LAPSUS$: Recent techniques, tactics and procedures

research.nccgroup.com/2022/04/28/lapsus-recent-techniques-tactics-and-procedures/

April 28, 2022

Authored by: David Brown, Michael Matthews and Rob Smallridge

tl;dr

This post describes the techniques, tactics and procedures we observed during recent LAPSUS$ incidents.

Our findings can be summarised as below:

- Access and scraping of corporate Microsoft SharePoint sites in order to identify any credentials which may be stored in technical documentation.
- Access to local password managers and databases to obtain further credentials and escalate privileges.

- Living of the land – tools such as RVTools to shut down servers and ADExplorer to perform reconnaissance.
- Cloning of git repositories and extraction of sensitive API Keys.
- Using compromised credentials to access corporate VPNs.
- Disruption or destruction to victim infrastructure to hinder analysis and consume defensive resource.

Summary

LAPSUS$ first appeared publicly in December 2021, however, NCC Group first observed LAPSUS$ months prior during an incident response engagement. We believe the group has also operated prior to this date, though perhaps not under the "LAPSUS$" banner.

Over the last 5 months, LAPSUS$ has gained large notoriety with some successful breaches of some large enterprises including, Microsoft, Nvidia, Okta & Samsung. Little is still known about this group with motivations appearing to be for reputation, money and "for the lulz".

Notifications or responsibility of victims by LAPSUS$ are commonly reported via their telegram channel and in one case a victim's DNS records were reconfigured to LAPSUS$ controlled domains/websites. However, not all victims or breaches appear to actively be announced via their telegram channel, nor are some victims approached with a ransom. This distinguishes themselves from more traditional ransomware groups who have a clear modus operandi and are clearly financially focused. The result of this is that LAPSUS$ are less predictable which may be why they have seen recent success.

This serves as a reminder for defenders for defence in depth and the need to anticipate different tactics that threat actors may use.

It is also worth mentioning the brazen behaviour of this threat actor and their emboldened attempts at Social Engineering by offering payment for insiders to provide valid credentials.

This tactic is potentially in response to greater home working due to the pandemic which means there is a far larger proportion of employees with VPN access and as such a greater pool of potential employees willing to sell their credentials.

To combat this, organisations need to ensure they have extensive VPN logging capabilities, robust helpdesk ticketing as well as methods to help identify anomalies in VPN access.

It is notable that the majority of LAPSUS$ actions exploit the human element as opposed to technical deficiencies or vulnerabilities. Although potentially viewed as unsophisticated or basic these techniques have been successful, so it is vital that organisations factor in controls and mitigations to address them.

Initial access

Threat Intelligence shows that LAPSUS$ utilise multiple methods to gain Initial access.

The main source of initial access is believed to occur via stolen authentication cookies which would grant the attacker access to a specific application. These cookies are usually in the form of Single sign-on (SSO) applications which would allow the attacker to pivot into other corporate applications ultimately bypassing controls such as multi-factor authentication (MFA).

Credential access and Privilege escalation

Credential Harvesting and privileged escalation are key components of the LAPSUS$ breaches we have seen, with rapid escalation in privileges the LAPSUS$ group have been seen to elevate from a standard user account to an administrative user within a couple of days.

In the investigations conducted by NCC Group, little to no malware is used. In one case NCC Group observed LAPSUS$ using nothing more than the legitimate Sysinternals tool ADExplorer, which was used to conduct reconnaissance on the victim's environment.

Access to corporate VPNs is a primary focus for this group as it allows the threat actor to directly access key infrastructure which they require to complete their objectives.

In our incident response cases, we saw the threat actor leveraging compromised employee email accounts to email helpdesk systems requesting access credentials or support to get access to the corporate VPN.

Lateral Movement

In one incident LAPSUS$ were observed to sporadically move through the victim environment via RDP in an attempt to access resources deeper in the victim environment. In some instances, victim controlled hostnames were revealed including the host "VULTR-GUEST" which refers to infrastructure hosted on the private cloud service, Vultr[3].

Exfiltration

LAPSUS$'s action on objectives appears to focus on data exfiltration of sensitive information as well as destruction or disruption. In one particular incident the threat actor is observed to utilise the free file drop service "filetransfer[.]io".

Impact

NCC Group has observed disruption and destruction to client environments by LAPSUS$ such as shutting down virtual machines from within on-premises VMware ESXi infrastructure, to the extreme of mass deletion of virtual machines, storage, and configurations in cloud environments making it harder for the victim to recover and for the investigation team to conduct their analysis activities.

The theft of data reported appears to heavily be focused on application source code or proprietary technical information. With a targeting of internal source code management or repository servers. These git repositories can contain not only commercially sensitive intellectual property, but also in some cases may include additional API keys to sensitive applications including administrative or cloud applications.

Recommendations

- Ensure that Cloud computing environments have sufficient logging enabled.
- Ensure that cloud administrative access is configured to prevent unauthorised access to resources and that API keys are not overly permissive to the permissions they require.
- Utilise MFA for user authentication on both cloud and remote access solutions to help reduce the risk of unauthorised access.
- Ensure logging is in place to record MFA device enrolment
- Security controls such as Conditional Access can help restrict or prevent unauthorised access based on criteria such as geographical location.
- Implement activities to detect and investigate anomalies in VPN access.
- Ensure a system is in place to record all helpdesk queries.
- Avoid using SMS as an MFA vector to avoid the risk of SIM swapping.
- Securing source code environments to ensure that users can only access the relevant repositories.
- Secret Scanning[1][2] on source code repositories should be conducted to ensure that sensitive API credentials are not stored in source code. GitHub and Gitlab offer detection mechanisms for this
- Remote Desktop services or Gateways used as a primary or secondary remote access solution should be removed from any corporate environment in favour for alternative solutions such as secured VPNs, or other Remote Desktop applications which mitigate common attack techniques such as brute force or exploitation and can offer additional security controls such as MFA and Conditional Access.
- Centralise logging including cloud applications (SIEM solution).
- Offline or immutable backups of servers should be taken to ensure that in the event of a data disruption or destruction attack, services can be restored.
- Reduce MFA token/Session cookie validity times
- Ensure principle of least privilege for user accounts is being adhered to.
- Social engineering awareness training for all staff.

Indicators of Compromise

Indicator Value	Indicator Type	Description
104.238.222[.]158	IP address	Malicious Lapsus Network Address
108.61.173[.]214	IP address	Malicious Lapsus Network Address
185.169.255[.]74	IP address	Malicious Lapsus Network Address
VULTR-GUEST	Hostname	Threat Actor Controlled Host
hxxps://filetransfer[.]io	Domain	Free File Drop Service Utilised by the Threat Actor

MITRE ATT&CK

Technique Code	Technique
T1482	Discovery – Domain Trust Discovery
T1018	Discovery – Remote System Discovery
T1069.002	Discovery – Groups Discovery: Domain Groups
T1016.001	Discovery – System Network Configuration Discovery
T1078.002	Privilege Escalation – Domain Accounts
T1555.005	Credential Access – Credentials from Password Stores: Password Managers
T1021.001	Lateral Movement – Remote Services: Remote Desktop Protocol
T1534	Lateral Movement – Internal Spearphishing
T1072	Execution – Software Deployment Tools
T1213.002	Collection – Data from Information Repositories: Sharepoint
T1039	Collection – Data from Network Shared Drive
T1213.003	Collection – Data from Information Repositories: Code Repositories
T1567	Exfiltration – Exfiltration Over Web Service
T1485	Impact – Data Destruction
T1529	Impact – System Shutdown/Reboot

References