Mphasis
The Next Applied

BianLian Ransomware

Date: 06th June 2024 | Severity: High

Summary

- BianLian is a ransomware developer, deployer, and data extortion cybercriminal group that has targeted organizations in multiple U.S. critical infrastructure sectors since June 2022. They have also targeted Australian critical infrastructure sectors in addition to professional services and property development.
- The group gains access to victim systems through valid Remote Desktop Protocol (RDP) credentials, uses open-source tools and command-line scripting for discovery and credential harvesting, and exfiltrates victim data via File Transfer Protocol (FTP), Rclone, or Mega. BianLian group actors then extort money by threatening to release data if payment is not made.
- BianLian ransomware group claimed responsibility for the attack by adding Northern Minerals to its extortion page on the dark web.

Attack Vectors

- BianLian group uses valid accounts for lateral movement through the network and to pursue other follow-on activity.
- BianLian group actors used RDP with valid accounts as a means of gaining initial access and for lateral movement. threat actors used phishing to obtain valid user credentials for initial access.
- BianLian group actors used PowerShell to disable AMSI on Windows. See Appendix: Windows PowerShell and Command Shell Activity for additional information.
- Using Windows Command Shell to disable antivirus tools, for discovery, and to execute their tools on victim networks. See Appendix: Windows PowerShell and Command Shell Activity for additional information.
- BianLian group actors changed the password of an account they created. BianLian actors modified the password of an account they added to the local Remote Desktop Users group.
- used SoftPerfect Network Scanner, which can discover shared folders. BianLian group actors used SharpShares to enumerate accessible network shares in a domain.
- Malware collects data stored in the clipboard from users copying information within or between applications.
- BianLian group actors used Rclone to exfiltrate data to a cloud account they control on the same service to avoid typical file transfers/downloads and network-based exfiltration detection.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 96e02ea8b1c508f1ee3c1535547f9b89396f557011e61478644ae5876cdaaca5 • da7a959ae7ea237bb6cd913119a35baa43a68e375f892857f6d77eaa62aabbaf • a201e2d6851386b10e20fbd6464e861dea75a802451954ebe66502c2301ea0ed • f7a3a8734c004682201b8873691d684985329be3fcdba965f268103a086ebaad • a92dd4885af317d36cd62dac31d0d5c93febd367e8f4412e7593fb48c9f34256 • ea5c88fe464562227f483e8fc4eb2cf43e98a897aaaa3e94de4d236d5dc6e7e7 • 60b1394f3afee27701e2008f46d766ef466caa7711c45ddfd443a71efc39a407 • 4c008ac5c07d1573a98eb87bffe64e9c9e946de63b40df3f686881cf0698eef7 • f3a4fb09a0498e7ab3b33338ca6bc03460e43d437d9f3afbfc1a521c1029ff19 • 46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b • 0c756fc8f34e409650cd910b5e2a3f00 • 8b65c9437445e9bcb8164d8557ecb9e3585c8bebf37099a3ec1437884efbdd24 • dda89e9e6c70ff814c65e1748a27b42517690acb12c65c3bbd60ae3ab41e7aca • 99fc3e13f3b4d8debf1f2328f56f3810480ee2eed9271ebf413c0015c0a54c23 • 99fc3e13f3b4d8debf1f2328f56f3810480ee2eed9271ebf413c0015c0a54c23 • c5fa6a7a3b48a2a4bbcbbbb1ca50c730f3545e3fbb03fa17fb814ad7a400a21f
Email	• swikipedia@onionmail[.]org • mail2tor[.]com

Recommendation

- Auditing remote access tools on your network to identify currently used and/or authorized software.
- Reviewing logs for execution of remote access software to detect abnormal use of programs running as a portable executable.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (e.g., hard drive, storage device, or the cloud).
- Maintain offline backups of data, and regularly maintain backup and restoration (daily or weekly at minimum). By instituting this practice, an organization minimizes the impact of disruption to business practices as they will not be as severe and/or only have irretrievable data Maintain offline backups of data, and regularly maintain backup and restoration (daily or weekly at minimum). By instituting this practice, an organization minimizes the impact of disruption to business practices as they will not be as severe and/or only have irretrievable data.
- Monitor network traffic and look for indicators of compromise, such as unusual network traffic patterns or communication with known command-and-control servers.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https[:]//www.sentinelone.com/anthology/bianlian/
- https[:]//www.bleepingcomputer.com/news/security/australian-mining-company-discloses-breach-after-bianlian-leaks-data/