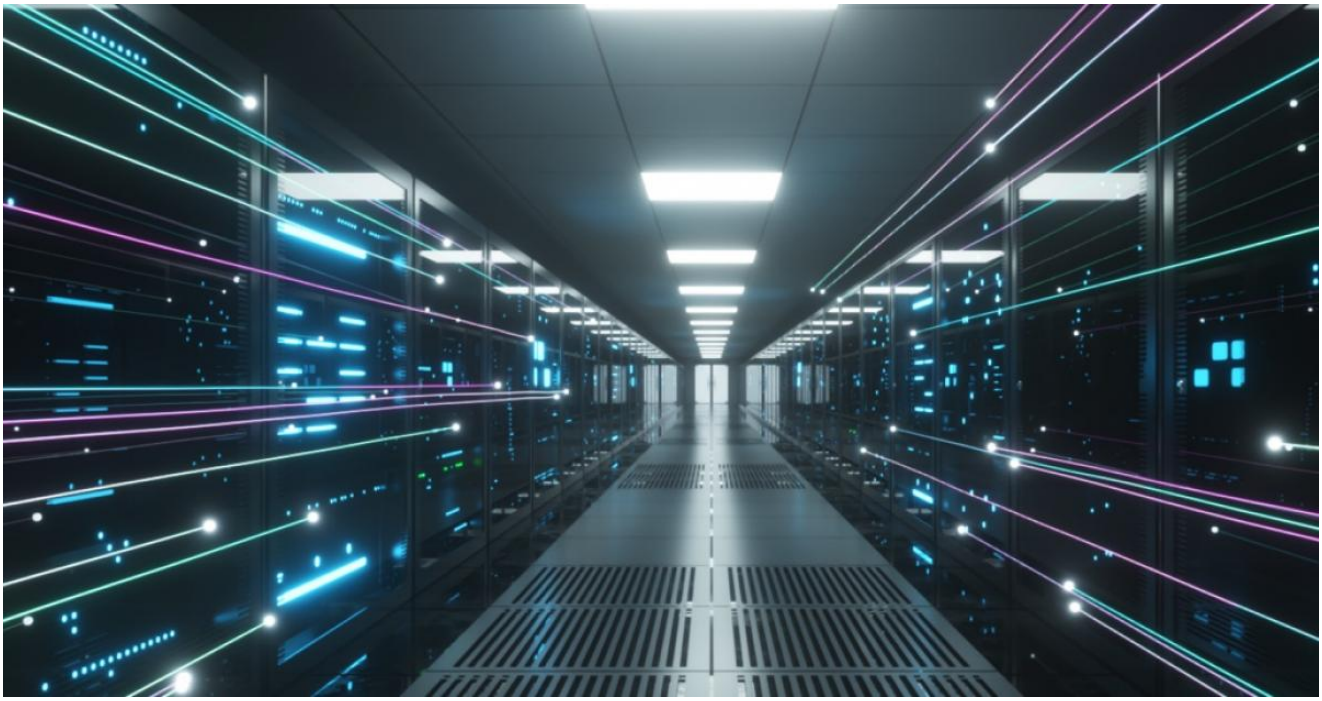
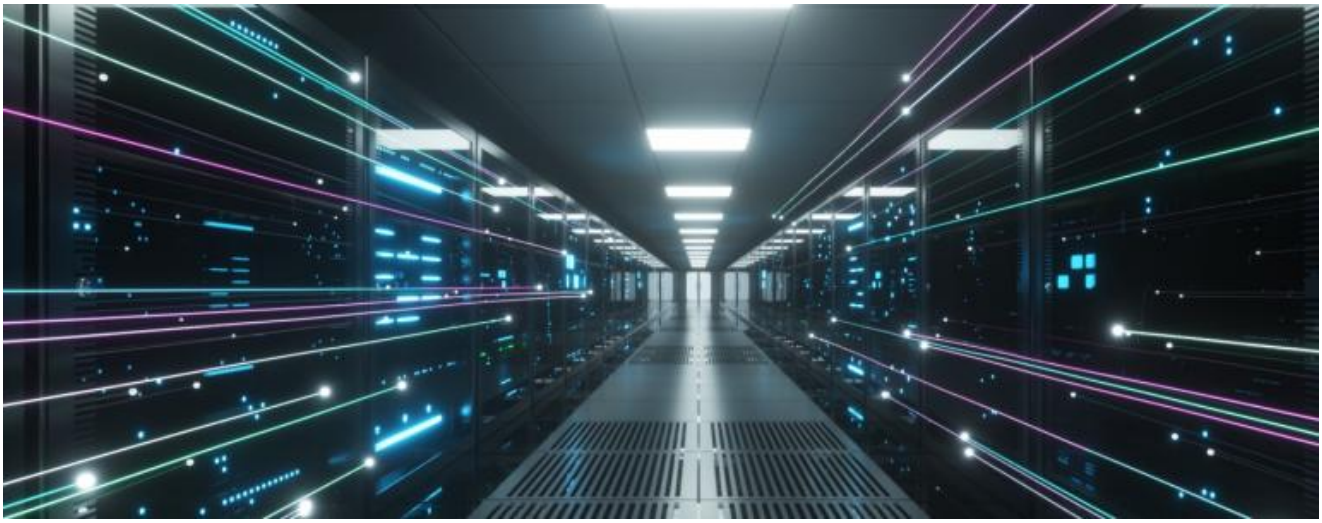
Cobalt Strike: Favorite Tool from APT to Crimeware

proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware

June 23, 2021



Blog
Threat Insight
Cobalt Strike: Favorite Tool from APT to Crimeware



June 29, 2021 Selena Larson and Daniel Blackford

(Updated 8/18/2021 at the request of a third-party)

Key Findings

- Malicious use of Cobalt Strike in threat actor campaigns is increasing.
- Threat actor use of Cobalt Strike increased 161 percent from 2019 to 2020 and remains a high-volume threat in 2021.
- Cobalt Strike is currently used by more cybercrime and general commodity malware operators than APT and espionage threat actors.

Overview

In 2021, Cobalt Strike is appearing in Proofpoint threat data more frequently than ever. Cobalt Strike is a legitimate security tool used by penetration testers to emulate threat actor activity in a network. However, it is also increasingly used by malicious actors – Proofpoint saw a 161 percent increase in threat actor use of the tool from 2019 to 2020. This aligns with observations from other security firms as more threat actors adopt hacking tools in their operations.

When mapped to the MITRE ATT&CK framework, Proofpoint's visibility into the attack chain focuses on Initial Access, Execution, and Persistence mechanisms. That is: How are threat actors attempting to compromise hosts and what payloads are they deploying first? Our corpus of threat actor data includes criminal and state-associated threat actor groups. Based on our data, Proofpoint assesses with high confidence that Cobalt Strike is becoming increasingly popular among threat actors as an initial access payload, not just a second-stage tool threat actors use once access is achieved, with criminal threat actors making up the bulk of attributed Cobalt Strike campaigns in 2020.

Background

In December 2020, the world learned about an expansive and effective espionage campaign that successfully backdoored the popular network monitoring software SolarWinds. Investigators revealed tools used by the threat actors included Cobalt Strike Beacon. This campaign was attributed to threat actors working for Russia's Foreign Intelligence Service – a group with Cobalt Strike in their toolbox since at least 2018. This high-profile activity was part of a clever attack chain enabling advanced threat actors to surreptitiously compromise a relatively small number of victims. The tool used, and customized to fit their needs, is almost a decade old but increasingly popular.

Cobalt Strike debuted in 2012 in response to perceived gaps in an existing red team tool, the Metasploit Framework. In 2015, Cobalt Strike 3.0 launched as a standalone adversary emulation platform. By 2016, Proofpoint researchers began observing threat actors using Cobalt Strike.

Historically, Cobalt Strike use in malicious operations was largely associated with well-resourced threat actors, including large cybercrime operators like TA3546 (also known as FIN7), and advanced persistent threat (APT) groups such as TA423 (also known as Leviathan or APT40). Proofpoint researchers have attributed two-thirds of identified Cobalt Strike campaigns from 2016 through 2018 to well-resourced cybercrime organizations or APT groups. That ratio decreased dramatically the following years – between 2019 and present, just 15 percent of Cobalt Strike campaigns were attributable to known threat actors.

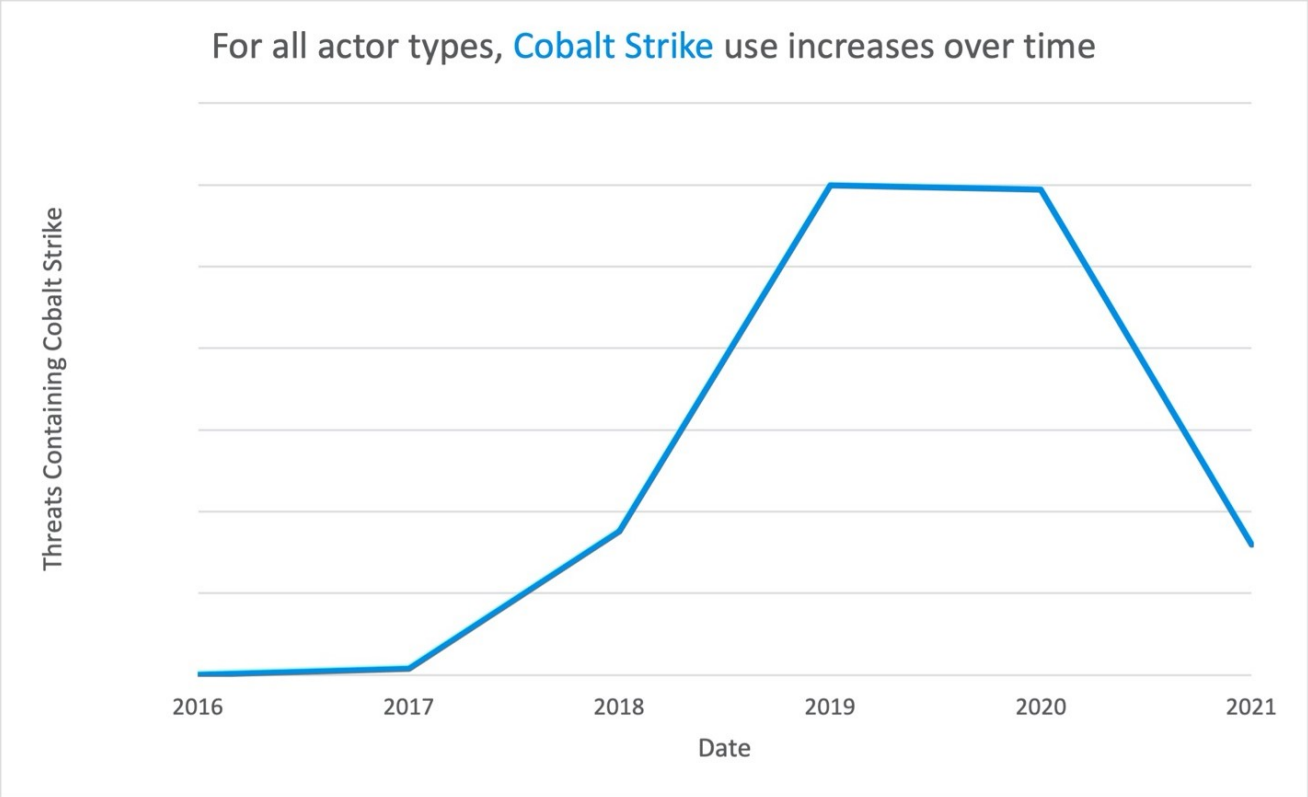


Figure 1: Number of email messages associated with a Cobalt Strike payload observed over time. Note: 2021 figures include data through May 2021.

Threat actors can obtain Cobalt Strike in a variety of ways: purchasing it directly from the vendor's website, which requires verification; buying a version on the dark web via various hacking forums; or using cracked, illegitimate versions of the software. In March 2020, a cracked version of Cobalt Strike 4.0 was released and made available to threat actors.

Cobalt Strike's Appeal

Cobalt Strike is used by a diverse array of threat actors, and while it is not unusual for cybercriminal and APT actors to leverage similar tooling in their campaigns, Cobalt Strike is unique in that its built-in capabilities enable it to be quickly deployed and operationalized regardless of actor sophistication or access to human or financial resources. The job of simulating actor attacks and penetrating defenses might become a bit more straightforward when both sides are using the same tool.

Cobalt Strike is also session-based — that is, if threat actors can access a host and complete an operation without needing to establish ongoing persistence, there will not be remaining artifacts on the host after it is no longer running in-memory. In essence: they can hit it and forget it.

Threat actors can also use the malleability of Cobalt Strike to create customized builds that add or remove features to achieve objectives or evade detection. For example, APT29 frequently uses custom Cobalt Strike Beacon loaders to blend in with legitimate traffic or evade analysis.

For defenders, customized Cobalt Strike modules often require unique signatures, so threat detection engineers may be required to play catch-up to Cobalt Strike use in the wild. Cobalt Strike is also appealing to threat actors for its inherent obfuscation. Attribution gets more difficult if everyone is using the same tool. If an organization has a red team actively making use of it, it is possible malicious traffic could be mistaken as legitimate. The software's ease of use can improve the capabilities of less sophisticated actors. For sophisticated actors, why spend development cycles on something new when you already have a great tool for the job?

Proofpoint data shows Cobalt Strike is a popular tool for everything from strategic compromises to noisy, widespread campaigns. The following examples illustrate a small sampling of the types of threat actors leveraging Cobalt Strike tracked by Proofpoint.

Threat Actors

TA800

TA800 is a large crimeware group tracked by Proofpoint since mid-2019. This actor attempts to deliver and install banking malware or malware loaders, including The Trick and BazaLoader. In April 2020, TA800 became the first group observed distributing BazaLoader. In these early campaigns, the threat actor distributed emails with a malicious link to an executable or a landing page hosted on Google Docs with a link to an executable. The executable downloaded the BazaLoader backdoor which in turn downloaded Cobalt Strike. In February 2021, the group pivoted to distributing Cobalt Strike as a first-stage payload via malicious URLs. There has been some evidence suggesting TA800's NimzaLoader is being used to download and execute Cobalt Strike as its secondary payload.

TA547

TA547 is a crimeware actor tracked by Proofpoint since October 2017. This group appears to be interested in distributing primarily banking trojans – including The Trick and ZLoader – to various geographic regions. Since mid-2020, this actor favors using malicious Microsoft Office attachments to distribute malware. In February 2021, TA547 began distributing Cobalt Strike as a second-stage payload for command and control.

TA415

TA415 is an APT actor believed to be associated with People's Republic of China (PRC) state interests. The group has been noted in United States court filings to be tied to PRC's Ministry of State Security. TA415 is also known as Barium and APT41. Proofpoint identified TA415 delivering Cobalt Strike as a first-stage payload in limited campaigns during mid-2020. In September 2020, the United States Department of Justice announced the indictment of several threat actors associated with this threat group, and detailed the threat actors use of Cobalt Strike in the indictment. Based on recent reporting by Group-IB, TA415 used Cobalt Strike in a campaign against an entity in the airlines sector.

The following timeline provides a small sample of threat actor use of Cobalt Strike across cybercrime and APT threats. The selected events were identified based on their significance, and are not representative of the full Cobalt Strike threat landscape.

STRIKE THREATS

JANUARY 2016

FIN7 aka Carabank targeted financial organizations globally, features Cobalt Strike implants

MAY 2017

The Cobalt Group targets banks, banking software vendors, and ATM software and hardware vendors

OCTOBER 2017

Leviathan espionage actor targeted defense and maritime targets in the U.S. and Western Europe

APRIL 2018

APT10 threat actors use Cobalt Strike in attacks on multiple Japanese organizations

AUGUST 2018

TA505 distributes tens of thousands of malicious attachments containing macros which, if enabled, download Cobalt Strike backdoor

NOVEMBER 2018

APT29 targeted multiple industries masquerading as the U.S. Department of State

2019

APT41 threat actors use Cobalt Strike on Indian government computers

Note: The specific timing of this campaign was not detailed in the U.S. Department of Justice indictment.

NOVEMBER 2019

TA2101 targeting German institutions impersonating the Bundeszentralamt fur Steuern, the German Federal Ministry of Finance

JUNE 2020

TA800 leverages COVID-19 themes to distribute BazaLoader > BazaBackdoor > Cobalt Strike

Figure 2: Timeline of threats using Cobalt Strike. Links to the sources are available in the References section.

Attack Chain

Proofpoint has observed dozens of threat actors using Cobalt Strike. However, like their legitimate counterparts, threat actors exhibit many attack paths and use cases of the malicious actor emulation software. Threat actors use different lure themes, threat types, droppers, and payloads. For example, the earliest Cobalt Strike campaigns distributed email threats with malicious document attachments to distribute the malware, but campaigns distributing malicious URLs directly in the email body have overtaken attachments as the more frequently utilized threat type.

While instances of Cobalt Strike being sent directly as an initial payload have dramatically increased, deployment as a second stage payload remains popular. Cobalt Strike has been observed in a variety of attack chains alongside malware such as The Trick, BazaLoader, Ursnif, IcedID, and many more popular loaders. In these cases, the preceding malware typically loads and executes Cobalt Strike. Likewise, there is a wide array of techniques leveraged in cases where Cobalt Strike is delivered directly, such as via malicious macros in weaponized Office documents, compressed executables, PowerShell, dynamic data exchange (DDE), HTA/HTML files, and traffic distribution systems.

After Cobalt Strike has been executed and a Beacon established for C2 communication, actors have been observed attempting to enumerate network connections and dumping Active Directory credentials as they try to move laterally to a network resource such as a Domain Controller, allowing for deployment of ransomware to all networked systems. For example, the Cobalt Strike documentation states:

Use the net dclist command to find the Domain Controller for the domain the target is joined to. Use the net view command to find targets on the domain the target is joined to.

In addition to network discovery and credential dumping, Cobalt Strike Beacon also has the capability to elevate privileges, load and execute additional tools, and to inject these functions into existing running host processes to attempt to avoid detection.

Outlook

Proofpoint researchers anticipate Cobalt Strike will continue to be a commonly used tool in threat actor toolsets. According to internal data, tens of thousands of organizations have already been targeted with Cobalt Strike, based on observed campaigns. We expect this number to increase in 2021.

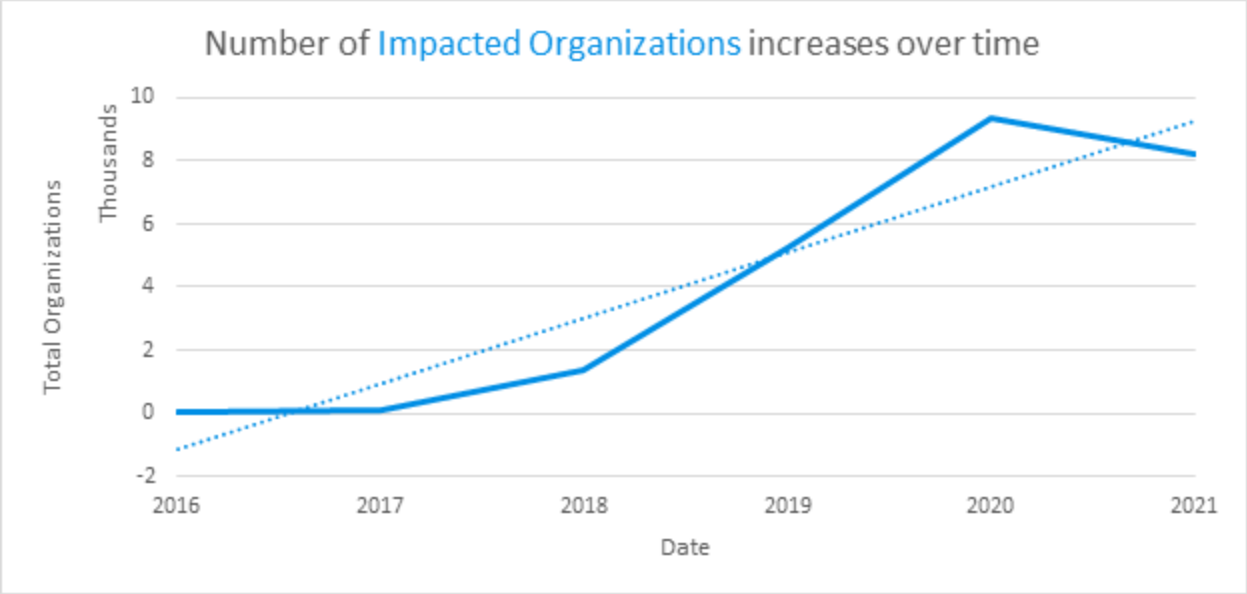


Figure 3: Number of customers targeted by threats using Cobalt Strike

Conclusion

Cobalt Strike is a useful tool, for legitimate security researchers and threat actors alike. Its malleability coupled with its usability makes it a robust and effective tool for siphoning data, moving laterally, and loading additional malware payloads.

Cobalt Strike is not the only red team tool appearing more often in Proofpoint data. Others include Mythic, Meterpreter, and the Veil Framework.

The use of publicly available tooling aligns with a broader trend observed by Proofpoint: Threat actors are using as many legitimate tools as possible, including executing Windows processes like PowerShell and WMI; injecting malicious code into legitimate binaries; and frequently using allowable services like Dropbox, Google Drive, SendGrid, and Constant Contact to host and distribute malware.

References

The following references are associated with the above timeline.

January 2016 – Odinaff: New Trojan used in high level financial attacks

May 2017 – Microsoft Word Intruder Integrates CVE-2017-0199, Utilized by Cobalt Group to Target Financial Institutions

October 2017 – Leviathan: Espionage actor spearphishes maritime and defense targets

April 2018 – APT攻撃者グループ menuPass(APT10) による新たな攻撃を確認

November 2018 – Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign

2019 – Seven International Cyber Defendants, Including “Apt41” Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally

November 2019 – TA2101 plays government imposter to distribute malware to German, Italian, and US organizations

September 2020 – Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity

December 2020 – Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

March 2021 – NimzaLoader: TA800’s New Initial Access Malware

May 2021 – New sophisticated email-based attack from NOBELIUM

Detections

Proofpoint Emerging Threats includes robust detections for Cobalt Strike. The following are a sample of our detections as they relate to the behaviors described in this report.

2028591 ET TROJAN Cobalt Strike Malleable C2 Request YouTube Profile

2028589 ET TROJAN Cobalt Strike Malleable C2 Response O365 Profile M2

2032749 ET TROJAN Cobalt Strike Malleable C2 Amazon Profile

2032746 ET TROJAN Cobalt Strike Malleable C2 QiHoo Profile

2027082 ET TROJAN Observed Malicious SSL Cert CobaltStrike C2

2023629 ET INFO Suspicious Empty SSL Certificate - Observed in Cobalt Strike

2032362 ET TROJAN Cobalt Strike Beacon Activity

2032951 ET TROJAN Observed Cobalt Strike User-Agent

Is your organization protected against malicious threat actors? Learn about Malware protection.

Subscribe to the Proofpoint Blog