Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

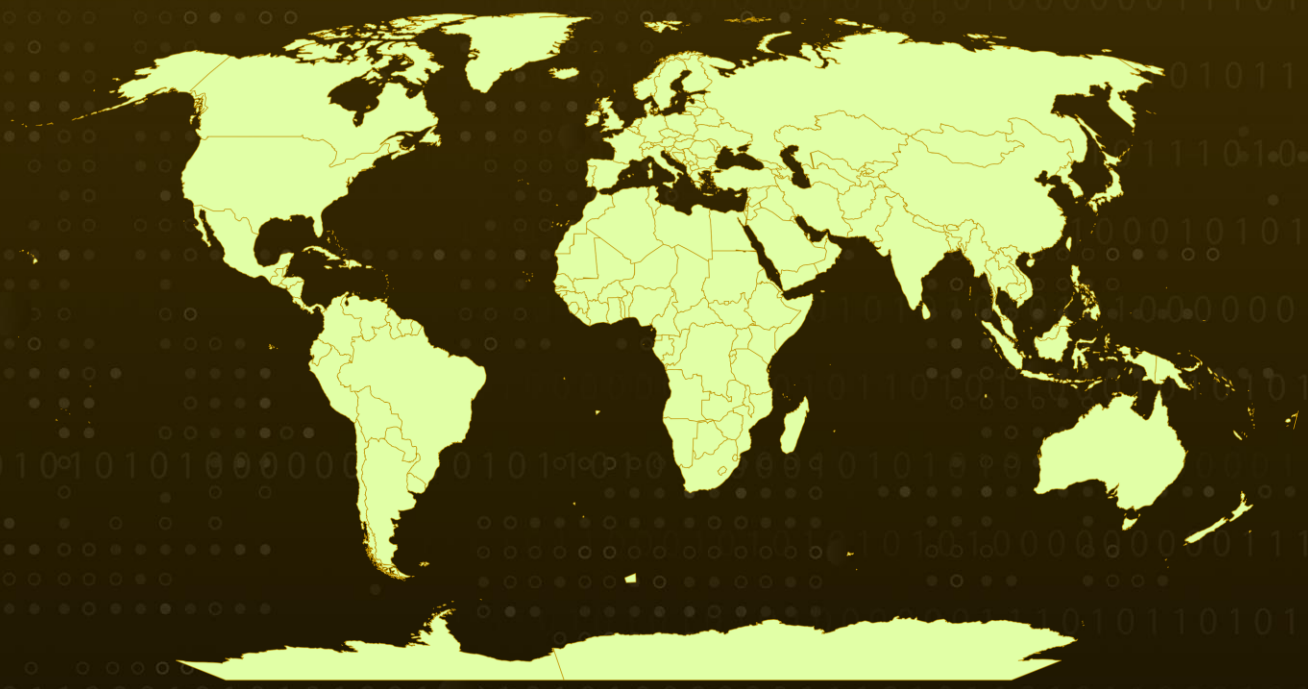
3AM Ransomware: LockBit's Failed Standoff Revealed

Date of Publication	Admiralty Code	TA Number
September 14, 2023	A1	TA2023370

Summary

Attack Began: September 2023
Malware: 3AM Ransomware
Attack Region: Worldwide
Attack: A new ransomware variant, self-dubbed '3AM' has arisen as a result of a rogue attack conducted by a ransomware affiliate. Initially, this affiliate attempted to install the LockBit ransomware on a target's network, but after their failed LockBit attempt, they switched to the 3AM ransomware.

Attack Regions



Attack Details

#1 A novel ransomware strain, known as '3AM,' is a 64-bit executable created using the Rust programming language. It was recently identified in a cyberattack orchestrated by a ransomware affiliate. Initially, the attacker attempted to deploy **LockBit** on the target's network, but when met with resistance, swiftly transitioned to the '3AM' ransomware variant. The name '3AM' is derived from its mention in the ransom note.

#2 The malicious campaign began with the threat actor using the 'gpresult' command to extract enforced policy settings for a specific user on the compromised computer. Additionally, the attacker executed various components of the Cobalt Strike framework in an attempt to elevate privileges by utilizing 'PsExec.'

#3 Following that, the adversaries ran reconnaissance commands such as 'whoami,' 'netstat,' 'quser,' and 'net share.' They also tried to enumerate other servers for lateral movement using 'quser' and 'net view' commands. To maintain a foothold, they created a new user and used the 'Wput' tool to transfer victims' files to their designated FTP server.

#4 When the encryption process begins, the 3AM ransomware takes steps to disable various services on the compromised system. It proceeds to append the encrypted files with the '.threeamtime' extension. After successfully encrypting the files, the malware proceeds to remove the Volume Shadow Copies (VSS). Subsequently, a file named 'RECOVER-FILES.txt' is generated within each scanned folder, containing the ransom note.

Recommendations

Robust Backup Strategy: Establish regular backups for all assets to guarantee their comprehensive security. Employ the 3-2-1-1 backup framework and utilize specialized tools to enhance backup durability and accessibility.

Zero Trust Model: Adopt a Zero Trust security model, which requires verification from anyone trying to access resources on a network, regardless of location, to minimize the attack surface.

User and Entity Behavior Analytics: Implement User and Entity Behavior Analytics (UEBA) tools to analyze user and entity behavior, enabling the detection of suspicious activities, including unauthorized use of reconnaissance commands. Additionally, employ event correlation mechanisms to link activities across diverse systems and users, facilitating the identification of coordinated reconnaissance attempts.

Behavioral Anomaly Detection: Deploy advanced behavioral anomaly detection systems that can identify deviations from normal user and system behavior, flagging activities such as frequent and unusual execution of reconnaissance commands.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**TA0008** Lateral Movement	**TA0040** Impact	**T1490** Inhibit System Recovery
T1486 Data Encrypted for Impact	**T1059** Command and Scripting Interpreter	**T1569.002** Service Execution	**T1070** Indicator Removal
T1070.004 File Deletion	**T1570** Lateral Tool Transfer	**T1049** System Network Connections Discovery	**T1543.003** Windows Service
T1548 Abuse Elevation Control Mechanism	**T1068** Exploitation for Privilege Escalation	**T1083** File and Directory Discovery	**T1055** Process Injection

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	185.202.0[.]111, 212.18.104[.]6, 85.159.229[.]62

TYPE	VALUE
SHA256	079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22, 307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e, 680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4, 991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af, ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc

References

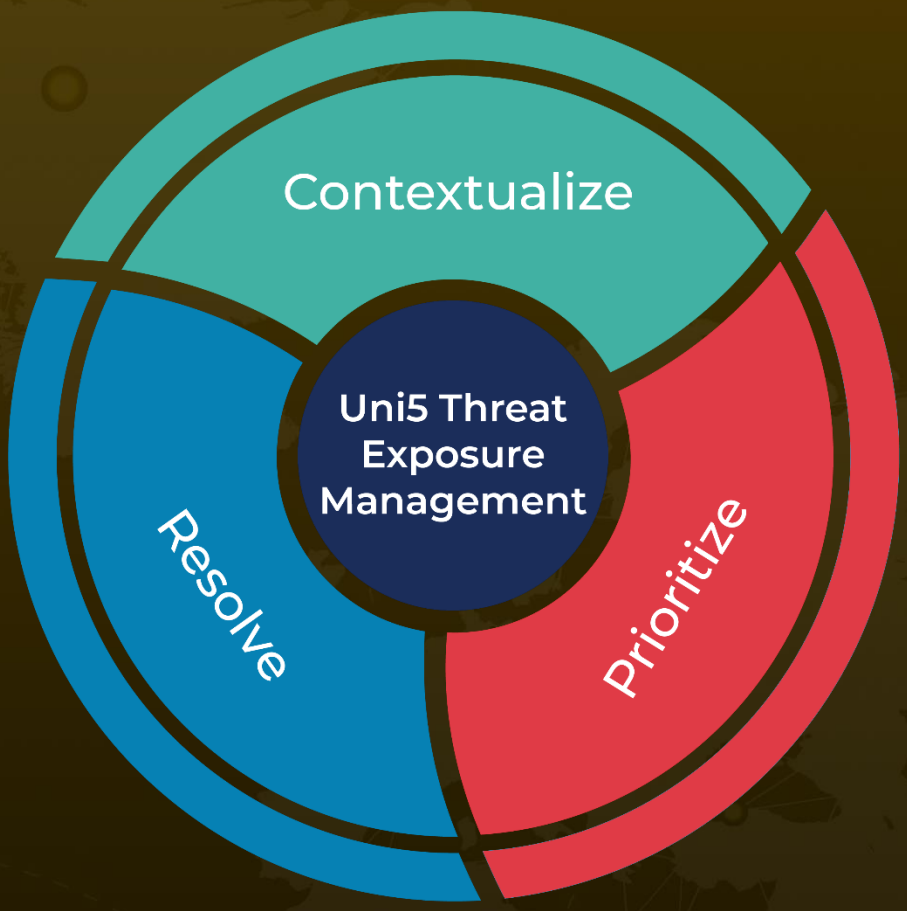
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3am-ransomware-lockbit

https://www.hivepro.com/lockbit-ransomware-evolving-tactics-and-pervasive-impact-in-2023/

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

September 14, 2023 • 3:30 AM

More at www.hivepro.com