WEEKLY RANSOMWARE ROUND-UP

Various ransomware groups are active in the global cyber space. In addition to data encryption, they publish the compromised victim details and threatens to leak the data. It is a part of the double extortion 'name and shame' technique and is supposed to persuade the compromised organizations to pay the ransom.

RANSOMWARE NAME	OVERVIEW	ATT&CK MATRIX
LockBit	Ransomware-as-a-service Model Ransom Technique: Double extortion Leverages SMB and PSEXEC for the propagation on a network Uses Neshta and Cobalt Strike etc. Actively exploiting vulnerabilities Uses already compromised credentials available on the various data leak forums to target the network Last reference: November, 2022	T1595.002: Vulnerability Scanning T1548: Abuse Elevation Control T1562.001: Disable or Modify Tools T1070 Indicator Removal on Host T1133: External Remote Services T1059: Command and Scripting Interpreter T1018: Remote System Discovery T1133: External Remote Services T1082: System Information Discovery T1486: Data Encrypted for Impact
Hive	Ransomware-as-a-service Model Ransom Technique: Double extortion Uses phishing emails, leaked VPN credentials and vulnerabilities exploitation as initial access vector Exploits exchange server (ProxyShell) vulnerabilities Leverages tools like Cobalt Strike, Mimikatz Last reference: November, 2022	T1566: Phishing T1190: Exploit Public Information T1598: Phishing for Information T1486: Data Encrypted for Impact T1133: External Remote Services T1059: Command and Scripting Interpreter T1059.001: PowerShell T1070.001: Clear Windows Event Logs T1003: OS Credential Dumping T1003.005: Cached Domain Credentials T1021: Remote Services
ALPHV (BlackCat)	Ransomware-as-a-service Model Ransom Technique: Double extortion Written in Rust Leverages tools NETSCAN, SLIVER, MIMIKATZ and Cobalt Strike etc. Targeted systems: Windows, ESXi, Debian, Ubuntu Last reference: November, 2022	T1595: Active Scanning T1190: Exploit Public-Facing Application T1003: OS Credential Dumping T1018: Remote System Discovery T1021: Remote Services T1490: Inhibit System Recovery T1005: Data from Local System T1485: Data Destruction

WEEKLY RANSOMWARE ROUND-UP

RANSOMWARE NAME	OVERVIEW	ATT&CK MATRIX
REvil(SODINOKIBI)	Ransomware-as-a-service Model Recently active in cyber space after a six-month hiatus Active vulnerability exploitation Ransom Technique: Double extortion Malwares: AUTOSEVEN, NESHTA Last reference: November, 2022	T1134: Access Token Manipulation T1036: Masquerading T1204.002: User Execution: Malicious File T1112: Modify Registry T1485: Data Destruction T1486: Data Encrypted for Impact T1189: Drive-by Compromise T1041: Exfiltration Over C2 Channel T1105: Ingress Tool Transfer
BlackByte	Ransomware-as-a-service Model Ransom Technique: Double extortion Encryption using ChaCha8 and Curve25519. Vulnerability exploited: CVE-2021-34473, CVE-2021-34523, and CVE-2021-3120 Last reference: November, 2022	T1595.002: Vulnerability Scanning T1059: Command and Scripting Interpreter: PowerShell T1027: Obfuscated Files of Info. T1562.001 and .004: Impair Defenses T1490 Inhibit System Recovery T1112 Modify Registry
Black Basta	Reportedly linked to financially motivated threat actor. Ransom Technique: Double extortion Leverages QBot malware to move laterally throughout the network. Uses SYSTEMBC Tunneler Last reference: November, 2022	T1059: Command and Scripting Interpreter T1047: Windows Management Instrumentation T1543: Create or Modify System Process T1055: Process Injection T1112: Modify Registry T1021: Remote Services T1486: Data Encrypted for Impact

Other recent activities:

- Venus ransomware targets publicly exposed RDP services
- Some ransomware groups also use publicly available compromised credentials on the leaked forums to target the organisations network

CMTX alert references:
[CMTX-P022022082]: Increase in Ransomware Campaigns

References:
https://attack.mitre.org/techniques/enterprise/

Note: Mostly reported ransomware attacks primarily use two methods e .g; phishing and vulnerability exploitation in addition to other techniques to compromise the systems. Please do follow the best practices and recommendations as mentioned in the below provided links.

References for best practices and remedial measures:

https://www.cyberswachhtakendra.gov.in/alerts/ransomware.html
https://www.cisa.gov/stopransomware
https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat