AL2025_42 Fake Microsoft Teams Installers Distribute Oyster Malware (September 29th , 2025)

Description

Cybercriminals are tricking users into downloading fake Microsoft Teams installers from malicious websites promoted through search engine ads and manipulated search results. These fraudulent sites closely imitate Microsoft's official download pages but instead deliver the **Oyster backdoor** malware. Once installed, the malware gives attackers persistent access to the victim's computer, enabling them to steal data, execute commands, and install additional malicious tools.

Attack Details

- Malicious domains, such as teams-install[.]top, impersonate Microsoft's official Teams download site.
- The fake "MSTeamsSetup.exe" is code-signed with stolen or fraudulent certificates to appear legitimate.
- When executed, the installer drops a malicious DLL (**CaptureService.dll**) into the %APPDATA%\Roaming directory.
- Persistence is maintained via a scheduled task named "CaptureService" that runs every 11 minutes.
- Oyster provides attackers with capabilities to execute commands, deploy additional payloads, and exfiltrate data.
- Similar malvertising campaigns previously delivered Oyster through fake PuTTY and Chrome installers.

Remediation

- **Download Software from Official Sources: Only use Microsoft's official domain (https://www.microsoft.com) to download Teams and other applications.**
- **Block Malvertising Domains: Update web filters and DNS security tools to block suspicious domains and ads.**
- **Monitor for Persistence Mechanisms: Check for unusual scheduled tasks such as "CaptureService."**
- **Endpoint Protection: Ensure antivirus and EDR solutions are updated to detect Oyster-related activity.**
- **User Awareness: Train employees to avoid clicking on sponsored search results when downloading enterprise software.**

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Abrams, L. (2025, September 27). Fake Microsoft Teams installers push Oyster malware via malvertising. BleepingComputer. Retrieved from https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-installers-push-oyster-malware-via-malvertising/

- CybersecurityNews. (2025, September 27). Weaponized Microsoft Teams installer distributes Oyster backdoor via malvertising. CybersecurityNews. Retrieved September 27, 2025, from https://cybersecuritynews.com/weaponized-microsoft-teams-installer/