Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Kanti Ransomware Strikes Cryptocurrency Users

Date of Publication	Admiralty Code	TA Number
July 21, 2023	A1	TA2023308

Summary

First Seen: July 2023
Malware: Kanti ransomware
Targeted Industry: Cryptocurrency
Attack Region: Worldwide
Affected Platforms: Windows and Linux
Attack: Kanti is a novel strain of ransomware that has been specifically designed to target cryptocurrency users. This sophisticated ransomware is cunningly crafted to infiltrate systems and encrypt files, particularly those related to crypto wallets, with a particular focus on BTC (Bitcoin) users.

Attack Regions

Attack Details

#1 Kanti ransomware is a sophisticated strain of NIM-Based Ransomware that sets itself apart by offering cross-platform support. It skillfully compiles code into executable files, ensuring compatibility with both Windows and Linux operating systems. Its primary targets are cryptocurrency users, adeptly employing crypto wallet-related file names, with Bitcoin users being of particular interest.

#2 Kanti ransomware employs various distribution channels, such as spam emails and deceptive phishing websites, cunningly aimed at individuals involved in cryptocurrency activities. Once executed, the ransomware which is deftly disguised under incorrect file associations runs a targeted command to directly execute the malicious ransomware binary "Locked_253_BTC.zip".

#3 The ransomware thoroughly scans system volumes, meticulously identifying files and directories slated for encryption. It proceeds to replace the original files with their encrypted counterparts, appending the extension ".kanti". Finally, deletes the ransomware binary and leaves a distinctive mark on its victims' systems by placing a ransom note called "Kanti.html" on the Desktop.

Recommendations

Cryptocurrency users must maintain vigilance against phishing emails and suspicious websites to reduce the risk of falling victim to Kanti ransomware. Exercise caution with untrusted links and email attachments, verifying their authenticity before opening to avoid potential risks and phishing attempts.

Implement regular backup procedures and store the backups offline or on a separate network to safeguard your data against potential ransomware attacks.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0040 Impact	T1204 User Execution	T1059 Command and Scripting Interpreter	T1070 Indicator Removal
T1036 Masquerading	T1082 System Information Discovery	T1083 File and Directory Discovery	T1486 Data Encrypted for Impact
T1566.002 Spearphishing Link	T1566 Phishing	T1070.004 File Deletion	T1036.008 Masquerade File Type

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	48eaf4aec9e5b9d51e8b4a98ac22b8f0ed0f7deadeff333d93e1fdc268abd932, 556d38e14124cedbd9c477ffa3dba03979b347f20046733db51a42638cf68849, ce61f7dad5a1bb7ef8dedb6938b3e6f4fbd4bf991fdd62212578a92c9ae6dec1
SHA1	1e761ae5802cf9085d42cf6d991d7e15ab8976b7, cc0d3593e977845bf6d4e23359b625b43c57e0e0, 3775db152fdf754105ae0b5ced67897209d6203d
MD5	c25e3f897192c324d689d5d3bbd180bb, c82127fd8c4f288ebbe07a12606ff87c, d8b6fe900e0a446d3ff44e967d358700

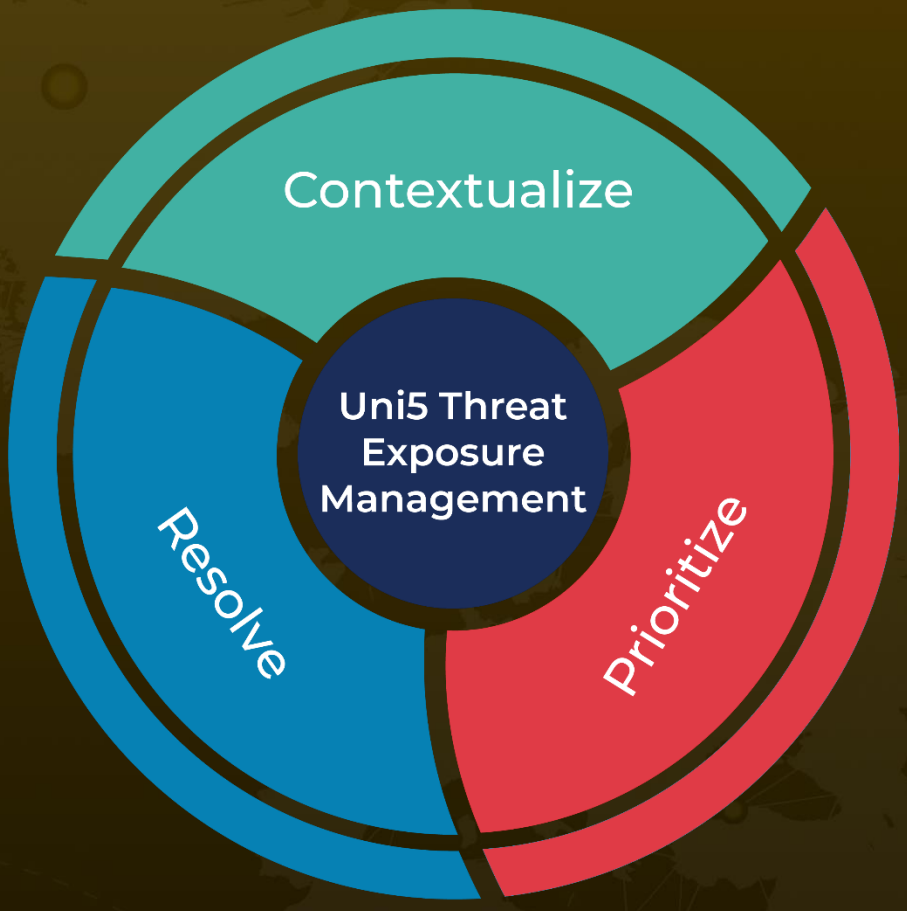
References

https://blog.cyble.com/2023/07/20/kanti-a-nim-based-ransomware-unleashed-in-the-wild/

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

July 21, 2023 • 5:00 AM

More at www.hivepro.com