Quorum Cyber

Threat Intelligence
Cobalt Strike
Post-Exploitation Tool

TLP Status: White

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control 3

Revision History 3

Related Documents 3

Cobalt Strike 4

Overview 4

Impact 4

Incident Detection 4

Targeted Products 5

Containment, Mitigations & Remediations 5

Indicators of Compromise 5

Threat Group 8

Threat Landscape 8

Mitre Methodologies 8

Further Information 9

Document Control

Revision History

Version	Date	Summary of Changes
1.0	11/05/2023	Initial Report

Related Documents

The following documents are either referenced within, or are related to the content of this document:

Document Name	Date	Version
-	-	-

Cobalt Strike

Overview

Cobalt Strike is a notorious post-exploitation tool that is used by threat actors to gain access to target systems and for the purposes of maintaining persistence. The tool was originally designed as adversary simulation software used to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors[1]. It is often used in conjunction with additional malware payloads, such as: Clop, Conti, Emotet and QakBot. Cobalt strike allows threat actors to simulate legitimate network traffic and evade detection.

Originally a red teaming tool, the malware has since been cracked with reports of malicious activity dating back to at least 2019, the malware has been active for several years, with reports dating back to at least 2019. The exact method of initial access is not clear, but it is likely that threat actors implement social engineering, phishing, or exploit kits to gain a foothold on targeted systems. Cobalt Strike remains a significant threat to organisations and as such, network defenders should be vigilant with regards to monitoring for any signs of Cobalt Strike operations. In addition to its own capabilities, Cobalt Strike leverages the capabilities of other well-known tools such as Metasploit and Mimikatz.

The primary malicious operations associated with Cobalt Strike occur via its ability to establish command and control (C2) communications with target networks, thus creating a persistent access channel between the target and the threat actor. This is achieved through the Beacon feature of the tool, which can be installed as a client for the threat actor on the target system[2]. The Beacon allows files to be uploaded as well as for C2 communications to be sent in a mode of stealth, thus applying the mechanism of persistence.

The post-exploitation tool has been attributed to numerous advanced persistent threat (APT) groups, including the Sangria Tempest (also known as FIN7), Forrest Blizzard (also known as APT28) and Gingham Typhoon (also known as APT40). LockBit ransomware has also recently been observed sideloading Cobalt Strike through Microsoft security tools.

Impact

Successful compromise by Cobalt Strike will result in the establishment of C2 channels between the target and the threat actor systems. The communication channel allows the threat actors to exfiltrate data from the target, compromise additional systems via lateral movement as well as the delivery of additional malware components such as ransomware.

Incident Detection

A comprehensive Endpoint Detection and Response (EDR) solution, such as Microsoft Defender, can provide additional protection against post-exploitation malware threats such as Cobalt Strike. The solution functions with the intent to alert system users of potential breaches and prevent further progress prior to the associated malware applying significant damage.

Additionally, an open-source set of YARA rules, for the detection of the Cobalt Strike post-exploitation tool in network and system scans, can be found within the Google Cloud Threat Intelligence GitHub Repository.

[1] Features | Beacon, C2 Profiles, Attack Packages, and More | Cobalt Strike
[2] Cobalt Strike: How It Became a Favorite Tool of Hackers (esecurityplanet.com)

Targeted Products

- WindowsOS
- MacOS
- LinuxOS

Containment, Mitigations & Remediations

It is advised that an EDR solution, such as the Microsoft Defender suite, is utilised to monitor for the presence of post-exploitation tools such as Cobalt Strike. Additionally, threat hunts can be conducted to detect for successful Cobalt Strike compromise via the YARA rules mentioned previously.

The Cybersecurity & Infrastructure Security Agency recommended that the following mitigation steps are implemented as a protective measure to counteract cyber-attacks associated with the abuse of C2 frameworks such as Cobalt Strike[3]:

- Maintain up-to-date antivirus signatures and engines.
- Ensure that operating system patches are applied as soon as possible.
- Disable File and Printer sharing services.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Do not add users to the local administrator's group, unless this is necessary.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on workstations and servers.
- Scan for and remove suspicious e-mail attachments.
- Restrict user access to websites with suspicious content.
- Exercise caution when using removable media, such as USB drives and external drives.
- Scan all software downloaded from the Internet prior to execution.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs)

Indicators of Compromise

Cobalt Strike Associated File Hashes (SHA256):

- ba95ee90c4e4cb5f04ac023bdd963690b6bb6907ec4e872a498ac498e43674dd
- 6237b5f8b6ee20c3fad9463266a4a7c787f2738f71dc81792cd6a0efe38b8685

[3] MAR-10398871.r1.v2.WHITE.pdf (cisa.gov)

- 0938ad03e8a0fbfc8be6f8fcfe7730849fd0716a387f98a33a5afe356d423a6f
- 22c88741be5ea8c2540177e0679788d28ea64d79a15bedb9ce4880414215d366
- 399a89bb438d1c63d096dec691e0209a9d3feca4b953a4ebbac3b9261355857c
- 5594c9a9d5fb71ee9886dcbee938d70125039952851726760fbd27156fa72029
- 657b9651aa07792ecd8e0a5b013171be078528eb3d2bd50bb5a7628a3dfeb999
- 670c13936c0f868599a05bb46060183ce52eee6395e878b408ed7694c7933e39
- 80842fc68ad1eaecd259596e4a532330a40a74eef4ec54919894c2cd8d68c105
- 87551c0e16b59c46d8692636eebb28805905e2dc37939340b292acc12ca86d41
- 8919125fd72fd2e9e63efe0383f2d3efb842b8736bfbc00384c822afd5827638
- 9f34157b6f5dbf43a5b0b30a64f5ba381b37340f9776f233b83994de2448439c
- a284bbded1bc2e95ee51d4c7170271c0dc56c533ddb0383a77f246553cf25f4a
- a6b559ae918510fae2d4efcba569942d2a4f5553a37f4edb97a411223f5e579a
- e0a5810dbb6e7055ed41d764722f807f7eafa4ba4830d82386f51518b36b507a
- e9649b6b6b52a6cbc61e1c403d12beb0e56f1f9a77c23ad1ae5cf259d7982184
- ea4458d03c6b89ecc3d549a4d61443abbc9bc4c56d45f1c01a7dac5297a7a876
- ef3d3fa3654da8ea930e6138221f1312e522182fbaf1ac759f9ef4f6c0fbf623
- f9af9081fc07cef3788490cb68ea15ae6e6dde4d12fad238593c354911633b5b
- f9deaf0a1a553734cd27789e7e3e99f22d7e922c7cb053c11f8ec43ccee7d2ee

Cobalt Strike Associated IP Addresses:

- 103[.]149[.]200[.]79
- 154[.]88[.]26[.]221
- 82[.]157[.]110[.]128
- 46[.]29[.]164[.]11
- 47[.]107[.]76[.]95
- 101[.]43[.]165[.]220
- 119[.]91[.]45[.]113
- 124[.]222[.]111[.]174
- 152[.]67[.]117[.]125
- 182[.]254[.]240[.]188
- 100[.]42[.]76[.]82
- 101[.]43[.]205[.]85
- 118[.]31[.]8[.]234
- 121[.]37[.]101[.]254

- 139[.]224[.]189[.]177
- 188[.]166[.]179[.]67
- 43[.]154[.]46[.]217
- 47[.]94[.]130[.]42
- 81[.]69[.]221[.]247
- 82[.]156[.]10[.]244

Cobalt Strike Associated URLs:

- hxxp[://]82[.]157[.]161[.]99:1001/ga[.]js
- hxxp[://]iobs[.]pingan[.]com[.]cn:443/audiencemanager[.]js

Cobalt Strike Associated Malware Signatures:

- BackDoor.CobaltStrike.86
- BackDoor.Meterpreter.72
- HEUR/QVM19.1.33EF.Malware.Gen
- HEUR/QVM20.1.3091.Malware.Gen
- HEUR/QVM20.1.33EF.Malware.Gen
- Malicious
- PUA.RiskWare.Cobaltstrike
- Trojan-Downloader.Win64.Agent
- Trojan.BF619EAC0CDF3F68
- Trojan.Generic.zujr
- Trojan.Inject3.1988
- Trojan.Inject3.2700
- Trojan.Win32.CobaltStrike
- Trojan.Win32.CobaltStrike.4!c
- Trojan.Win32.Inject3.horsiq
- Trojan.Win32.Inject3.hpcmug
- Trojan.Win64.Cobaltstrike
- Win.Trojan.CobaltStrike-7899872-1
- Win.Trojan.CobaltStrike-8091534-0
- Win.Trojan.CobaltStrike-904

Threat Group

Cobalt Strike has been attributed as being a post-exploitation tool employed by several APT groups, such as Sangria Tempest (also known as FIN7), Forrest Blizzard (also known as APT28) and Gingham Typhoon (also known as APT40).

Threat Landscape

The stealth capabilities of the Cobalt Strike post-exploitation tool results in significant difficulties with regards to counteracting associated attack efforts as the techniques applied are implemented with the objective of evading detection. However, Cobalt Strike as been a favoured tool of threat actors since at least 2019 and as such, network defenders have significantly enhanced their ability to detected and defend against attacks. As time progresses, it is therefore likely that threat actors will pivot to other post-exploitation toolsets to for the purposes of continued targeting involving the establishment of C2 channels.

Mitre Methodologies

Execution
T1059 - Command and Scripting Interpreter[4]
T1059.001 - Command and Scripting Interpreter: PowerShell[5]

Persistence
T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder[6]

Privilege Escalation
T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder[7]

Defence Evasion
T1112 - Modify Registry[8]

Credential Access
T1539 - Steal Web Session Cookie[9]

Discovery
T1012 - Query Registry[10]
T1082 - System Information Discovery[11]

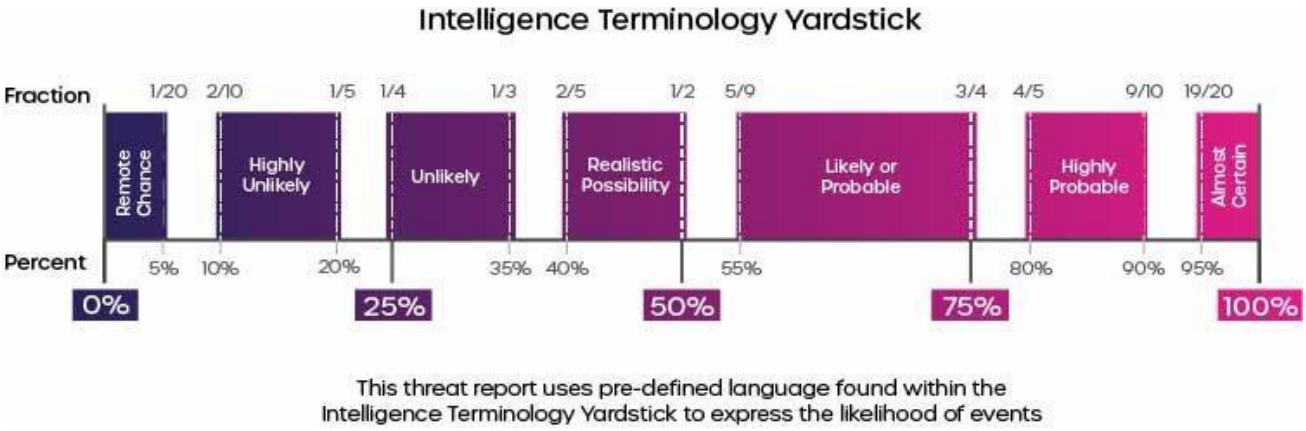
Command and Control
T1071 - Application Layer Protocol[12]
T1071.001 - Application Layer Protocol: Web Protocols[13]

[4] Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®
[5] Command and Scripting Interpreter: PowerShell, Sub-technique T1059.001 - Enterprise | MITRE ATT&CK®
[6] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[7] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[8] Modify Registry, Technique T1112 - Enterprise | MITRE ATT&CK®
[9] Steal Web Session Cookie, Technique T1539 - Enterprise | MITRE ATT&CK®
[10] Query Registry, Technique T1012 - Enterprise | MITRE ATT&CK®
[11] System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®
[12] Application Layer Protocol, Technique T1071 - Enterprise | MITRE ATT&CK®
[13] Application Layer Protocol: Web Protocols, Sub-technique T1071.001 - Enterprise | MITRE ATT&CK®

Further Information

- CISA Cobalt Strike Analysis
- Esecurityplanet Cobalt Strike Report

Intelligence Cut-off Date (ICoD): 11/05/2023 10:00 UTC



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events