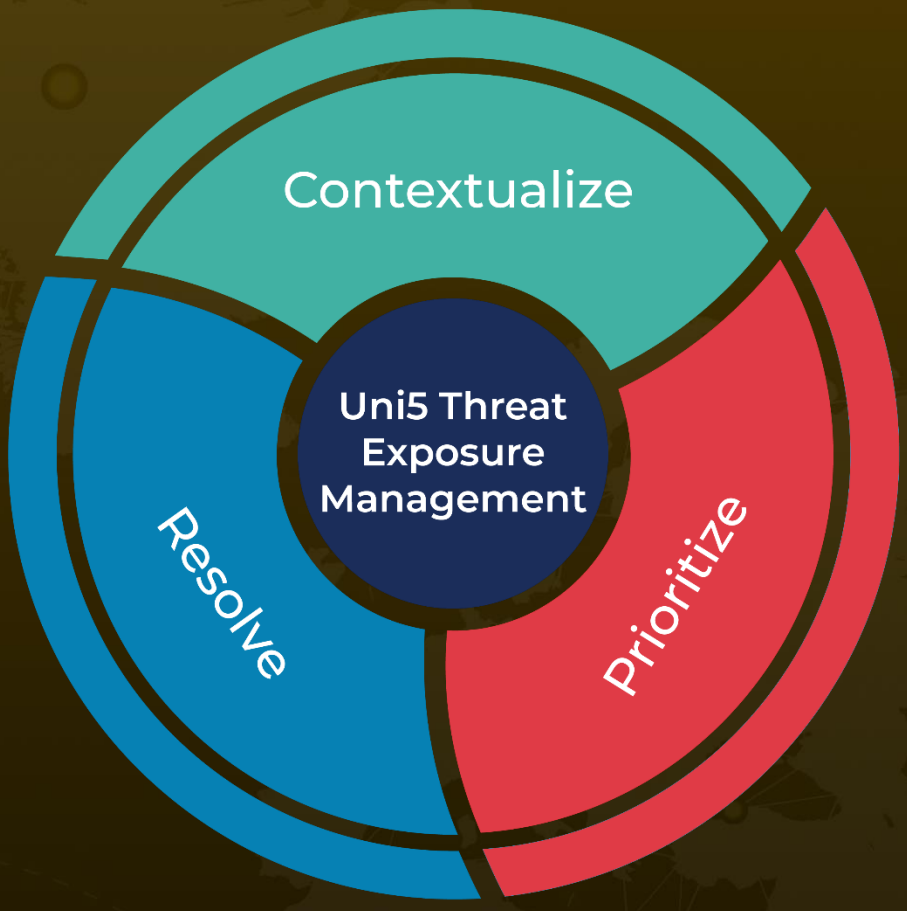
References

https://www.fortinet.com/blog/threat-research/ransomware-roundup-kadavro-vector-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

April 17, 2023 • 7:25 AM

More at www.hivepro.com