ADVISORY FOR IM SECTORS

BlackSuit group targets media conglomerate with ransomware

Original report published on: Jun 27, 2024 [1]

Executive Summary

On 27 June 2024, BlackSuit, a cybercrime group, claimed responsibility for a cyberattack on Kadokawa corporation, a media conglomerate in Japan. This impacted Niconico, a popular Japanese video-sharing platform owned by Dwango, Kadokawa's subsidiaries around 8 June and Kadokawa's websites and networks on 14 June. BlackSuit encrypted data on the servers and claimed to have exfiltrated 1.5TB of data including contracts, emails, employee personal data, business plans, project details and financial data. [2]

BlackSuit claimed to have conducted significant reconnaissance to understand Kadokawa's infrastructure with its subsidiaries and how they were managed by VMware ESXi and vSphere. BlackSuit then encrypted Kadokawa's data. BlackSuit claimed to have retained undetected access to Kadokawa's network despite the latter's efforts to contain the cyberattack through IP address blocking and changing of administrator credentials. [3]

Background

Since May 2023, BlackSuit has been a rebrand of the Royal ransomware group. BlackSuit targets large and small to medium-sized businesses but excludes 9 Commonwealth of Independent States. BlackSuit often extorts their victims twice, first for the decryption key to restore encrypted systems or data and, secondly for not disclosing the exfiltrated data.

The group is known to use payloads for both Windows and Linux environments and a customised encryptor that utilises OpenSSL's implementation of Advanced Encryption Standard (AES). Initial access is obtained via phishing, Remote Desktop Protocol (RDP) or virtual private network (VPN) access with stolen or leaked credentials and exploiting vulnerabilities.

After gaining access, BlackSuit uses living off the land binary, like PsExec and RDP, together with Remote Monitoring and Management (RMM) tools for lateral movement and maintaining persistence. Sensitive data is exfiltrated before the customised encryptor is deployed to lock up systems.

Detection and Mitigation Techniques

- Deploy secured email gateway to scan and block suspicious or malicious emails.
- Place strict network access control for publicly accessible RDP or remove public access if not required.
- Perform regular patching of publicly accessible servers to reduce the risk of exploitation.
- Ensure that endpoint detection response and/or antivirus are installed and updated on all devices in the network.
- Use network segmentation together with IDS/IPS to monitor for unusual or suspicious internal network traffic.
- Apply strict data loss prevention policies for sensitive data.

Indicators of Compromise [4]

Indicator	Type	Description
f1684fb118d4d8fc56653fcc49e12a659b64c4459ba037fa94f21783235cc6ba	SHA256	BlackSuit ransomware
dede96fd44c0f78eb79ceb63b898874e8922efc59d8bfb9f86505b1992bc00a3	SHA256	BlackSuit ransomware
79ab73a0e9dd8eac045c00fd1bd172a7f359588901f93c83e6740157eb21e7df	SHA256	BlackSuit ransomware
d96ff4b3e188f7ff96ed28c1381a6318dd76bb1fbd6ca02c6ab0236e1c7f35aa	SHA256	BlackSuit ransomware
.blacksuit	Extension	Encrypted files extension
WLm87eV1oNRx6P3E4Cy9	Mutex	Mutex value object created by the BlackSuit ransomware

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID and name	Details
Initial Access	T1566 – Phishing	Emails with malicious attachments or links are used to deliver the ransomware payload.
Initial Access	T1190 - Exploit Public-Facing Application	Exploiting common or known vulnerabilities of public-facing applications
Initial Access	T1078 - Valid Accounts	Abuse credentials of existing accounts that are stolen or leaked
Execution	T1204 - User Execution	Execution of malicious files by users.
Execution	T1059 - Command and Scripting Interpreter	Use of command-line interfaces for script execution.
Persistence	T1547 - Boot or Logon Autostart Execution	Techniques to maintain persistence on the system.
Privilege Escalation	T1068 - Exploitation for Privilege Escalation	Exploiting vulnerabilities to gain higher-level permissions.
Defense Evasion	T1027 - Obfuscated Files or Information	Hiding malicious payloads using obfuscation techniques.
Defense Evasion	T1562 - Disabling Security Tools	Tampering with or disabling security software and logs.
Credential Access	T1003 - Credential Dumping	Extracting passwords and other credentials from the operating system and software.
Discovery	T1049 - System Network Connections Discovery	Identifying connected networks and systems.
Lateral Movement	T1021 - Remote Services	Using remote desktop or other remote services to move laterally across the network.
Collection	T1005 - Data from Local System	Collecting files and information from the local system.
Exfiltration	T1041 - Exfiltration Over C2 Channel	Transferring data to an external server.
Impact	T1486 - Data Encrypted for Impact	Encrypting data to render it inaccessible.

References

1. https://www.bleepingcomputer.com/news/security/blacksuit-ransomware-gang-claims-attack-on-kadokawa-corporation/
2. https://therecord.media/niconico-japan-video-streaming-site-cyberattack
3. https://en.wikipedia.org/wiki/2024_cyberattack_on_Kadokawa_and_Niconico#/media/File:Blacksuit's_Statement_on_Kadokawa_Corp._cyberattack.png
4. https://areteir.com/article/understanding-blacksuit-ransomware/