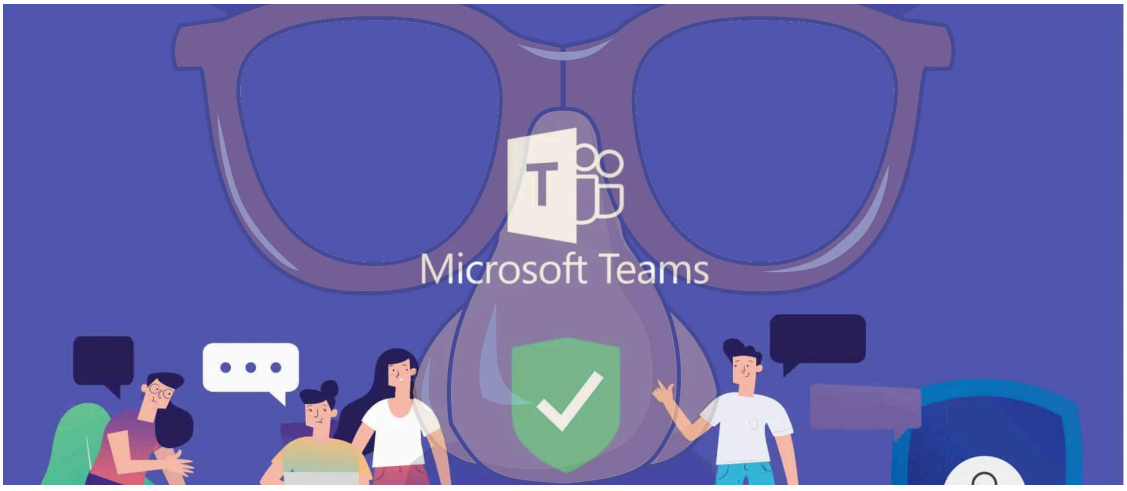
Fake Microsoft Teams updates lead to Cobalt Strike deployment

By Ionut Ilascu

Published: 2020-11-09 · Archived: 2026-04-06 01:14:20 UTC

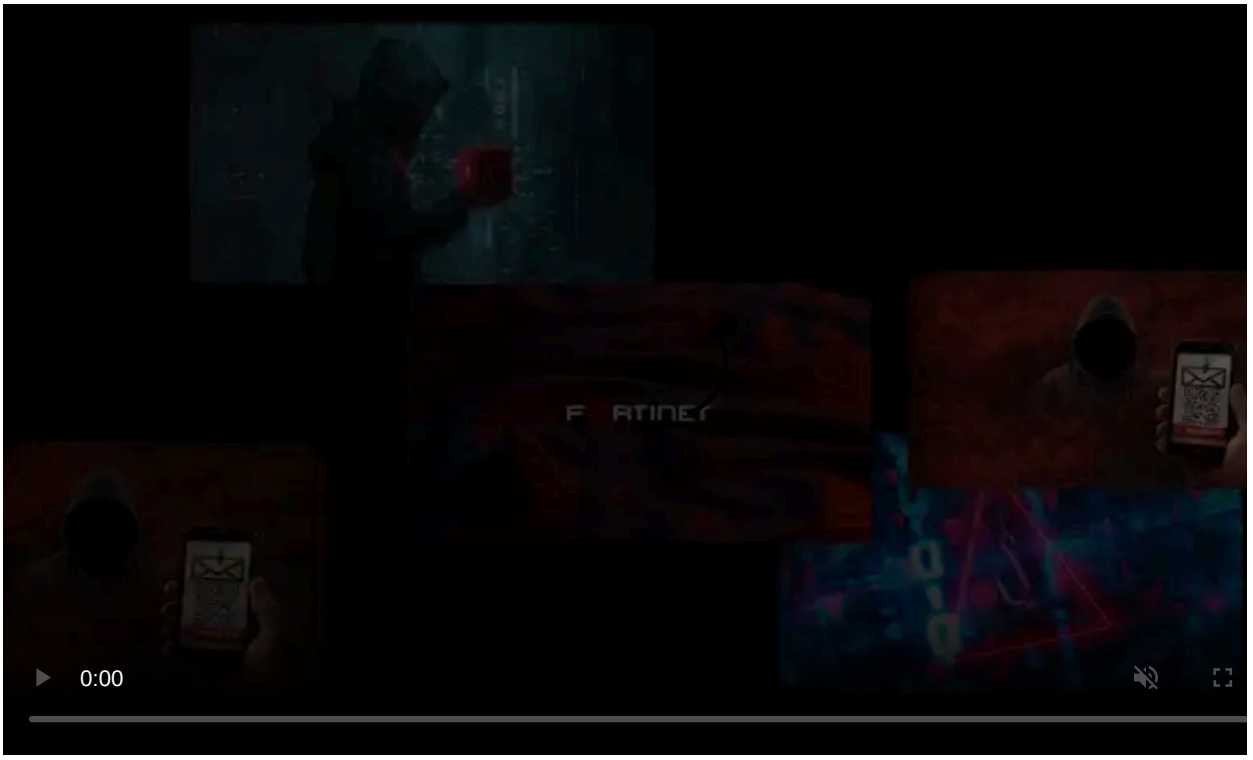


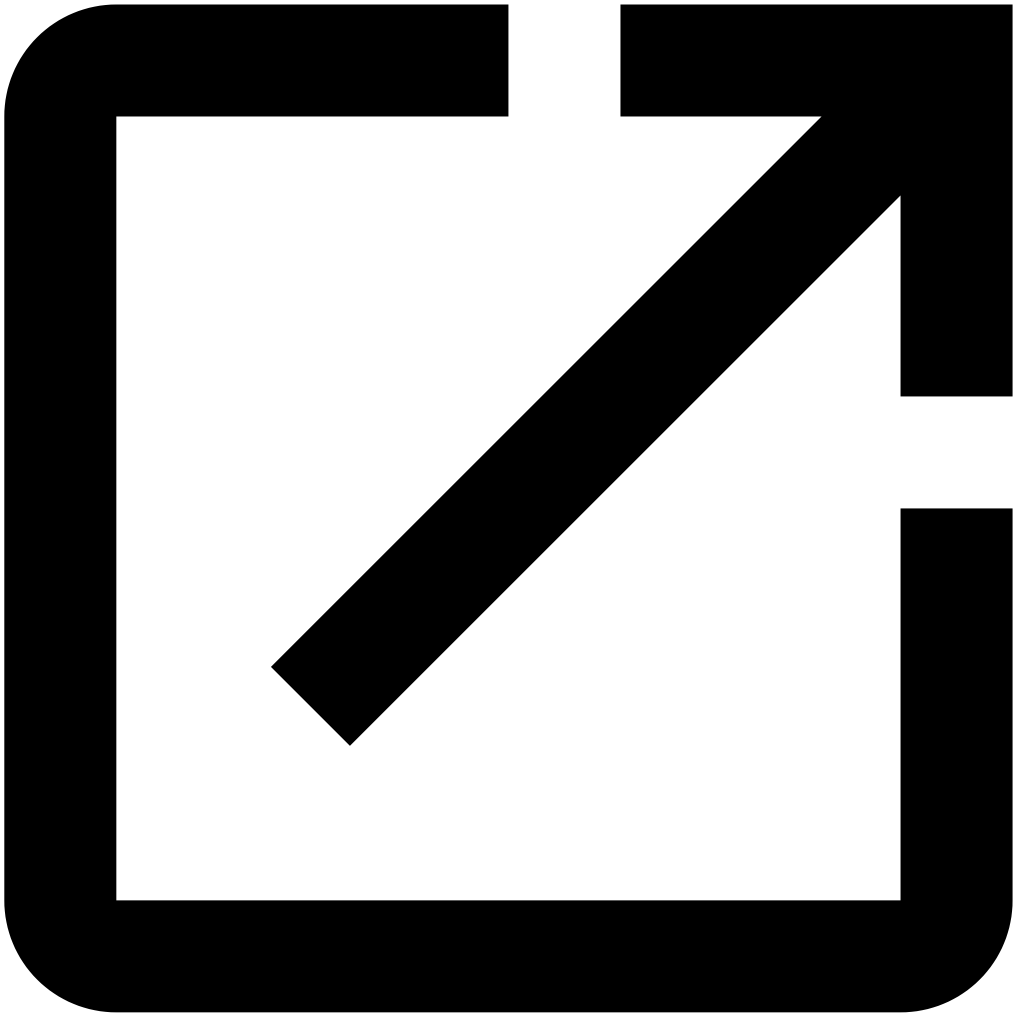
Ransomware operators are using malicious fake ads for Microsoft Teams updates to infect systems with backdoors that deployed Cobalt Strike to compromise the rest of the network.

The attacks target organizations in various industries, but recent ones focused on the education sector (K-12), which depends on videoconferencing solutions due to Covid-19 restrictions.

From infostealer to Cobalt Strike

In a non-public security advisory seen by BleepingComputer, Microsoft is warning its customers about these FakeUpdates campaigns, offering recommendations that would lower the impact of the attack via its Defender ATP service.


0:00



FakeUpdates attacks were seen in 2019 delivering DoppelPaymer ransomware. But this year, the malvertising campaigns dropped WastedLocker and showed technical evolution.

For instance, they started using signed binaries and various second-stage payloads.

More recently, the attackers exploited the ZeroLogon (CVE-2020-1472) critical vulnerability to gain admin access to the network. This occurred via the SocGholish JavaScript framework, found earlier this year on dozens of hacked newspaper sites owned by the same company.

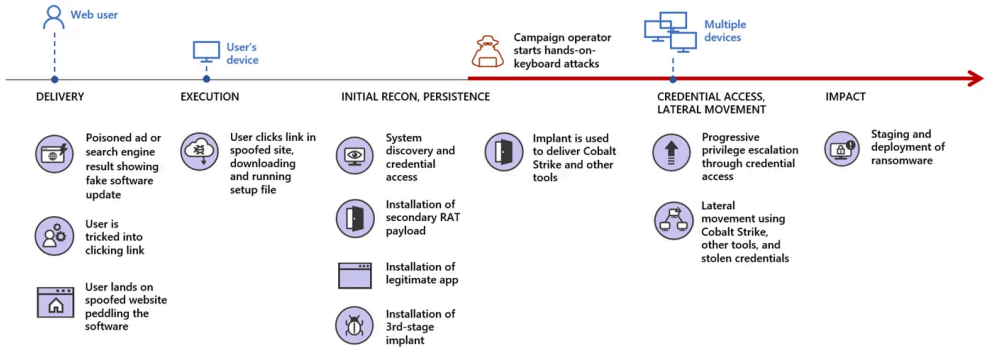
Planting the malicious fake ads that lure unsuspecting users into clicking it to install an update was possible by poisoning search engine results or through malicious online advertisements.

In at least one attack Microsoft detected, the crooks purchased a search engine ad that caused top results for Teams software to point to a domain under their control.

Clicking on the link downloaded a payload that executed a PowerShell script to retrieve more malicious content. It also installed a legitimate copy of Microsoft Teams on the system to keep victims unaware of the attack.

Microsoft says that in many cases the initial payload was Predator the Thief infostealer, which sends the attacker sensitive information like credentials, browser, and payment data. Other malware distributed this way includes Bladabindi (NJRat) backdoor, and ZLoader stealer.

The malware also downloaded other payloads, with Cobalt Strike beacons being among them, thus allowing the attacker to discover how they could move laterally across the network.



source: Microsoft

In several of the observed attacks, the last stage was detonating file-encrypting malware on the network computers.

Microsoft is warning that the same patterns seen in the FakeUpdates campaigns using Teams updates as lure were observed in at least six others, suggesting the same actor behind them. In some variations of the same theme, the attacker used the IP Logger URL shortening service.

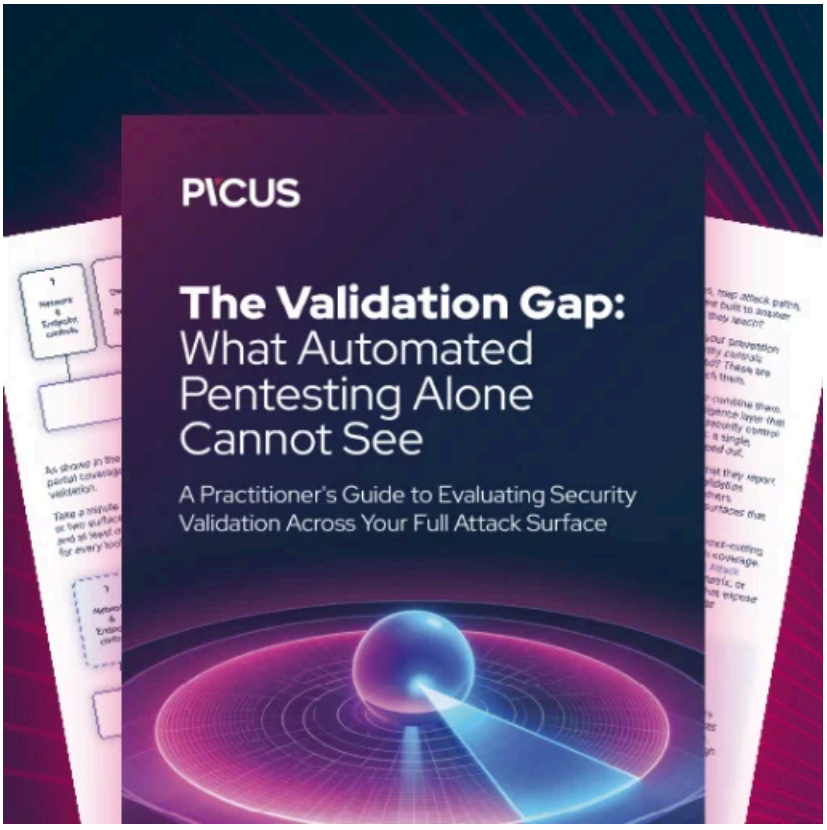
Mitigation advice

Microsoft recommends using web browsers that can filter and block malicious websites (scam, phishing, malware and exploit hosts) along with using strong, random passwords for local administrators.

Limiting admin privileges to essential users and avoiding domain-wide service accounts that have the same permissions as an administrator are also on the list of measures that would reduce the impact of an attack.

To minimize the attack surface, Microsoft recommends blocking executable files that do not meet specific criteria such as prevalence and age or are outside a regularly maintained trusted list.

Blocking JavaScript and VBScript code from downloading executable content also adds to the defenses of the environment.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/