Malicious Teams Installers Drop Oyster Malware

Archived: 2026-04-05 19:43:11 UTC

The Blackpoint SOC is tracking a new campaign where threat actors are abusing SEO poisoning and malvertising to lure users into downloading a fake Microsoft Teams installer. Victims searching for Teams online are redirected to rogue ads and fraudulent download pages, where they are offered a malicious **MSTeamsSetup.exe** instead of the legitimate client. This activity closely resembles tactics seen in earlier fake PuTTY campaigns, highlighting a recurring trend of adversaries weaponizing trusted software brands to gain initial access.

Execution of the fake installer results in the deployment of the Oyster backdoor, also known as Broomstick. Oyster is a modular, multistage backdoor that provides persistent remote access, establishes Command and Control (C2) communications, collects host information, and enables the delivery of follow-on payloads. By hiding behind a widely used collaboration platform, Oyster is well positioned to evade casual detection and blend into the noise of normal enterprise activity.

This campaign highlights how threat actors are pairing malvertising with commodity malware families to lower the barriers to infection. By exploiting user trust in familiar enterprise software and search engine results, attackers increase their chances of successful compromise while maintaining stealthy, long-term access. Organizations should encourage personnel to use bookmarks and verified vendor domains when downloading software and remain vigilant to the fact that even common productivity tools can be abused as vehicles for malware delivery.

Key Findings

- Threat actors are leveraging SEO poisoning and malicious advertisements to trick users into downloading backdoored versions of Microsoft Teams from spoofed websites.
- These fake installers mimic the legitimate Teams client but silently deploy a persistent backdoor in the background without user awareness.
- The backdoor, known as Oyster (or Broomstick), enables remote access, gathers system information, and supports delivery of additional payloads while evading detection through stealthy execution.
- This activity mirrors tactics seen in earlier fake PuTTY campaigns, demonstrating a continued trend of adversaries abusing trusted software to establish initial access.
- Organizations should download collaboration and administrative tools only from verified sources, ideally using saved bookmarks, rather than relying on search engine results.
- Blackpoint has observed this killchain bypass some traditional AV/EDR Vendors

Observed Killchain

Oyster Joins the Call

The Blackpoint SOC is tracking a new campaign delivering the Oyster backdoor through trojanized Microsoft Teams installers. These malicious installers are being distributed through a combination of SEO poisoning and malvertising, designed to socially engineer users into downloading what appears to be a legitimate version of Microsoft Teams from spoofed websites.

In one identified campaign, the malware was delivered from the domain **teams-install[.]top** When users searched for “teams download” via search engines, they were presented with a malicious sponsored advertisement that closely mimicked the official Microsoft download portal. Clicking on the ad redirected users to the spoofed site, where a file named **MSTeamsSetup.exe** was served, masquerading as a legitimate Teams client.

Figure 1: The malicious domain serving the fake Microsoft Teams Installer.

Analysis of the binaries also revealed that the malicious installers are signed with untrustworthy certificates in an attempt to appear legitimate. The **MSTeamsSetup.exe** samples we examined were signed by issuers such as **4th State Oy** and **NRM NETWORK RISK MANAGEMENT INC.** By attaching a digital signature, threat actors aim to bypass basic trust checks and reduce suspicion from both end users and security controls that flag unsigned executables.

Execution of the trojanized installer drops a DLL named **CaptureService.dll** into a randomly generated folder under **%APPDATA%\Roaming**. It then creates a scheduled task named **CaptureService**, configured to regularly invoke the DLL, providing persistence on the host. The scheduled task executes **rundll32.exe** with **CaptureService.dll** as its payload, establishing the Oyster backdoor.

The execution of this trojanized installer results in the following kill chain:

Figure 2: The resulting process tree associated with execution of the trojanized installer.

Oyster, also known as Broomstick, is a modular backdoor that enables remote access, system profiling, and deployment of additional payloads. Its lightweight execution and use of DLL sideloading via **rundll32.exe** allow it to blend into normal Windows activity while maintaining persistence. In this campaign, Oyster was observed communicating with **nickbush24[.]com** and **techwisenetwork[.]com,** attacker controlled C2 domains.

This activity highlights the continued abuse of SEO poisoning and malicious advertisements to deliver commodity backdoors under the guise of trusted software. 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. To reduce exposure, organizations

should encourage personnel to download collaboration tools only from verified Microsoft domains and avoid reliance on search engine advertisements for critical software.

Indicators of Compromise (IOCs)

MSTeamsSetup.exe	9dc86863e3188912c3816e8ba21eda939107b8823f1afc190c466a7d5ca708d1
MSTeamsSetup.exe	ac5065a351313cc522ab6004b98578a2704d2f636fc2ca78764ab239f4f594a3
Setup.exe	512D7EFB22BC59C84683F931D5AD1E1A092791EEFF20B45DF0E37864A95EA4D3
setup_v12.8.exe	035945729AD4E4B7C6CE4D5760C5F59BAF35A74CD7EB75EEDC91135F0BAE34FC
CaptureService.dll	d47f28bf33f5f6ee348f465aabbfff606a0feddb1fb4bd375b282ba1b818ce9a
CaptureService.dll	d46bd618ffe30edea56561462b50eb23feb4b253316e16008d99abb4b3d48a02
SecurityCore.dll	E764CDE2EC7A245E8C886453783DC1192791B15B34C4A603379DCB5EFFD097D6
rororordl.dll	C4856A275BDEE556B6E771B27BD59347D97FC5F6404EC8E8D8D75833AB5F7B6B
Ads.dll	90b633cacfa185dd912a945f370e14191644ecff1300dbce72e2477171753396
CaptureService	Malicious Scheduled Task
team[.]frywow[.]com	Malvertising Domain
teams-install[.]icu	Malvertising Domain
teams-install[.]top	Malvertising Domain
anydesksoftware[.]net	Malvertising Domain
nickbush24[.]com	Oyster C2
techwisenetwork[.]com	Oyster C2
maddeehot[.]online	Oyster C2
server-na-qc2[.]farsafe[.]net	Oyster C2
urbangreencorner[.]com	Oyster C2
gloitch[.]com	Oyster C2
zephalon[.]com	Oyster C2
doctorreportcard[.]com	Oyster C2
185.28.119[.]166	Oyster C2
45.86.230[.]127	Oyster C2
146.19.49[.]226	Oyster C2
149.56.95[.]175	Oyster C2

185.28.119[.]252	Oyster C2
45.66.248[.]112	Oyster C2
54.39.83[.]187	Oyster C2
185.28.119.228	Oyster C2
4th State Oy	Malicious Cert Signer
NRM NETWORK RISK MANAGEMENT INC.	Malicious Cert Signer
Management Performance Auto Service Ltd.	Malicious Cert Signer

Recommendations

- Download software only from official vendor domains and use saved bookmarks instead of relying on search results or ads.
- Use allowlisting or reputation controls to block unsigned or untrusted installers.
- Monitor for new scheduled tasks in **%APPDATA%**, especially ones named **CaptureService**.
- Monitor for **rundll32.exe** launched by installers or loading DLLs from suspicious directories.
- Monitor for newly registered or suspicious domains in network traffic.
- Train users on SEO poisoning and malvertising risks to reduce successful lures.

DATE PUBLISHED September 26, 2025

AUTHORSam Decker, Nevan Beal

Inside the SOC Episode #002, April 7th, 10:00 AM MT

Roadk1ll, a new malware strain is already being observed in the wild.

Inside the SOC Episode #002, we'll break down how it works, along with a real MSP compromise and modern cloud attack patterns

Live on April 7 at 10:00 AM MT

Save your seat

Source: https://blackpointcyber.com/blog/malicious-teams-installers-drop-oyster-malware/