K logix
Be confident.

DECEMBER 2024 | THREAT INTEL NEWSLETTER

Weak Links: Exploiting the Supply Chain

C-Suite level threat review by applicable business area addressing active threats.

Reflecting on the 2024 threat landscape reveals the growing effectiveness and prominence of supply chain attacks. Internal tracking and external reports confirm a sharp rise in this attack-type in 2024. This report examines the threat actor LAPSUS$ who is notorious for conducting supply chain compromise. LAPSUS$ came to mind following a recent FBI alert on a surge in fraudulent emergency data requests (EDRs), a tactic LAPSUS$ has employed for some time. This report also examines VEILDrive, a recent threat campaign that exploits third-party relationships to conduct its nefarious activities. As security leaders start to strategize for 2025, a key part of that strategy should be implementing robust controls to safeguard against supply chain risk.

LAPSUS$:

LAPSUS$ is a loosely organized transnational crime group whose members have historically included teenagers. Despite its members' youth, LAPSUS$ has gained notoriety for its adeptness at social engineering and success in supply chain compromise. It often targets downstream vendors in sectors like telecommunications, technology and IT services.

VEILDrive Campaign:

The threat campaign, VEILDrive, discovered in September 2024, is likely being orchestrated by Russian threat actors. VEILDrive led to the compromise of a critical infrastructure company in the United States. The campaign's success relied on the earlier breach of a third-party IT support company as well as the use of common Microsoft services to facilitate phishing and command-and-control (C2) operations.

LAPSUS$

Threat Level: Medium

Attack:

LAPSUS$ conducts thorough reconnaissance on an organization prior to an attack, meticulously studying its structure and supply chain relationships (MITRE T1591.002). In its 2022 breach of the identity provider, Okta, LAPSUS$ succeeded by compromising a third-party customer support center (MITRE T1566). LAPSUS$ is also known to target downstream vendors. For example, LAPSUS$ will target telecommunication companies to conduct SIM swapping, which is when a threat actor transfers an individual's phone number to its own devices, enabling the circumvention of MFA controls. SIM swapping relies on information gathered from various sources like open-source intelligence and fraudulent EDRs (MITRE T1593). To get a company to respond to fraudulent EDR, LAPSUS$ will use compromised email accounts of police departments and government agencies.

Remediation:

- Implement secure account recovery methods that include identity verification through multiple channels. For example, help desk personnel can use both call-back and email verification for account recovery requests.
- Regularly assess the security posture of third-party vendors, focusing on their vulnerability to social engineering.
- Develop joint incident response plans with key third-party vendors to ensure swift action in the event of a security breach.

VEILDrive Campaign

Threat Level: Medium

Attack:

To gain initial access to the victim organization, the threat actor leveraged a previously compromised account from an IT support company. The threat actor used this account to pose as a trusted IT team member and request access to an employee's device via Microsoft Teams, exploiting trust between the employee and the third-party IT provider (MITRE T1566.003). Once access was obtained, the threat actor downloaded a remote monitoring and management (RMM) tool hosted on the SharePoint of a different compromised organization (MITRE T1219); the use of SharePoint likely helped the attacker evade detection. The attacker then downloaded malware and created scheduled tasks to periodically download an RMM tool called LiteManager, establishing persistence (MITRE T1053). The attacker also used OneDrive as a command-and control server. This cloud-based C2 method allows the attacker to evade traditional detection mechanisms, making it harder for security tools to flag the malicious activity.

Remediation:

- Consider restricting the Microsoft Teams feature that permits one-on-one chats with accounts outside of the organization.
- Expand social engineering training to include scenarios involving impersonation of trusted personnel. Emphasize identifying red flags that signal unusual or out-of-the-ordinary requests, even from seemingly legitimate sources.
- Monitor for unauthorized RMM tools.

LAPSUS$:

- **An overview of LAPSUS$, including their capabilities and techniques:** https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf
- **Review of how threat actors, such as LAPSUS$, use fraudulent EDRs:** https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergency-data-requests/

VEILDrive Campaign:

- **Analysis of how the campaign was uncovered and the methods used to compromise an organization:** https://www.hunters.security/en/blog/veildrive-microsoft-services-malware-c2
- **Succinct overview of the threat campaign:** https://thehackernews.com/2024/11/veildrive-attack-exploits-microsoft.html

How K logix Can Help

Technology Advisory

- Email Security
- Endpoint Detection and Response (EDR)
- Identity and Access Management (IAM)
- Managed Security Service Provider (MSSP)
- Security Information and Event Management (SIEM)
- Cloud Security Posture Management (CSPM)
- SaaS Security Posture Management (SaaS)

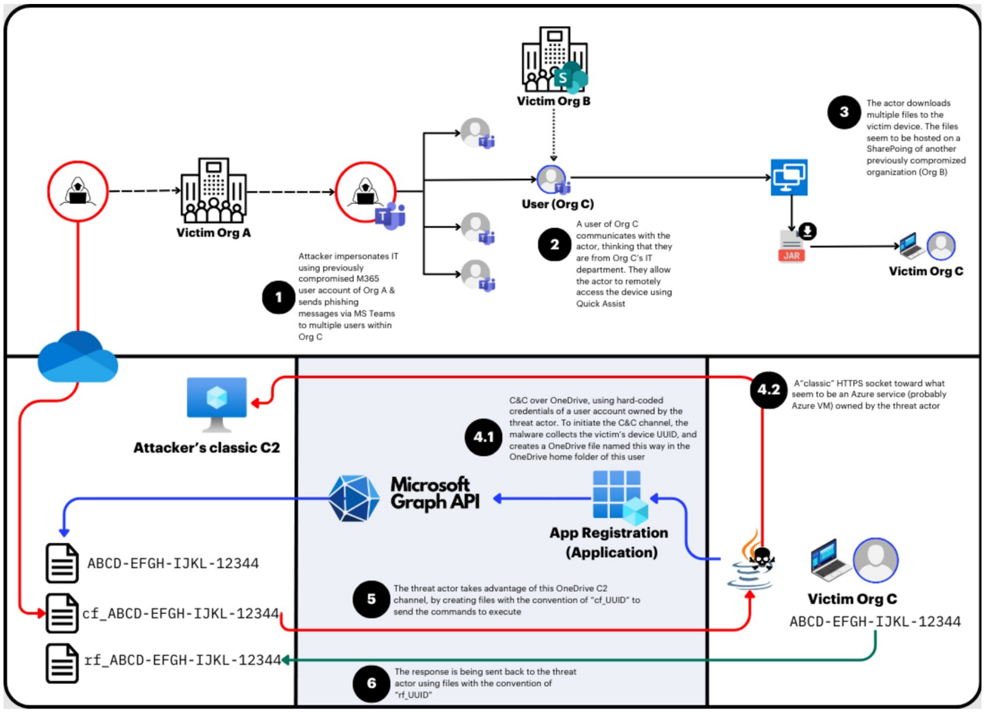
Program Advisory

- Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
- Cloud Security Maturity
- Identity and Access Management Program Maturity

Threat Intelligence

- Notification to customers of threats
- On-demand briefings
- Threat exposure workshops
- User awareness training seminars
- Monthly and quarterly threat intelligence reports

Summary of the VEILDrive Campaign Attack Flow:



1 Attacker impersonates IT using previously compromised M365 user account of Org A & sends phishing messages via MS Teams to multiple users within Org C

2 A user of Org C communicates with the actor, thinking that they are from Org C's IT department. They allow the actor to remotely access the device using Quick Assist

3 The actor downloads multiple files to the victim device. The files seem to be hosted on a SharePoing of another previously compromized organization (Org B)

4.1 C&C over OneDrive, using hard-coded credentials of a user account owned by the threat actor. To initiate the C&C channel, the malware collects the victim's device UUID, and creates a OneDrive file named this way in the OneDrive home folder of this user

4.2 A"classic" HTTPS socket toward what seem to be an Azure service (probably Azure VM) owned by the threat actor

5 The threat actor takes advantage of this OneDrive C2 channel, by creating files with the convention of "cf_UUID" to send the commands to execute

6 The response is being sent back to the threat actor using files with the convention of "rf_UUID"

Source: https://www.hunters.security/en/blog/veildrive-microsoft-services-malware-c2

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.