THREAT ADVISORY *CRITICAL*

October 2, 2024

Storm-0501 Ransomware Threatens Hybrid Cloud Environments

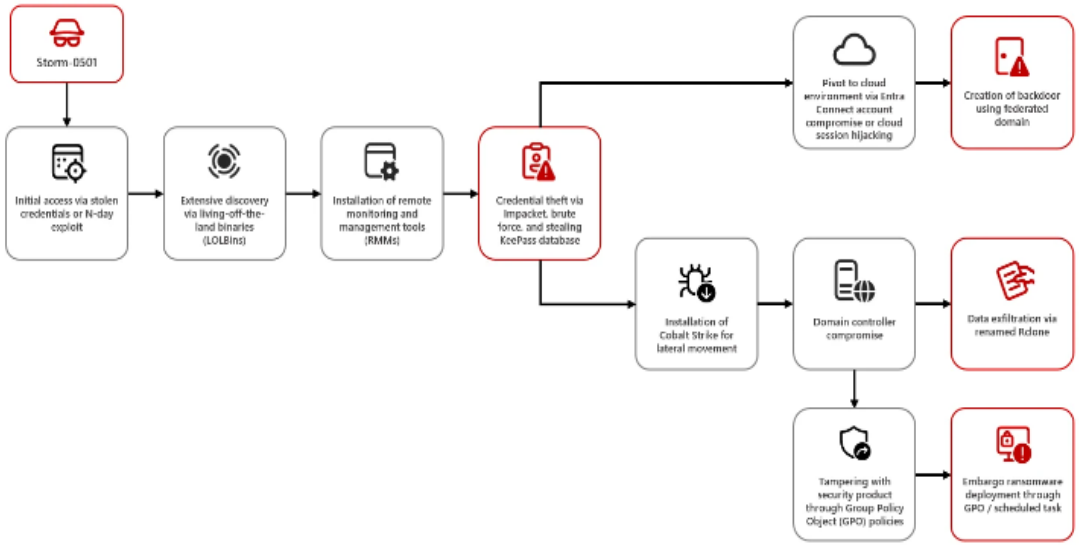
SUMMARY

The threat actor group Storm-0501 has been launching ransomware attacks against government, manufacturing, transportation, and law enforcement sectors in the U.S. This complex, multi-phase operation is aimed at penetrating hybrid cloud environments, allowing the attackers to move laterally from on-premises systems to the cloud. Their objectives include data theft, credential compromise, system manipulation, persistent backdoor installation, and ransomware deployment. According to Microsoft, "Storm-0501 is a financially motivated group that utilizes commercial and open-source tools to carry out its ransomware activities."

TECHNICAL DETAILS

The threat actor known as Storm-0501 targets cloud environments by exploiting weak credentials and privileged accounts, aiming to steal data and deploy ransomware. According to Microsoft, Storm-0501 initially gains network access using stolen or purchased credentials or by exploiting known vulnerabilities. Recent attacks have involved vulnerabilities like CVE-2022-47966 (Zoho ManageEngine), CVE-2023-4966 (Citrix NetScaler), and possibly CVE-2023-29300 or CVE-2023-38203 (ColdFusion 2016). Once inside the network, the attacker moves laterally within the compromised environment using widely used frameworks like Impacket and Cobalt Strike. Data is exfiltrated using a custom Rclone binary, disguised as a legitimate Windows tool, while PowerShell cmdlets are used to disable security agents.

Storm-0501 exploits stolen Microsoft Entra ID (formerly Azure AD) credentials to further expand access, particularly focusing on synchronization accounts between on-premises Active Directory (AD) and cloud environments. Microsoft Entra Connect Sync accounts, responsible for synchronizing data between on-prem AD and Entra ID, hold significant privileges. If attackers gain access to Directory Synchronization Account credentials, they can use tools like AADInternals to alter cloud passwords, bypassing security defenses. If a domain administrator or other highly privileged accounts are accessible on-prem and in the cloud without adequate protections (like multi-factor authentication), Storm-0501 can reuse these credentials to regain access to the cloud environment.



After gaining control of the cloud infrastructure, the attackers establish persistence by creating a new federated domain within the Microsoft Entra tenant. This enables them to authenticate as any user for whom they know or have configured the "Immutableid" property. With this access, they can deploy the Embargo ransomware or maintain backdoor access for future use.

Once Storm-0501 has fully compromised the victim's network—exfiltrating sensitive data and moving laterally to the cloud—they deploy Embargo ransomware across the organization. This typically involves using compromised high-privilege accounts, such as Domain Admins, to execute the ransomware through scheduled tasks or Group Policy Objects (GPOs), encrypting files across multiple systems. In some cases, however, rather than deploying ransomware immediately, the group may maintain backdoor access for extended periods, likely for continued exploitation or delayed ransom demands. Microsoft notes that Storm-0501 doesn't always prioritize ransomware deployment, sometimes opting for persistence and long-term access over immediate encryption operations.

INDICATORS OF COMPROMISE (IOCs)

- efb2f6452d7b0a63f6f2f4d8db49433259249df598391dd79f64df1ee3880a8d
- a9aeb861817f3e4e74134622cbe298909e28d0fcc1e72f179a32adc637293a40
- caa21a8f13a0b77ff5808ad7725ff3af9b74ce5b67426c84538b8fa43820a031
- d37dc37fdcebbe0d265b8afad24198998ae8c3b2c6603a9258200ea8a1bd7b4a
- 53e2dec3e16a0ff000a8c8c279eeeca8b4437edb8ec8462bfbd9f64ded8072d9
- 827f7178802b2e92988d7cff349648f334bc86317b0b628f4bb9264285fccf5f
- ee80f3e3ad43a283cbc83992e235e4c1b03ff3437c880be02ab1d15d92a8348a
- de09ec092b11a1396613846f6b082e1e1ee16ea270c895ec6e4f553a13716304
- d065623a7d943c6e5a20ca9667aa3c41e639e153600e26ca0af5d7c643384670
- c08dd490860b54ae20fa9090274da9ffa1ba163f00d1e462e913cf8c68c11ac1

RECOMMENDATIONS

- Enforce strong, complex passwords and regularly update them. Implement multi-factor authentication (MFA) for all privileged accounts, especially on-premises and cloud access. Regularly audit and monitor the use of privileged accounts and restrict their usage wherever possible.
- Apply timely patches to known vulnerabilities, particularly for critical systems like Zoho ManageEngine, Citrix NetScaler, and ColdFusion. Continuously monitor for emerging vulnerabilities and update systems accordingly.
- Protect Microsoft Entra Connect Sync accounts with MFA and restrict their permissions. Regularly audit and secure the synchronization process between on-premises AD and Microsoft Entra ID to prevent unauthorized access.
- Implement strict access controls to segment critical assets and limit lateral movement. Apply the principle of least privilege to minimize exposure of sensitive systems.
- Deploy endpoint detection and response (EDR) solutions to identify malicious activity like lateral movement, data exfiltration, and unauthorized tools (Impacket, Cobalt Strike). Use PowerShell logging and monitoring to detect abnormal scripts that may disable security agents.
- Maintain regular backups of critical systems, ensuring they are isolated from the main network to avoid ransomware encryption. Test recovery procedures to ensure rapid restoration in case of ransomware deployment.

REFERENCES

- https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/
- https://www.bleepingcomputer.com/news/security/embargo-ransomware-escalates-attacks-to-cloud-environments/
- https://thehackernews.com/2024/09/microsoft-identifies-storm-0501-as.html
- https://cyble.com/blog/the-rust-revolution-new-embargo-ransomware-steps-in/