Fake Microsoft Teams installers push Oyster malware via malvertising

Data: 2025-09-27 19:49:35

Autor: Inteligência Against Invaders

Hackers have been spotted using SEO poisoning and search engineadvertisements to promote fake

Microsoft Teams installers that infect Windows devices with the Oyster backdoor, providing initial

access to corporate networks.

The Oyster malware, also known as Broomstick and CleanUpLoader, is a backdoor that first appeared in mid-2023 and has since been linked to multiple campaigns. The malware provides attackers with remote access to infected devices, allowing them to execute commands, deploy additional payloads, and transfer files.

Oyster is commonly spread through malvertising campaigns that impersonate popular IT tools, such as Putty and WinSCP.Ransomware operations, like Rhysida, have also utilized the malware to breach corporate networks.

Fake Microsoft Teams installer pushes malware

In a new malvertising and SEO poisoning campaign spotted by Blackpoint SOC, threat actors are promoting a fake site that appears when visitors search for “Teams download.”

[IMAGEM REMOVIDA]

[IMAGEM REMOVIDA]VirusTotal] was code-signed with certificates from”4th State Oy” and “NRM NETWORK RISK MANAGEMENT INC” to add legitimacy to the file.

However, when executed, the fake installer dropped a maliciousDLL named CaptureService.dll [VirusTotal] into the %APPDATA%Roaming folder.

For persistence, the installer creates a scheduled task named”CaptureService” to execute the DLL every11 minutes, ensuring the backdoor remains active even on reboots.

This activity resembles previous fake Google Chrome and Microsoft Teams installers that pushed Oyster, highlighting how SEO poisoning and malvertising remain a popular tactic for breaching corporate networks.

“This activity highlights the continued abuse of SEO poisoning and malicious advertisements to

deliver commodity backdoors under the guise of trusted software," concludes Blackpoint.

"Much like the fake PuTTY campaigns observed earlier this year, threat actors are exploiting user trust in search results and well-known brands to gain initial access."

As IT admins are a popular target for gaining access to credentials with high privileges, they are advised only to download software from verified domains and to avoid clicking on search engine advertisements.

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

You may also like: