

## LAPSUS\$, DEV-0537, Strawberry Tempest, Group G1004

Archived: 2026-04-05 18:37:28 UTC

Enterprise [T1531 Account Access Removal](#)

[LAPSUS\\$](#) has removed a targeted organization's global admin accounts to lock the organization out of all access. [\[2\]](#)

Enterprise [T1087 .002 Account Discovery: Domain Account](#)

[LAPSUS\\$](#) has used the AD Explorer tool to enumerate users on a victim's network. [\[2\]\[5\]](#)

Enterprise [T1098 .003 Account Manipulation: Additional Cloud Roles](#)

[LAPSUS\\$](#) has added the global admin role to accounts they have created in the targeted organization's cloud instances. [\[2\]](#)

Enterprise [T1583 .003 Acquire Infrastructure: Virtual Private Server](#)

[LAPSUS\\$](#) has used VPS hosting providers for infrastructure. [\[2\]](#)

Enterprise [T1586 .002 Compromise Accounts: Email Accounts](#)

[LAPSUS\\$](#) has payed employees, suppliers, and business partners of target organizations for credentials. [\[2\]\[5\]](#)

Enterprise [T1584 .002 Compromise Infrastructure: DNS Server](#)

[LAPSUS\\$](#) has reconfigured a victim's DNS records to actor-controlled domains and websites. [\[5\]](#)

Enterprise [T1136 .003 Create Account: Cloud Account](#)

[LAPSUS\\$](#) has created global admin accounts in the targeted organization's cloud instances to gain persistence. [\[2\]](#)

Enterprise [T1555 .003 Credentials from Password Stores: Credentials from Web Browsers](#)

[LAPSUS\\$](#) has obtained passwords and session tokens with the use of the Redline password stealer. [\[2\]](#)

[.005 Credentials from Password Stores: Password Managers](#)

[LAPSUS\\$](#) has accessed local password managers and databases to obtain further credentials from a compromised network. [\[5\]](#)

Enterprise [T1485 Data Destruction](#)

[LAPSUS\\$](#) has deleted the target's systems and resources both on-premises and in the cloud. [\[2\]\[5\]](#)

Enterprise [T1213 .001 Data from Information Repositories: Confluence](#)

[LAPSUS\\$](#) has searched a victim's network for collaboration platforms like Confluence and JIRA to discover further high-privilege account credentials. <sup>[2]</sup>

[.002 Data from Information Repositories: Sharepoint](#)

[LAPSUS\\$](#) has searched a victim's network for collaboration platforms like SharePoint to discover further high-privilege account credentials. <sup>[2][5]</sup>

[.003 Data from Information Repositories: Code Repositories](#)

[LAPSUS\\$](#) has searched a victim's network for code repositories like GitLab and GitHub to discover further high-privilege account credentials. <sup>[2][5]</sup>

[.005 Data from Information Repositories: Messaging Applications](#)

[LAPSUS\\$](#) has searched a victim's network for organization collaboration channels like MS Teams or Slack to discover further high-privilege account credentials. <sup>[2]</sup>

Enterprise [T1005 Data from Local System](#)

[LAPSUS\\$](#) uploaded sensitive files, information, and credentials from a targeted organization for extortion or public release. <sup>[2]</sup>

Enterprise [T1114 .003 Email Collection: Email Forwarding Rule](#)

[LAPSUS\\$](#) has set an Office 365 tenant level mail transport rule to send all mail in and out of the targeted organization to the newly created account. <sup>[2]</sup>

Enterprise [T1068 Exploitation for Privilege Escalation](#)

[LAPSUS\\$](#) has exploited unpatched vulnerabilities on internally accessible servers including JIRA, GitLab, and Confluence for privilege escalation. <sup>[2]</sup>

Enterprise [T1133 External Remote Services](#)

[LAPSUS\\$](#) has gained access to internet-facing systems and applications, including virtual private network (VPN), remote desktop protocol (RDP), and virtual desktop infrastructure (VDI) including Citrix. <sup>[2][5]</sup>

Enterprise [T1589 Gather Victim Identity Information](#)

[LAPSUS\\$](#) has gathered detailed information of target employees to enhance their social engineering lures. <sup>[2]</sup>

[.001 Credentials](#)

[LAPSUS\\$](#) has gathered user identities and credentials to gain initial access to a victim's organization; the group has also called an organization's help desk to reset a target's credentials. <sup>[2][5]</sup>

### [.002 Email Addresses](#)

[LAPSUS\\$](#) has gathered employee email addresses, including personal accounts, for social engineering and initial access efforts. <sup>[2]</sup>

Enterprise [T1591 .002 Gather Victim Org Information: Business Relationships](#)

[LAPSUS\\$](#) has gathered detailed knowledge of an organization's supply chain relationships. <sup>[2]</sup>

### [.004 Gather Victim Org Information: Identify Roles](#)

[LAPSUS\\$](#) has gathered detailed knowledge of team structures within a target organization. <sup>[2]</sup>

Enterprise [T1656 Impersonation](#)

[LAPSUS\\$](#) has called victims' help desk and impersonated legitimate users with previously gathered information in order to gain access to privileged accounts. <sup>[2]</sup>

Enterprise [T1578 .002 Modify Cloud Compute Infrastructure: Create Cloud Instance](#)

[LAPSUS\\$](#) has created new virtual machines within the target's cloud environment after leveraging credential access to cloud assets. <sup>[2]</sup>

### [.003 Modify Cloud Compute Infrastructure: Delete Cloud Instance](#)

[LAPSUS\\$](#) has deleted the target's systems and resources in the cloud to trigger the organization's incident and crisis response process. <sup>[2]</sup>

Enterprise [T1111 Multi-Factor Authentication Interception](#)

[LAPSUS\\$](#) has replayed stolen session token and passwords to trigger simple-approval MFA prompts in hope of the legitimate user will grant necessary approval. <sup>[2]</sup>

Enterprise [T1621 Multi-Factor Authentication Request Generation](#)

[LAPSUS\\$](#) has spammed target users with MFA prompts in the hope that the legitimate user will grant necessary approval. <sup>[2]</sup>

Enterprise [T1588 .001 Obtain Capabilities: Malware](#)

[LAPSUS\\$](#) acquired and used the Redline password stealer in their operations. <sup>[2]</sup>

### [.002 Obtain Capabilities: Tool](#)

[LAPSUS\\$](#) has obtained tools such as RVTools and AD Explorer for their operations. <sup>[2][5]</sup>

Enterprise [T1003 .003 OS Credential Dumping: NTDS](#)

[LAPSUS\\$](#) has used Windows built-in tool `ntdsutil` to extract the Active Directory (AD) database. <sup>[2]</sup>

[.006 OS Credential Dumping: DCSync](#)

[LAPSUS\\$](#) has used DCSync attacks to gather credentials for privilege escalation routines. <sup>[2]</sup>

Enterprise [T1069 .002 Permission Groups Discovery: Domain Groups](#)

[LAPSUS\\$](#) has used the AD Explorer tool to enumerate groups on a victim's network. <sup>[2]</sup>

Enterprise [T1598 .004 Phishing for Information: Spearphishing Voice](#)

[LAPSUS\\$](#) has called victims' help desk to convince the support personnel to reset a privileged account's credentials. <sup>[2]</sup>

Enterprise [T1090 Proxy](#)

[LAPSUS\\$](#) has leverage NordVPN for its egress points when targeting intended victims. <sup>[2]</sup>

Enterprise [T1597 .002 Search Closed Sources: Purchase Technical Data](#)

[LAPSUS\\$](#) has purchased credentials and session tokens from criminal underground forums. <sup>[2]</sup>

Enterprise [T1593 .003 Search Open Websites/Domains: Code Repositories](#)

[LAPSUS\\$](#) has searched public code repositories for exposed credentials. <sup>[2]</sup>

Enterprise [T1489 Service Stop](#)

[LAPSUS\\$](#) has shut down virtual machines from within a victim's on-premise VMware ESXi infrastructure. <sup>[5]</sup>

Enterprise [T1199 Trusted Relationship](#)

[LAPSUS\\$](#) has accessed internet-facing identity providers such as Azure Active Directory and Okta to target specific organizations. <sup>[2]</sup>

Enterprise [T1552 .008 Unsecured Credentials: Chat Messages](#)

[LAPSUS\\$](#) has targeted various collaboration tools like Slack, Teams, JIRA, Confluence, and others to hunt for exposed credentials to support privilege escalation and lateral movement. <sup>[2]</sup>

Enterprise [T1204 User Execution](#)

[LAPSUS\\$](#) has recruited target organization employees or contractors who provide credentials and approve an associated MFA prompt, or install remote management software onto a corporate workstation, allowing [LAPSUS\\$](#) to take control of an authenticated system. <sup>[2]</sup>

Enterprise [T1078 Valid Accounts](#)

[LAPSUS\\$](#) has used compromised credentials and/or session tokens to gain access into a victim's VPN, VDI, RDP, and IAMs. <sup>[2][5]</sup>

[.004 Cloud Accounts](#)

[LAPSUS\\$](#) has used compromised credentials to access cloud assets within a target organization. [\[2\]](#)

Mobile [T1451 SIM Card Swap](#)

[LAPSUS\\$](#) has used SIM swapping to gain access to victims' mobile devices. [\[6\]\[7\]](#)

---

Source: <https://attack.mitre.org/groups/G1004/>