Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Money Message Ransomware Strikes with Million-Dollar Demands

Date of Publication	Admiralty Code	TA Number
April 7, 2023	A1	TA2023174

Summary

First appeared: March 2023
Threat Actor: Money Message
Malware: Money Message Ransomware
Attack Region: Worldwide
Targeted Industries: BFSI, Transportation and Logistics, Professional Services, Airline, and Education.
Attack: 'Money Message' is a new ransomware group that targets victims all over the world, demanding million-dollar ransoms to avoid data leaks and deliver a decryptor.

Attack Regions

Attack Details

#1

Money Message is a newly identified ransomware group that encrypts on both Windows and Linux operating systems and its approach to target network shares resembles that of the Maze and Petya ransomware. It deploys a double extortion technique, stealing data before encrypting it, to extort ransom from its victims. Notably, they have attacked an Asian airline with almost $1 billion in annual revenue and a Taiwanese PC parts manufacturer, MSI, stealing 1.5TB of data, including source code and databases, and demanding $4,000,000 in ransom payment.

#2

The Money Message ransomware binary is a 32-bit C/C++ executable. The Money Message ransomware takes its configuration parameters from the malware binary's overlay upon execution. When launched, it will remove Shadow Volume Copies. After encrypting the device, the ransomware will generate a ransom letter called "money_message.log", which contains a URL to a TOR negotiation site used to negotiate with the threat actors.

Recommendations

- Businesses must be vigilant and take precautions as necessary to avoid becoming a victim of such attacks. Routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned. It's important to verify the authenticity of email attachments and untrusted links before opening them.

- To safeguard against Money Message Ransomware, it's recommended to conduct regular offline backups and use reputed anti-virus and Internet security software on all connected devices. Additionally, turn on automatic software updates wherever possible and pragmatic and consider implementing proactive security measures like blocking indicators of compromise (IoCs).

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement
TA0040 Impact	T1204 User Execution	T1140 Deobfuscate/Decode Files or Information	T1562 Impair Defenses
T1007 System Service Discovery	T1083 File and Directory Discovery	T1135 Network Share Discovery	T1021 Remote Services
T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp[:]//blogvl7tjyjvsfthobttze52w36wwiz34hrfcmorgvdzb6hikucb7aqd[.]onion hxxp[:]//p6kxp556kkcbjdjsg24g3edmvr7v7ujecuychw4ibvqhl6wuomnrgbqd[.]onion/
SHA256	dc563953f845fb88c6375b3e9311ebed49ce4bcd613f7044989304c8de384dac,4f8bd37851b772ee91ba54b8fd48304a6520d49ea4a81d751570ea67ef0a9904,bbdac308d2b15a4724de7919bf8e9ffa713dea60ae3a482417c44c60012a654b
SHA1	456e5cb1739cb5f29020d1a692289a5af07ce90d 3b4ecff980285461642cc4aef60d4a1b9708453e a85ff9091f298ea2d6823a7b0053daa08b237423
MD5	400fa5d02c1ac704cd290d959b725e67 abe3c3cc45dec9c01762ba3e534564ed 163e651162f292028ca9a8d7f1ed7340

References

https://blog.cyble.com/2023/04/06/demystifying-money-message-ransomware/

https://twitter.com/Threatlabz/status/1641113991824158720

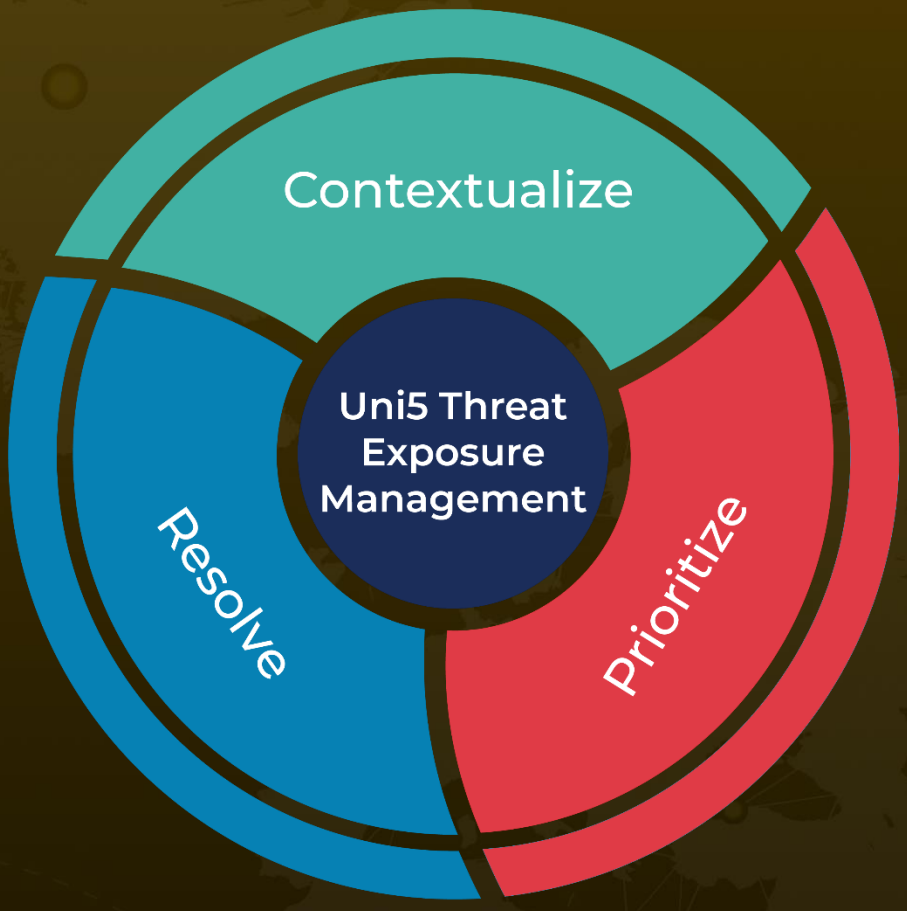
http://pastenet.com/aIw8imWO/

https://www.bleepingcomputer.com/news/security/money-message-ransomware-gang-claims-msi-breach-demands-4-million/

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 7, 2023 • 6:50 AM

More at www.hivepro.com