ADVISORY FOR ICM SECTORS

Evolution of BianLian ransomware

Original report published on: May 16, 2023[1]

Executive Summary

Since June 2022, BianLian, a ransomware group known for its global attacks, particularly in the U.S.[1], shifted tactics from data encryption to solely data exfiltration after Avast released a decryption tool[2] in January 2023. The group, adept at using compromised Remote Desktop Protocol (RDP) credentials, recently collaborated with White Rabbit and Mario threat actor groups in December 2023, signalling an evolution in their extortion strategies.

Background

BianLian is a ransomware developer, deployer, and data extortion cybercriminal group. Originally, their operations were the typical double-extortion model of encrypting files and threatening to leak data. However, in Jan 2023, Avast, a cybersecurity firm offering antivirus software, released a free decryptor capable of reversing its encryption to the public. [2] This event marked a significant change to BianLian's operational methods as they stopped encrypting victim data and only did data exfiltration-based extortion since then.

Though they changed some of their tactics, they have been staying consistent in their methods for initial access and lateral movement which is by leveraging compromised Remote Desktop Protocol (RDP) credentials likely acquired from initial access brokers.

On 15 December 2023, Resecurity researchers reported a collaboration observed between the BianLian, White Rabbit and Mario threat actor groups in running joint extortion campaigns.[3] Although 60% of their victims are from United States, the groups are financially motivated and have also targeted systems globally and indiscriminately across different sectors.

In September 2023, some of BianLian's victims include 2 Singapore-based travel and construction companies, telecommunications companies PT Smartfren Telecom from Indonesia and TELNET Redes Inteligentes from Spain.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Refer to the MITRE ATT&CK techniques in this advisory:
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Validate and add malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR).
- Keep all operating systems, software, and firmware up to date.
- Disable command-line and scripting activities and permissions if there is no business need.

- Restrict usage of PowerShell and update Windows PowerShell or PowerShell core logging to the latest version.
- Closely monitor inbound and outbound network traffic for suspicious communications or data transmissions

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

Indicators of Compromise

File name	SHA256
def.exe	7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893
encryptor.exe	1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43
exp.exe	0c1eb11de3a533689267ba075e49d93d55308525c04d6aff0d2c54d1f52f5500
system.exe	40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Resource Development	T1587.001	Develop Capabilities: Malware
Initial Access	T1133	External Remote Services
	T1566	Phishing
	T1078	Valid Accounts
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1053.005	Scheduled Task/Job: Scheduled Task
Persistence	T1098	Account Manipulation
	T1136.001	Create Account: Local Account
Defence Evasion	T1112	Modify Registry
	T1562.001	Impair Defences: Disable or Modify Tools
	T1562.004	Impair Defences: Disable or Modify System Firewall
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory
	T1003.003	OS Credential Dumping: NTDS

	T1552.001	OS Credential Dumping: Credentials In Files
Discovery	T1087.002	Account Discovery: Domain Account
	T1482	Domain Trust Discovery
	T1083	File and Directory Discovery
	T1046	Network Service Discovery
	T1135	Network Share Discovery
	T1069.002	Permission Group Discovery: Domain Groups
	T1012	Query Registry
	T1018	Remote System Discovery
	T1033	System Owner User Discovery
Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol
Collection	T1115	Clipboard Data
Command and Control	T1105	Ingress Tool Transfer
	T1219	Remote Access Software
Exfiltration	T1537	Transfer Data to Cloud Account
	T1048	Exfiltration Over Alternative Protocol
	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage
Impact	T1486	Data Encrypted for Impact

References

1. ^ "CISA CyberSecurity Advisories - BianLian".
2. ^ "Avast Decrypted BianLian ransomware".
3. ^ "Resecurity Exposing Cyber Extortion Trinity: BianLian, White Rabbit and Mario Ransomware Gangs Spotted Joint Campaign".