Case Study 2023-02-23

Case Study: Research & Higher Education Incident #001: Ransomware - 2022

SUMMARY

An institution of higher education (IHE) in Virginia was subject to an intrusion by a criminal affiliate assessed by the institution to be associated with BianLian ransomware. The attack was thwarted before widespread exfiltration or encryption of systems was completed by the cybercriminals.

FURTHER INFORMATION

On Monday, July 25, 2022, tooling alerted institutional technology staff of a password spray from a service account within the academic network; further review indicated suspicious activity on a Windows Activity Directory Domain Controller (DC) as well.

Response teams removed login privileges from the service account, rotated its password, isolated the source workstation, and began further analysis on the DC logs. Out-of-band communications were initiated with institutional leadership, and relevant institutional vendors (such as cybersecurity companies and insurance carriers) were engaged as additional response resources.

Initial access was likely gained in November 2021 when a banking trojan was downloaded and installed on a user workstation. Post-exploitation from that host yielded access to a service account with a weak password and finally a domain administrator account.

Multiple Remote Access Software were used for command and control by the threat actors including Atera and Splashtop, as well as a custom backdoor written in Golang. Publicly available offensive tools implicated in various stages of the attack were used for port scanning, dumping LSASS, and attacking Kerberos. Attempted use of Cobalt Strike and WinSCP to exfiltrate data was automatically blocked and logged by protection devices.

RESPONSE

Based on the analysis by the various responders including retroactive hunts, additional mitigation measures were taken: password resets were forced on all Active Directory (AD) accounts (including the KRBTGT account twice), backups were isolated, all remote access was moved behind Multi-Factor Authentication (MFA), and observed Indicators of Compromise (IOCs) were added to block and alert lists. Compromised hosts were rebuilt, Microsoft LAPS was implemented for workstations and servers, and Group Policy Objects were reviewed for anomalies.

IMPACT

Due to the successful detection of suspicious post-compromise activity; the well-arranged architecture by the IT team including redundancy of systems in place; and the quick response time, the institution was able to avoid serious system downtime or interruption to academic operations despite the Fall 2022 academic semester beginning during recovery.

Due to mandatory password resets, university constituents did need to engage with the institutional help desk to cycle their passwords to regain access to systems.

Analysis concluded 16 servers and 30 workstations were impacted by the compromise, so those had to be rebuilt using backups preserved from prior to the initial compromise. During that recovery, older operating systems (Server 2012 and earlier) were upgraded to Server 2016 and Server 2019 versions.

LESSONS LEARNED

- Ensure recent, reliable, isolated backups
- Document processes and tabletop those plans
- Leadership buy-in is critical before and during an incident
- Engage quickly with partners
- Follow the principle of least privilege
- Block/alert on commodity remote software not in use by the organization

MITRE ATT&CK® TECHNIQUES

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1047	Windows Management Instrumentation
	T1059	Command and Scripting Interpreter
Persistence	T1078	Valid Accounts: Domain Accounts
	T1133	External Remote Services
	T1136	Create Account: Local Account
Defense Evasion	T1202	Indirect Command Execution
Credential Access	T1003	OS Credential Dumping: LSASS Memory
	T1110	Brute Force: Password Spraying
Discovery	T1007	System Service Discovery
	T1016	System Network Configuration Discovery
	T1018	Remote System Discovery
	T1057	Process Discovery
	T1069	Permission Groups Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1135	Network Share Discovery
Lateral Movement	T1021	Remote Services
	T1570	Lateral Tool Transfer
Collection	T1005	Data from Local System
	T1119	Automated Collection
Command and Control	T1219	Remote Access Software
Impact	T1486	Data Encrypted for Impact
	T1489	Service Stop
	T1490	Inhibit System Recovery
	T1491	Defacement: Internal Defacement

ADDITIONAL RESOURCES

Malware metadata and tool usage match those documented here:
https://redacted.com/blog/bianlian-ransomware-gang-gives-it-a-go