

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**

MICROSOFT CORPORATION, a Washington Corporation, FORTRA, LLC, a Delaware Limited Liability Company, and HEALTH-ISAC, INC., a Florida Corporation,

Plaintiffs,

v.

JOHN DOES 1-2, JOHN DOES 3-4 (AKA CONTI RANSOMWARE GROUP), JOHN DOES 5-6 (AKA LOCKBIT RANSOMWARE GROUP), JOHN DOES 7-8 (AKA DEV-0193), JOHN DOES 9-10 (AKA DEV-0206), JOHN DOES 11-12 (AKA DEV-0237), JOHN DOES 13-14 (AKA DEV-0243), JOHN DOES 15-16 (AKA DEV-0504), Controlling Computer Networks and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

Case No.

FILED UNDER SEAL

**DECLARATION OF ROBERT G. ERDMAN II IN SUPPORT OF APPLICATION FOR AN
EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW
CAUSE RE PRELIMINARY INJUNCTION**

I, **Robert G. Erdman II**, declare as follows:

1. I am an Associate Vice President, Research & Development at Fortra. I make this declaration in support of Fortra LLC's Application for An Emergency *Ex Parte* Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my current role at Fortra, I lead the Fortra Threat Intelligence teams investigating and creating counter measures for Business Email Compromise (BEC), Phishing, malware/ransomware delivery, malicious domains, botnets and cracked versions of Cobalt Strike.¹ Prior to that, I served as the

¹ As used in this declaration and in others, "cracked versions of Cobalt Strike" refer to stolen, unlicensed, or otherwise unauthorized versions or copies of Cobalt Strike.

Director of Development, Infrastructure Protection at Fortra where I lead the vulnerability management, antivirus and penetration testing product development teams and as Head of Product Management for Fortra's Cyber Threat Solutions (CTS) Business Unit. I joined Fortra after having spent more than 25 years in the information technology industry. Prior to joining Fortra, I was with Spok Inc. where I most recently served as Sr. Technical Product Manager, Contact Centers & Platforms. While there, I worked with a variety of worldwide customers including Government, Healthcare, Financial & Military implementing mission critical Windows, Unix & Linux communications solutions. I am a current member of the U.S. Federal Bureau of Investigation's InfraGard. A true and correct copy of the current version of my curricula vitae is attached to this declaration as **Exhibit 1**.

3. In connection with my current role at Fortra, I have investigated the structure and function of a malicious software ("malware") command and control ("C2") architecture abusing a legitimate commercial adversary simulation software used for penetration testing called "Cobalt Strike," the activities carried throughout this infrastructure, and an assessment of the impact on Fortra's business and on users of the Internet. The abuse of Cobalt Strike by nefarious threat actors has caused, and continues to cause, extreme damage to Fortra, its reputation, and its customers, as well as other parties which, if allowed to continue, will be compounded as the case proceeds.

PLAINTIFF FORTRA

4. Fortra is a technology company that manufactures, distributes and sells a variety of software products and services to businesses, professional organizations and educational institutions around the world. Fortra's products address a wide range of cybersecurity and automation needs across a multitude of platforms. In cybersecurity, our solutions typically fall into four categories: Infrastructure Protection, Data Protection, Security Awareness Training & Managed Services.

5. The company Fortra, is a well-known cybersecurity software development company that is trusted by government, industry and the security community at large.

COBALT STRIKE

Legitimate Versions of Cobalt Strike

6. Cobalt Strike is a commercial security testing tool made by the company Fortra. Cobalt Strike was created in 2012 to enable threat-representative security tests. Cobalt Strike is a threat emulation tool that provides a post-exploitation agent and covert communication channels ideal for Adversary Simulation and Red Team exercises, replicating the tactics and techniques of an advanced adversary in a network. Cobalt Strike is used to challenge security teams and measure incident response with malleable command and control known as “C2,” which allows network indicators to imitate different malware and social engineering processes to strengthen security operations for measuring security programs and incident response capabilities. Cobalt Strike has multiple manual and technical licensing restrictions that threat actors must break through to facilitate the alteration and malicious usage of the Cobalt Strike commercial product. Potential purchasers are investigated to determine if they are employed by a legitimate company or agency and are not subject to export restrictions. The Cobalt Strike software contains technical protections that require a valid, time limited license and a valid authorization ID or “watermark”. All downloads and updates of the Cobalt Strike product code are validated against the licensing and watermark requirements before access can proceed. Approved purchasers of Cobalt Strike sign a EULA agreement that forbids using the product on computer systems where they have not received the owner’s approval and malicious or illegal usage of the Cobalt Strike product. Fortra continuously monitors common hacker forums, file sharing sites and the internet at large with both manual and programmatic means to discover new instances of cracked Cobalt Strike.

7. Cobalt Strike itself is a Threat Emulation application used for Adversary Simulations with two primary components: the team server and the client. A team server accepts client connections. The client is how operators connect to a team server. These two components are contained in Java executable files (a JAR file). “Beacon” is the name for Cobalt Strike’s default payload used to create a connection from a computer system to the team server. The beacon file contains contact information such as the C2 IP

address or domain, connection port information, watermark,² and encryption keys. Legitimate penetration testers and red teamers use this application to test whether an organization’s system would potentially succumb to the infiltration of malware into the network.

Cracked Versions of Cobalt Strike

8. Authorized and properly purchased versions of Cobalt Strike will contain a valid authorization ID watermark that can be resolved to a legitimate end user license. Cracked, compromised versions of Cobalt Strike often consist of manipulated beacon files that are programmed to communicate with malicious C2 infrastructure to engage in illegal activities once a malware infiltrates a victim’s computer systems. Defendants have been able to utilize cracked versions to gain control of their victim’s machine and move laterally through the connected network to find other victims and install malware. Once they have gained control, Defendants are able to inflict further harm by exfiltrating the victim’s data and installing ransomware.

9. Cracked versions of Cobalt Strike are distributed in various forums and websites. Typically, these are the result of someone modifying a Cobalt Strike JAR file adding in technical computer code to bypass the license restrictions and rebuilding the Cobalt Strike JAR, or by crafting an authorization file with a fake authorization ID and distributing that with the JAR. Fortra has identified cracked copies of Cobalt Strike based on legitimate version 4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, and 4.7.

INVESTIGATION OF THE CRACKED COBALT STRIKE INFRASTRUCTURE

10. The C2 infrastructure at issue in this case—the “cracked Cobalt Strike” infrastructure—is a prolific and globally dispersed malware distribution infrastructure. As part of my investigation, I have been able to identify details regarding Defendants’ deployment of cracked Cobalt Strike, including the operational details about the malicious and cracked Cobalt Strike infrastructure, the methods of

² Watermarks are unique values associated with a certain Cobalt Strike license. Legitimate, licensed versions of Cobalt Strike have a watermark embedded into the beacon file that are associated with the Cobalt Strike license. Cobalt Strike watermarks can be identified in post-incident analysis and are considered valued intelligence in the security community.

communications among infected computers, how the infrastructure transmits threats to innocent computers, and the cracked Cobalt Strike infrastructure's mechanisms to evade detection and attempts to disrupt its operation.

11. The cracked Cobalt Strike infrastructure has targeted multiple computer systems and entities around the world. The cracked Cobalt Strike infrastructure is a complex and constantly evolving threat, which makes detection and disruption difficult, and further exacerbates the harm caused by Defendants. Defendants further this complex scheme by delivering ransomware, providing backdoor access to infected machines, and acting as a gateway malware dropper to deploy additional malicious software tools. For example, once installed, Defendants can utilize cracked versions of Cobalt Strike to further deliver ransomware to the victim's machine facilitating data exfiltration and eventually the complete compromise and destruction of the computer system.

12. Cracked Cobalt Strike can be delivered to a victim by many different methods. A phishing message containing a malicious payload is sent to targeted victims and when the payload is activated, the victim's computer executes a Cobalt Strike beacon that has been configured to communicate with Defendants' cracked Cobalt Strike C2 infrastructure. Cracked Cobalt Strike can also be delivered to a victim by hacking into an entity's network via any exploitable vulnerability and then placing a Cobalt Strike beacon on the exploited computer system under the Defendants control or by placing cracked Cobalt Strike on a malicious website and when a victim visits a specially crafted URL link the cracked Cobalt Strike beacon is delivered to the victim.

13. Once under command of the operators of cracked Cobalt Strike, the operators are able to leverage cracked versions of the Cobalt Strike application to infiltrate the security systems by providing a backdoor and serve as a gateway malware dropper to deploy additional ransomware such as Conti, Quantum Locker, Royal, Cuba, BlackBasta BlackCat, PlayCrypt, and LockBit to the victims' machine.

14. Fortra monitors many locations for cracked Cobalt Strike versions including social media, file sharing websites, illicit marketplaces, and internet search engines. Through these and related investigative steps, I have developed detailed information about the size, scope, and illegal activities of the

use of cracked Cobalt Strike to facilitate malware and ransomware attacks.

15. Fortra's investigation unfolded in several steps:
 - a. Identify the probable locations of a cracked version of Cobalt Strike;
 - b. Investigate the locations and confirm if a Cobalt Strike version is present;
 - c. If a Cobalt Strike version is present, determine if it is a *cracked* Cobalt Strike version based upon file hashes, watermarks, and licensing information;
 - d. Identify geolocation and hosting services provider of the machine containing the cracked Cobalt Strike version; and
 - e. Determine additional tactics, techniques and procedures utilized after Cobalt Strike is deployed on a victim's machine to identify additional malware or ransomware deployed by Defendants.

16. Based on our investigation and analysis, Fortra has determined that cracked Cobalt Strike functions as a robust delivery mechanism for threat actors to deploy ransomware and other malware for the purposes of stealing account credentials, taking control of victims' computers, and extorting victims into paying ransom payments. Additionally, I concluded that cracked Cobalt Strike operates as a ransom-as-a-service or malware-as-a-service, operating solely to perpetrate nefarious actions. I also conclude from these same facts, upon information and belief, that the Defendants must have known and intended that the Defendants' operation of cracked Cobalt Strike was to defraud end-user victims, by means of fraudulent pretenses and representations transmitted over the Internet, as further described below. As a result, Fortra has been directly injured in its business and property by these Defendants' acts and their coordinated pattern of acts.

ORGANIZATION OF THE DEFENDANTS' C2 INFRASTRUCTURE

17. As stated above, the infrastructure at issue is comprised of a network of computing devices, connected to the Internet, that are infected with a particular cracked version of Cobalt Strike. The cracked version of Cobalt Strike gives the Defendants in this matter remote control via the Internet over the operation of the compromised computing devices. Because Defendants can use the intrusion of individual

victim's computers to further compromising other computer devices, the cracked version of Cobalt Strike allows a single criminal or criminal organization to control the vast array of compromised computing devices.

18. The cracked Cobalt Strike C2 infrastructure is comprised of a large number of victim computers that have been compromised by the Defendants using cracked Cobalt Strike to deploy malware and ransomware payloads. The C2 infrastructure is utilized by the Defendants to transfer instructions to the compromised victim computers, for the purpose of exerting further control over the victim computers, allowing them to use their control of the computer's operation to carry out the numerous types of harmful activities described more fully later in this declaration. Further detail regarding the infected victim computers and the C2 computers is set forth below.

Infected Victim Computers

19. The total number of infected computers caused by cracked Cobalt Strike, over time, has been growing. Based on our investigation, we have observed that multiple entities have been impacted by the leveraging of cracked Cobalt Strike.

20. The compromised victim computers are responsible for performing the daily work of the Defendants' Cobalt Strike C2 infrastructure; through Defendants' control, they are able to further carry out their criminal enterprise. For example, Defendants are able to use their cracked Cobalt Strike infrastructure to install ransomware such as Conti, Quantum Locker, Royal, Cuba, BlackBasta BlackCat, PlayCrypt, and LockBit. These ransomware families are prolific amongst threat actors and their efficacy in causing harm is well known in the security community. The Conti ransomware once deployed on a victim's system, for example, will try to terminate a number of services to ensure that it can encrypt files, disable real time monitoring, and subsequently demand a ransom or to engage in other malicious activity directed at the victims. LockBit ransomware is malicious software designed to block user access to computer systems in exchange for a ransom payment. Later iterations of LockBit (LockBit 2.0 and 3.0) have increased sophistication: the "fastest encryption software" in the world, the ability to perform DDoS attacks on the victims' infrastructure, the ability to steal sensitive data, and the ability to use leak sites to expose

companies' proprietary data.

C2 Computers

21. The C2 computers are specialized computers and/or software (“servers”). Defendants purchased or leased these servers and use them to send commands to control the compromised victim computers. The C2 computers send the most fundamental instructions, modules, updates, and commands, and overall control of the cracked Cobalt Strike is carried out from these computers. C2 computers include the servers at various IP addresses (i.e., “Internet Protocol” address) and domains. *See Appendix A* to the Complaint.

22. Each instance of cracked Cobalt Strike is pre-programmed to connect and communicate with configured number of these C2 servers. When such a connection is made, the servers can download instructions or deploy additional malware or ransomware to the infected computing device and upload stolen information from it. This is how the Defendants are able to continue to expand the network of compromised computers to ensure that the harm caused is widespread.

23. To create the C2 infrastructure, Defendants set up accounts with web-hosting providers—i.e., companies, usually legitimate, that provide facilities where computers can be connected through high-capacity connections to the Internet and locate their servers in those facilities. By contacting a C2 server, cracked versions of Cobalt Strike can receive updated commands and modules from and communicate with the Defendants.

Overview of C2 Communications Channels

24. The Defendants are able to send and receive communications between their C2 servers and the infected victims' computers.

25. The primary C2 channel between infected victim computers and Defendants' C2 computers is comprised of particular IP addresses or internet domains associated with servers directly controlled by Defendants. The concurrently filed declaration of Christopher Coy describes how Defendants are able to use IP addresses and internet domains to communicate and their reliance on hosting services, registrars, and registries to facilitate these systems of communication. *See Coy Decl.* ¶ 35.

26. Through the use of cracked Cobalt Strike, once the victim's computer is infiltrated, the victim computer receives instructions from the C2 servers associated with the primary IP addresses directly controlled by Defendants.

Defendants' C2 Communications Tier is Designed to Evade Technical Counter-Measures

27. The most vulnerable points in the Defendants' C2 architecture are the C2 IP addresses and domains, as they can be identified and, if disconnected from the Internet, the Defendants' communications with compromised end-user computers will be severed and propagation of the cracked versions of Cobalt Strike are disabled. This is why the relief Fortra seeks is aimed at severing these lines of communication to facilitate the disruption of the C2 infrastructure. To counteract the vulnerable points in the C2 architecture, Defendants continue to employ features of the C2 infrastructure enable the cracked versions of Cobalt Strike to better withstand technical counter-measures. For example, Defendants do not use the same set of IP addresses and domains indefinitely; rather the Defendants will register new domains and IP addresses, so that once added to the compromised end-user computers, all subsequent communications can take place over the newly registered communication channels. This dynamic use of IP addresses and domains make attempts to disable the malware more difficult.

CRACKED COBALT STRIKE HAS AFFECTED VICTIMS IN NEW YORK

28. Through its investigation, Fortra has determined that cracked Cobalt Strike has been used in connection with affirmative targeting of victims in New York, including the Eastern District of New York.

29. Using technology that allows for the geographic location of IP addresses, I have investigated IP addresses known to be associated with cracked Cobalt Strike. Technology exists to determine the geographic location of IP addresses, alone or in association with domains. As can be seen below, in **Figure 1**, the I have identified over 50 unique IP addresses attributable to Defendants and cracked Cobalt Strike activity that are located within New York.

IP Address	Country	State	Hosting Provider
23.94.240.207	United States	New York	Racknerd LLC
23.94.255.18	United States	New York	Racknerd LLC
23.95.44.80	United States	New York	Virtual Machine Solutions LLC
23.95.48.45	United States	New York	Racknerd LLC
23.95.67.59	United States	New York	Racknerd LLC
24.199.98.19	United States	New York	DigitalOcean LLC
24.199.98.235	United States	New York	DigitalOcean LLC
24.199.113.87	United States	New York	DigitalOcean LLC
38.54.31.137	United States	New York	Lightnode-vn
38.60.31.200	United States	New York	Psinet Inc.
38.60.39.41	United States	New York	Psinet Inc.
38.60.49.64	United States	New York	Psinet Inc.
64.227.190.71	United States	New York	DigitalOcean LLC
67.205.139.137	United States	New York	DigitalOcean LLC
67.205.142.226	United States	New York	DigitalOcean LLC
67.207.90.203	United States	New York	DigitalOcean LLC
68.183.21.224	United States	New York	DigitalOcean LLC
104.131.5.230	United States	New York	DigitalOcean LLC
104.168.68.35	United States	New York	Racknerd LLC
107.172.29.162	United States	New York	Racknerd LLC
107.172.61.62	United States	New York	Racknerd LLC
107.172.78.195	United States	New York	Racknerd LLC
107.172.201.137	United States	New York	Colocrossing
107.172.208.88	United States	New York	Racknerd LLC
107.173.70.169	United States	New York	Colocrossing
107.173.122.167	United States	New York	Colocrossing
107.173.251.222	United States	New York	Racknerd LLC
107.174.66.104	United States	New York	Colocrossing
107.174.95.204	United States	New York	Colocrossing
107.174.186.22	United States	New York	Racknerd LLC
107.175.91.126	United States	New York	Racknerd LLC
107.175.111.199	United States	New York	Highlight Marketing LLC
154.38.114.212	United States	New York	Psinet Inc.
154.64.224.130	United States	New York	Psinet Inc.
157.230.188.71	United States	New York	DigitalOcean LLC
159.223.141.48	United States	New York	DigitalOcean LLC
159.223.190.172	United States	New York	DigitalOcean LLC
161.35.3.56	United States	New York	DigitalOcean LLC
165.227.85.160	United States	New York	DigitalOcean LLC
172.245.27.233	United States	New York	VPS ACE

IP Address	Country	State	Hosting Provider
192.3.204.163	United States	New York	Hudson Valley Host
192.3.223.126	United States	New York	Colocrossing
192.3.231.208	United States	New York	Colocrossing
192.210.162.147	United States	New York	Colocrossing
192.210.170.174	United States	New York	Racknerd LLC
192.227.155.185	United States	New York	Colocrossing
198.23.223.145	United States	New York	Colocrossing
198.98.50.31	United States	New York	Frantech Solutions
199.195.248.79	United States	New York	Frantech Solutions
199.195.249.113	United States	New York	Frantech Solutions
199.195.251.23	United States	New York	Frantech Solutions
199.195.251.219	United States	New York	Frantech Solutions
199.195.254.96	United States	New York	Frantech Solutions
204.10.120.109	United States	New York	Vinters Corp
206.189.228.101	United States	New York	DigitalOcean LLC
209.127.116.26	United States	New York	B2 Net Solutions Inc.

FIGURE 1 – Cracked Cobalt Strike Associated IP Addresses in New York

DEFENDANTS CAUSES SEVERE HARM

Threat Actors Use Cracked Cobalt Strike Versions to Cause Severe Harm by Engaging in Malicious Activities Against Victims Such as Deploying Ransomware And Other Types Of Dangerous Malware

30. Defendants have been able to inflict severe harm on individuals whose computing devices they compromise. Once Defendants gain access to a computing device through a cracked version of Cobalt Strike, Defendants can use the victim’s computer to send commands and instructions to the infected computing device to control it surreptitiously and deliver malware or ransomware that, among other things, enables Defendants to take control of the victim’s computer and extort money from them. Defendants rely on the legitimate functionality of Cobalt Strike to avoid detection and further cause harm.

31. Cracked Cobalt Strike is known to deliver other forms of malicious code, including ransomware. Ransomware is a type of malware that prevents victim user from accessing their systems or personal files and demands ransom payment in order to regain access. The introduction of ransomware can be extremely damaging. For example, in one instance, ransomware disrupted the IT network of a German

hospital which caused the death of a woman in need of emergency treatment. *See* Declaration of Christopher Coy ¶ 44 and Declaration of Errol Weiss ¶ 14, both concurrently filed.

32. Cracked Cobalt Strike is used in a variety of illegal activities, but it is well-known as a downloader/dropper for delivering major malware families in what is known as a “malware-as-a-service” criminal business model that delivers ransomware that locks a victim’s computer and demands payment to unlock it, banking Trojans that steal funds from victim accounts, and a wide range of other types of malware. The malware distributed by Defendants include Conti, which is a type of ransomware. Conti cyber threat actors remain active and reported Conti ransomware attacks against U.S. and international organizations have risen to more than 1,000. While Conti is considered a ransomware-as-a-service (RaaS) model ransomware variant, there is variation in its structure that differentiates it from a typical affiliate model. It is likely that Conti developers pay the deployers of the ransomware a wage rather than a percentage of the proceeds used by affiliate cyber actors and receives a share of the proceeds from a successful attack.

33. In order to avoid detection, Defendants rely on and abuse the legitimate functionalities and capabilities of Cobalt Strike (for penetration testing software to be effective, it has to be able to perform the test without detection).

34. The cracked Cobalt Strike can be used to deploy additional instances of malware. Each of these secondary malware infections makes further changes to the user’s computing device, including by adding files, changing registry settings, opening additional backdoors that allow control by other cybercriminals, and allowing yet further sets of malware to be downloaded onto the computing device. All of these malware variants are designed to attack computing device, may themselves be connected to other criminal infrastructure and receive additional commands.

35. Under these circumstances, the Defendants have a vested interest in increasing the number of computers belonging to their C2 network, as that relates directly to the number of computers they can attempt to infect with secondary malware.

Cracked Cobalt Strike Causes Severe Harm Both To Fortra’s Reputation, Brands And

Goodwill With Its Customers And The Public

36. Defendants inflict substantial damage on Fortra whose products and trademarks Defendants systematically abuse as part of the fraudulent operations involving cracked versions of Cobalt Strike.

37. The cracked versions of Cobalt Strike do not appear any different than the legitimate versions of Cobalt Strike used for legitimate penetration testing and red team operations. The user, thus, thinks the Cobalt Strike is developed, distributed, and commercially sold by Fortra, despite the fact that it is the criminal actors that are compromising the operating system. This harms Fortra's reputation and goodwill among the public. In particular, Defendants' cracked use of Fortra's legitimate penetration testing tool for unlawful cybercrime risks eroding trust within Fortra's customer base in the security industry, and risks eroding trust by the general public in security testing tools such as Cobalt Strike. This risks serious damage to Fortra's brand, trademarks and goodwill, given that both customers and internet users generally may come to wrongfully associate Fortra and Cobalt Strike with Defendants' unlawful activities.

38. More broadly, malicious use of cracked Cobalt Strike harms Fortra and Fortra's brand, trademarks and goodwill by damaging the customers' computing devices and the software installed on victim computing devices. Because Cobalt Strike is legitimate software, Defendants' misuse of cracked versions causes irreparable harm, where customers and potential customers mistakenly believe that it is Fortra's legitimate product offering that is responsible for these ransomware and malware attacks. In recent years, as the use of cracked Cobalt Strike to carryout malware and ransomware has increased; concurrently the negative opinion about Cobalt Strike and Fortra has also increase. Attached to this declaration as **Exhibit 2** is an article describing that "Cobalt Strike is one of the most popular tools used by cybercriminals" and questioning "whether Cobalt Strike is doing more harm than good by being commercially available."³ This negative opinion caused by Defendants malicious use of cracked Cobalt Strike is detrimental. Attached to this declaration as **Exhibit 3** is an article where Conti, which is described

³ Available at <https://venturebeat.com/business/more-can-be-done-to-curb-misuse-of-cobalt-strike-expert-says/>.

as “by far the most successful ransomware group in operation today” attempted to surreptitiously purchase a legitimate Cobalt Strike license under false pretense in addition to their prolific abuse of cracked Cobalt Strike.⁴ Attached to this declaration as **Exhibit 4** is an article that describes the “appeal” of Cobalt Strike for use by threat actors and notes a several-hundred percent increase in usage by threat actors over recent years.⁵ Attached to this declaration as **Exhibit 5** is an article that further describes “why attackers like Cobalt Strike” and cite to the session-based nature of Cobalt Strike where “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.”⁶ Attached to this declaration as **Exhibit 6** is an article that states that “Cobalt Strike is one of the top five tools used by attackers.”⁷ Attached to this declaration as **Exhibit 7** is an article describing Cobalt Strike as “the new favorite among thieves” because it is flexible and can be repurposed to fit the needs of the threat actor.⁸ Attached to this declaration as **Exhibit 8** is an article that describes Cobalt Strike as a “double-edged sword” because of its use both by members of the security community to protect against attacks and by cybercriminals to carryout the attack.⁹ Although some of the articles distinguish between cracked and legitimate versions of Cobalt Strike, others do not. Accordingly, Cobalt Strike being referred to repeatedly as a favorite tool amongst cybercriminals does not engender trust of Cobalt Strike and the Cobalt Strike brand because individuals may not be able to distinguish between nefarious use of cracked Cobalt Strike by criminals and legitimate uses. Attached to this declaration as **Exhibit 9** is an article describing the use

⁴ Available at <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/>.

⁵ Available at <https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware>.

⁶ Available at <https://www.bankinfosecurity.com/attackers-increasingly-using-cobalt-strike-a-16959>.

⁷ Available at <https://www.darkreading.com/attacks-breaches/cobalt-strike-becomes-a-preferred-hacking-tool-by-cybercrime-apt-groups/d/d-id/1341073>.

⁸ Available at <https://securityboulevard.com/2020/09/cobalt-strike-the-new-favorite-among-thieves/>.

⁹ Available at <https://cybernews.com/editorial/cobalt-strike-pentesting-tools-cybercriminals/>.

of cracked Cobalt Strike in connection with hacks of health-related organizations and noting that according to a warning issued by the Department of Health and Human Sciences, the number of organizations effected each year is in the tens of thousands.¹⁰ As described in the concurrently filed declaration of Errol Weiss, representing the membership interest of Health-ISAC, malicious use of cracked Cobalt Strike has had devastating impacts on the health community. Weiss Decl. ¶¶ 14-15. In turn, effected individuals who had their data hacked may place blame on Fortra and legitimate Cobalt Strike, thus further harming its reputation. Attached to this declaration as **Exhibit 10** is an article describing how hacking attempts against Ukrainian organizations perpetrated by threat groups associated with Russia have utilized cracked Cobalt Strike.¹¹ This could cause the incorrect perception that Fortra is responsible for the attacks against Ukrainian organization. Attached to this declaration as **Exhibit 11** is an article describing the recent identification by Google of 34 new cracked versions of Cobalt Strike, signaling that the increase in usage continues to increase.¹²

39. Victims of Defendants are usually unaware of the fact that their computing devices are infected and have become part of the C2 infrastructure. Even if aware of the infection, they often lack technical resources or skills to resolve the problem, allowing their computing devices to be misused indefinitely, as manual steps to remove the malicious software may be difficult for ordinary users. Thus, due to Defendants' abuse of Cobalt Strike, the community of victims who may ultimately learn that cracked Cobalt Strike was associated with compromise of their computers risk incorrectly believing that Fortra and Cobalt Strike is the source of this activity, when in fact the source is in fact Defendants' unlawful conduct. This poses a significant risk of reputational harm to Fortra. Further, even the security community that relies on legitimate uses of Cobalt Strike to improve security of institutions and individuals, risk developing a

¹⁰ Available at <https://www.bankinfosecurity.com/feds-warn-healthcare-over-cobalt-strike-infections-a-20242>.

¹¹ Available at <https://www.zdnet.com/article/ukrainian-organizations-warned-of-hacking-attempts-using-credomap-malware-cobalt-strike-beacons/#ftag=RSSbaffb68>.

¹² Available at <https://thehackernews.com/2022/11/google-identifies-34-cracked-versions.html>.

perception that this very useful tool is associated with cybercrime. This too poses significant risk of reputational harm to Fortra.

40. Fortra devotes significant computing and human resources to combating cracked Cobalt Strike and other malware infections and helping customers and victims in general determine whether or not their computing devices are infected and, if so, cleaning them. Not only does Fortra expend resources in helping users combat cracked Cobalt Strike, these efforts require in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Fortra's customers. Fortra has expended significant resources to investigate and track the Defendants' illegal activities and to counter and remediate the damage caused by the Defendants' criminal activity to Fortra, its customers, and the general public. Fortra actively combats the cracked versions of Cobalt Strike and has expended over a million dollar of dollars on this effort. Fortra has altered the Cobalt Strike technical licensing controls to eliminate methods of compromise that have been discovered in our research, Fortra has issued more than 900 DMCA violation notices to a variety of social media, file sharing and hacking forum providers.

41. Defendants' misuse of Cobalt Strike irreparably harms Fortra by damaging its reputation, brands, and customer goodwill. Defendants physically alter and corrupt Fortra's products and use those products in a cracked manner to carry out cybercrime, as detailed above. Cracked Cobalt Strike still bears the Fortra and Cobalt Strike trademarks. In some cases, this is meant to and does mislead Fortra's customers, as it may cause such customers to believe that activity is associated with legitimate penetration testing. But, more broadly, for the reasons discussed, simply by being associated with malicious activity, Defendants' misuse of cracked "Cobalt Strike" branded software causes extreme damage to Fortra's brands, trademarks, goodwill and trust within the security community and the public in general. The trademark registration for Fortra's trademark "Cobalt Strike," infringed by Defendants is attached to the Complaint as **Appendix E**.

42. In addition, Defendants reproduce Fortra's copyrighted code for Cobalt Strike. In particular, as an illustrative example, Defendants literally copy the entirety of Fortra's copyrighted Cobalt Strike "team server" code in a cracked version used for malicious purposes. Each cracked Cobalt Strike team server associated with the IP addresses and domains subject to this request for relief to the court,

contains a cracked reproduction of Fortra's copyrighted Cobalt Strike team server code. Defendants also engage in the cracked distribution of Fortra's copyrighted Cobalt Strike code as part of their enterprise, to compromise victim computers in the first instance, to intrude upon victims' computing resources and networks, and to deliver further forms of malware, as discussed. The Defendants' infringement involves cracked copying of executable code for all of the Cobalt Strike team server's web server, beacon and configuration features and functionality, including all of Fortra's creative and original method implementations, interfaces, parameters, variables, arrays, data types, operators, and objects. Copyright registrations for Fortra's Cobalt Strike code are attached to the Complaint as **Appendix D**.

43. Fortra has expended many of millions of dollars in security personnel, infrastructure and monitoring tools to maintain the integrity of the Fortra source code repositories and protect the Fortra proprietary Cobalt Strike source code from theft. Additionally, Fortra expends significant resources on security researchers to monitor for Cobalt Strike being listed on code sharing websites where Defendants have illegally decompiled and shared portions of copyrighted Cobalt Strike source code.

44. Fortra has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Fortra's products and services and the expenditures of significant resources by Fortra to market those products and services, Fortra has generated substantial goodwill with its customers, has established strong brands, has developed the Fortra name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade.

45. The activities of the Defendants injure Fortra and its reputation, brand, and goodwill because customers in the security community and users in general, subject to the negative effects of these malicious applications, may incorrectly believe that Fortra and Cobalt Strike are the sources of their computing device problems or risks to such devices, when in fact those risks flow from Defendants' activities. There is a great risk that users may attribute this problem to Fortra and associate these problems with Fortra's products, including legitimate versions of Cobalt Strike, thereby diluting, and tarnishing the value of the Fortra and Cobalt Strike trademarks and brands.

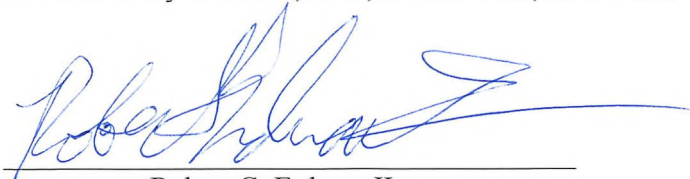
46. Based on my experience assessing cyber threats and the impact on business, I conclude that customers and the general public may, and often do, incorrectly attribute to Fortra the negative impact of attacks carried out by leveraging cracked Cobalt Strike as a result of having their computers hijacked and infected with a variety of malware, described earlier in this declaration. Further, based on my experience, I conclude that there is a serious risk that customers may stop supporting and using Fortra's products and services, including particularly Cobalt Strike, because Defendants' activities impair consumers' perception of Fortra and the Cobalt Strike brand and trademark in the market.

DISRUPTING CRACKED VERSIONS OF COBALT STRIKE

47. I believe that if provided advance notice that the C2 IP addresses and domains were to be disabled, the Defendants would take measures to keep cracked Cobalt Strike alive by migrating to new IP addresses and domains. As discussed, Defendants intentionally evade detection by changing the IP addresses and domains of its C2 servers over time. Therefore, a piecemeal approach to disconnecting the IP addresses and domains will fail. If less than all of the C2 servers are directed to be taken offline immediately and simultaneously, the infected end-user computers will be able to migrate to the remaining servers or to new C2 servers.

48. I believe that the only way to suspend the injury caused to Fortra, its consumers and the public, is to take the steps described in the [Proposed] *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Proposed TRO"). This relief will significantly hinder the Defendants' cracked Cobalt Strike monetization and capability and operational control, and stop the harmful activities of the Defendants.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 29th day of March, 2023, in New York, New York.



Robert G. Erdman II

EXHIBIT 1

Bio

Bob Erdman is Associate Vice President, Research & Development for Fortra's Cyber Threat Solutions (CTS) Business Unit. Bob joined Fortra after having spent more than 25 years in the information technology industry. Prior to joining Fortra, Bob was with Spok where he most recently served as Sr. Technical Product Manager, Contact Centers & Platforms. While there, Bob worked with a variety of worldwide customers including Government, Healthcare, Financial & Military implementing mission critical Windows, Unix & Linux communications solutions. Bob is a veteran of the United States Army National Guard and a current member of the US Federal Bureau of Investigation's InfraGard & Cyber Health Working Group.

Education

Jamestown College 1985-1990

B.A. Computer Science, B.A. Business Administration, B.A. Management Information Systems

Veteran, Honorable Discharge, DoD IT-II, Public Trust, Secret Eligible 1990-1996

FBI InfraGuard, Cyber-Health Working Group 2018-Present

AIX Community Advocate Level3 2020-Present

Redhat Linux Certified Engineer

Oracle Database Champion

Work Experience

Fortra, LLC 2023-Present

Associate Vice President, Research & Development

- Lead the strategic direction of the company's Threat Intelligence, Data Science and Infrastructure Protection teams
- Managed relationships with external intelligence partners, both public and private

HelpSystems, LLC

2022-2023

Director of Development

- Established an all company Threat Fusion Center combining threat intelligence and indicators of compromise from all company products and brands into a central managed location to service the needs of internal and external customers
- Performed due diligence investigations of potential M&A acquisitions to evaluate technology, personnel and integration capabilities
- Managed threat intelligence, data science and software development teams

HelpSystems, LLC

2019-2020

Associate Director of Development, Cyber Threat

- Leader of the Infrastructure Protection research and development teams consisting of both offensive and defensive security tools
- Provided strategic product direction to ensure customer and company objectives were fulfilled in a timely and cost efficient manner
- Performed intelligence gathering activities on threat actors and threat actor groups related to illicit usage of company created software products and BEC email compromises
- Managed the company DMCA activities in support of legal and law enforcement takedowns of improperly hosted company intellectual property

HelpSystems, LLC

2019-2020

Sr. Manager, Product Management, Cyber Threat

- Ensured that company revenue, ARR and licensing goals were met by leading the strategy and execution of the company's Offensive and Defensive cybersecurity product offerings
- Created product roadmap plans for multiple product lines incorporating business requirements, sales targets and stakeholder feedback
- Managed and mentored junior product team members to meet product delivery metrics and career advancement goals
- Collaborated with globally located Development Managers to transition product design and development activities to Agile processes and methodologies to provide products to HelpSystem's customer base on schedule with delivery projections
- Communicated with all areas of the organization as warranted to deliver on the product goals of the Cyber Threat division
- Facilitated interactions with third parties to assess partnership and licensing opportunities including hardware, software and services required for HelpSystem, LLC's product goals
- Cooperated with internal Security Stakeholders to implement improved processes and technologies to better protect the organization and the organization's intellectual property

- Interacted with HelpSystem's customers and prospects by providing webinars, roadmaps, product training and feedback presentations across global audiences

HelpSystems, LLC

2017-2019

Cross Platform Security Product Manager

- Ensured that company revenue, ARR and licensing goals were met by leading the strategy and execution of designated company product offerings on IBM i, Linux and Unix
- Created product roadmap plans for multiple products incorporating business requirements, sales targets and stakeholder feedback
- Collaborated with globally located Development teams to provide products to HelpSystem's customer base on schedule with delivery projections
- Communicated with all areas of the organization as warranted to deliver on the product goals of the designated products under management
- Facilitated interactions with third parties to assess partnership and licensing opportunities including hardware, software and services required for HelpSystem, LLC's product goals
- Performed due diligence activities on potential company acquisitions
- Interacted with HelpSystem's customers and prospects by providing webinars, roadmaps, product training and feedback presentations across global audiences

Spok Inc.

2012-2017

Product Manager, Technical Platforms & Security

- Lead the strategy and execution of the company's government and security certifications.
- Performed Security Assessments using various tools and techniques including DoD STIGs, Retina, Nessus, SCAP and other manual methods
- Oversaw strategy and development of products to ensure compliance with hardware and security requirements.
- Worked with third parties to assess partnerships and licensing opportunities including hardware, accessories and other solutions required for Spok products.
- Set pricing and margins for hardware products required by Spok software solutions to meet revenue and profitability goals.
- Lead strategy and operational development of hosted capabilities including vendor selection, team leadership and development of operational processes.
- Lead selection of 3rd party hardware, software and accessories required for Spok products. Ensured consistency and quality across all products.

Organizations and Services

Greater Grand Rapids Area Cable Commission, Itasca County Parks and Recreation Commission

Rotary International, Grand Rapids Centennial Club

Youth sports coach for Hockey, Basketball, Little League and Football associations

EXHIBIT 2

More can be done to curb misuse of Cobalt Strike, expert says

Kyle Alspach

@KyleAlspach

March 22, 2022 6:00 AM

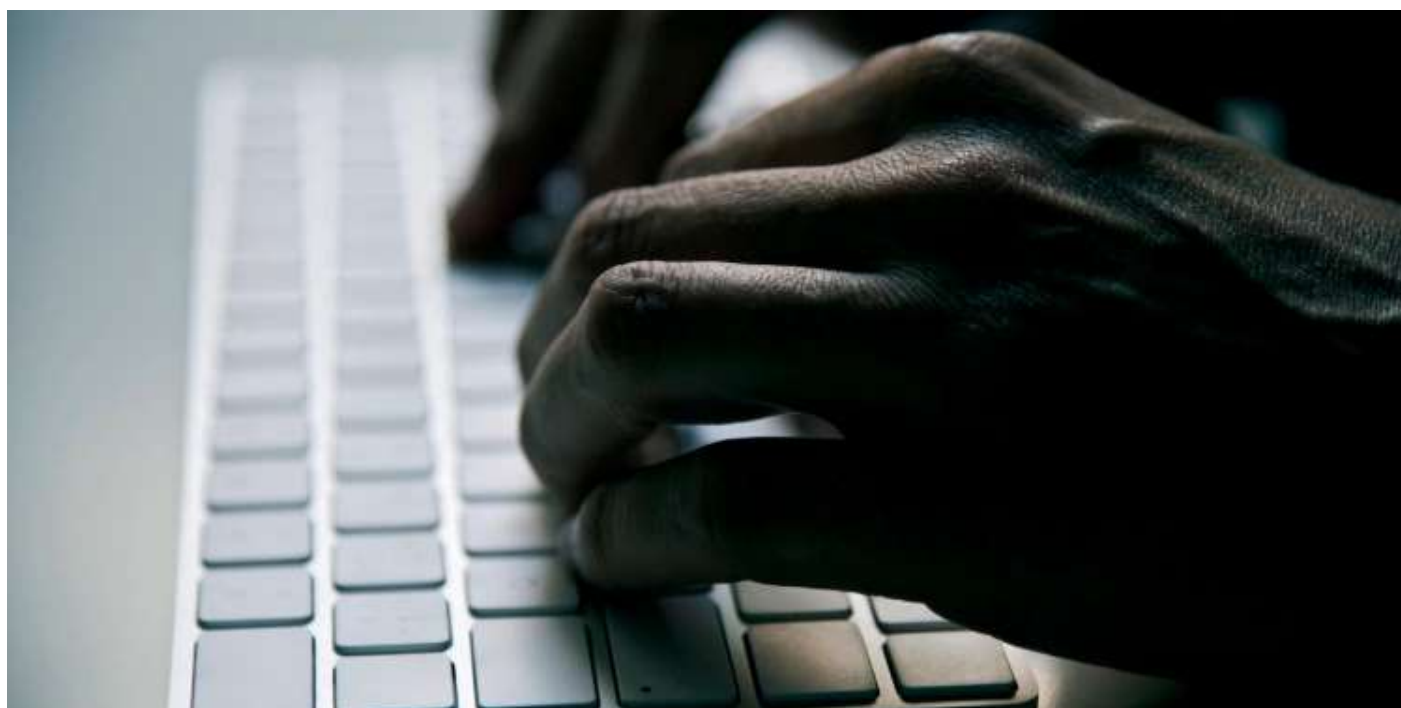
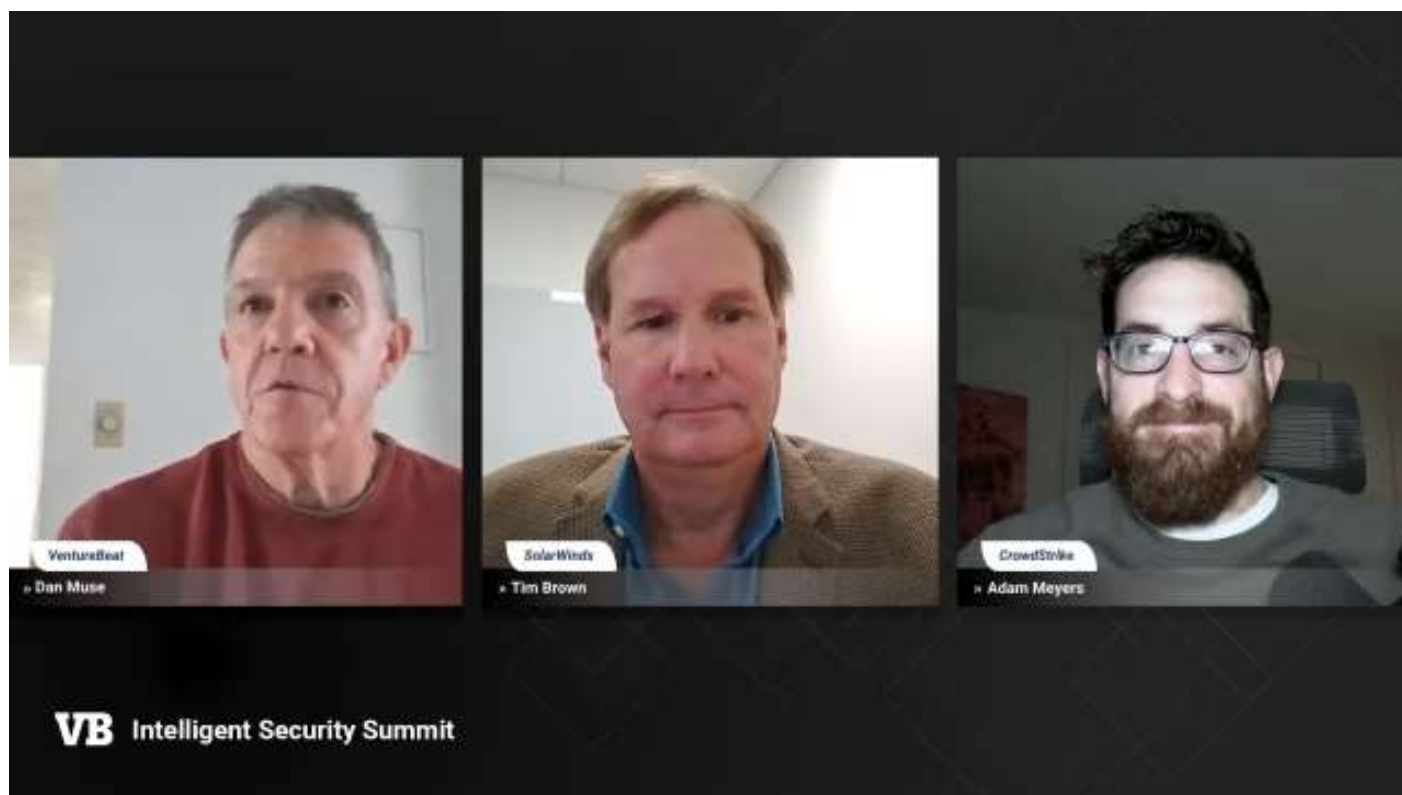


Image Credit: Getty Images

Join top executives in San Francisco on July 11-12, to hear how leaders are integrating and optimizing AI investments for success. [Learn More](#)

Although it's a commercially available software product from a U.S.-based cybersecurity vendor, Cobalt Strike is one of the most popular tools used by cybercriminals, primarily because of its versatility and efficacy in carrying out cyberattacks.

But while Cobalt Strike has been utilized for malicious purposes for years, the damage associated with its use has surged in the past few years. In particular, there's a strong [correlation](#) between use of Cobalt Strike and ransomware attacks, numerous researchers have [found](#).



combat the problem, according to the cofounder of [Red Canary](#), a [prominent](#) managed detection and response firm that has researched the issue.

“We just want to see some level of ownership over the proliferation of the tool,” said Keith McCammon, who is chief security officer at Red Canary and heads the company’s security strategy, operations and threat research.



EVENT

Transform 2023

Join us in San Francisco on July 11-12, where top executives will share how they have integrated and optimized AI investments for success and avoided common pitfalls.

[Register Now](#)

It's long been common for [threat actors](#) to use legitimate tools in illegitimate ways. But recently, "the costs associated with their use have gone completely out of control," McCammon said.

A prevalent threat

VentureBeat spoke with McCammon in connection with the release of Red Canary's [2022 Threat Detection Report](#). Cobalt Strike ranked as the third most prevalent threat tracked in the report, affecting 7.9% of Red Canary customers last year. The threat ranked behind only the TA551 threat group and the Mimikatz credential-stealing tool.

Cobalt Strike is widely used for its intended purpose by red teams — "ethical hackers" who play the part of a cyber adversary to test companies' defenses. But it's popular with cyber criminals for the same reason: The tool can be used to carry out a malicious cyber operation essentially from start to finish, McCammon said.

In at least one case, [documented](#) by Brian Krebs, the legitimate version of Cobalt Strike was obtained by a threat actor that had set up a shell company.

But for the most part, the cyber industry believes that [cybercriminals](#) are using cracked versions of the Cobalt Strike software, McCammon said.

Simply put, [Cobalt Strike](#) is popular because it does the job: According to the HelpSystems datasheet, the post-exploitation tool enables everything from client-side reconnaissance, to post-exploitation payload deployment, to covert communication.

"It is an end-to-end tool to orchestrate and execute a full-scope intrusion, and remain undetected," McCammon said.

Major ransomware groups such as Conti, Ryuk and REvil are known to have utilized Cobalt Strike significantly, helping to drive the expansion of the ransomware threat. In all, the number of ransomware attacks [more than doubled](#) in 2021 — jumping 105%

during the year compared to 2020, according to SonicWall. And the average ransom demand grew 36% to \$6.1 million last year, CrowdStrike [reported](#).

Tough questions

The use of Cobalt Strike by threat actors has become so costly that there is a question about whether Cobalt Strike is doing more harm than good by being commercially available, according to McCammon. If the tool were pulled from the market, eventually the cracked versions of the software would stop being effective as defenders caught up with it, he said.

But barring that unlikely move, there are many other steps that [HelpSystems](#) could take to assist with the problem, McCammon said.

It's true that HelpSystems has built in aspects that make Cobalt Strike harder to pirate, and make it easier to discern good use versus malicious use, he said. But the company can go further, according to McCammon.

For starters, there needs to be a level of transparency around the licensing process, he said. If HelpSystems were to provide a means of license attribution — in the cases where the legitimacy of the product use is in question — that could help to thwart illegitimate usage, McCammon said.

Another licensing issue is that, ironically, cyber researchers and defenders are unable to commercially acquire Cobalt Strike. Its sale is restricted to offensive cyber operations.

“That’s probably been one of the single biggest frustrations from the industry over the years,” said McCammon, who cofounded Red Canary in 2013. “We can’t control [criminals] getting their hands on it — but the thing that HelpSystems can control is to make sure that organizations that are in a position to defend, have the same level of access to it.”

Thus, there ought to be a license that allows defenders to legally acquire Cobalt Strike, he said. “And if there are constraints that come with that, those are probably things we can work through,” McCammon said.

Curbing misuse

In terms of curtailing the proliferation of Cobalt Strike in cybercrime, McCammon said he'd like to see HelpSystems do more as well. Ideally, he said, this would include seeking and validating illegitimate instances of the software or its corresponding infrastructure.

“Let’s focus on folks who shouldn’t have this in the first place, who absolutely did not buy it,” McCammon said. “And [HelpSystems can] take some ownership from that perspective. They should do their part to identify those instances, and do their part to support other organizations who are identifying it.”

And lastly, once HelpSystems has compiled this information, the company should disseminate it to those in the industry that are in a position to act on it, he said.

“It seems kind of utopian, but there’s precedent for working together in this way in InfoSec,” McCammon said. “When we do pinpoint malicious infrastructure or misuse, we can get that out to as many of the right folks as possible, as fast as possible.”

Ultimately though, when it comes to the threat posed by malicious Cobalt Strike usage, “none of these actions would even come close to solving the problem. But they’re steps in the right direction,” McCammon said. “The act of partnership, I think, is what the whole industry would benefit from.”

VentureBeat provided HelpSystems with the chance to respond to each of these points, including to the potential harms of Cobalt Strike’s commercial availability, questions about licensing and potential ways to curb illegitimate usage.

“At this time, we are not answering direct questions,” HelpSystems said in a statement provided to VentureBeat. “But please be aware that HelpSystems takes its vetting and product development processes seriously and remains dedicated to ensuring Cobalt Strike remains a world-class cybersecurity tool to help approved organizations with security operations and incident response.”

Strategic Cyber, the company that originally developed Cobalt Strike, was founded in 2012. HelpSystems [acquired](#) the Cobalt Strike maker in March 2020.

Eden Prairie, Minnesota-based HelpSystems is owned by [private equity](#) firms including TA Associates and Harvest Partners, and has made a string of acquisitions since

acquiring Cobalt Strike. The acquisitions have included Digital Guardian, PhishLabs, Agari, Beyond Security, Digital Defense, FileCatalyst and Vera. Most recently, HelpSystems has announced agreements over the past two months to acquire Tripwire and Alert Logic.

VentureBeat's mission is to be a digital town square for technical decision-makers to gain knowledge about transformative enterprise technology and transact. [Discover our Briefings.](#)

B

[Press Releases](#)[Contact Us](#)[Advertise](#)[Share a News Tip](#)[Contribute to DataDecisionMakers](#)[Careers](#)[Privacy Policy](#)[Terms of Service](#)[Do Not Sell My Personal Information](#)

© 2023 [VentureBeat](#). All rights reserved.

EXHIBIT 3



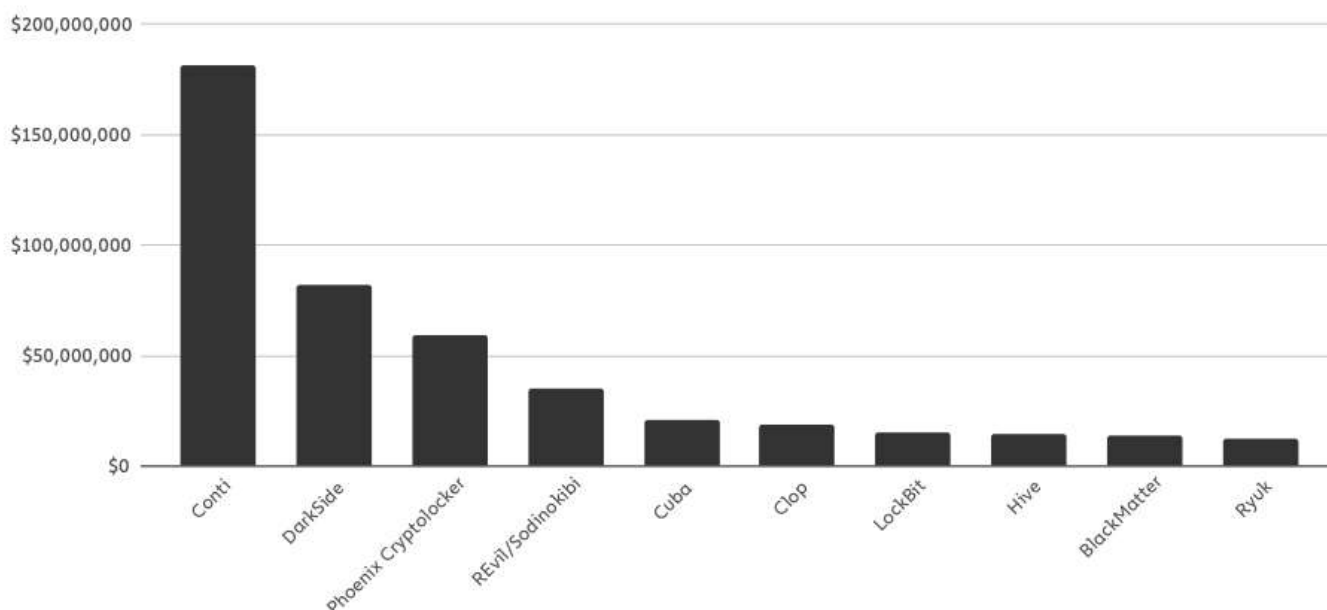
Conti Ransomware Group Diaries, Part III: Weaponry

March 4, 2022

23 Comments

Part I of this series examined newly-leaked internal chats from the **Conti** ransomware group, and how the crime gang dealt with its own internal breaches. Part II explored what it's like to be an employee of Conti's sprawling organization. Today's Part III looks at how Conti abused popular commercial security services to undermine the security of their targets, as well as how the team's leaders strategized for the upper hand in ransom negotiations with victims.

Top 10 ransomware strains by revenue | 2021



Conti is by far the most aggressive and profitable ransomware group in operation today. Image: Chainalysis

Conti is by far the most successful ransomware group in operation today, routinely pulling in multi-million dollar payments from victim organizations. That's because more than perhaps any other

ransomware outfit, Conti has chosen to focus its considerable staff and talents on targeting companies with more than \$100 million in annual revenues.

As it happens, Conti itself recently joined the \$100 million club. According to the latest Crypto Crime Report (PDF) published by virtual currency tracking firm **Chainalysis**, Conti generated at least \$180 million in revenue last year.

On Feb. 27, a Ukrainian cybersecurity researcher who is currently in Ukraine leaked almost two years' worth of internal chat records from Conti, which had just posted a press release to its victim shaming blog saying it fully supported Russia's invasion of his country. Conti warned it would use its cyber prowess to strike back at anyone who interfered in the conflict.

The leaked chats show that the Conti group — which fluctuated in size from 65 to more than 100 employees — budgeted several thousand dollars each month to pay for a slew of security and antivirus tools. Conti sought out these tools both for continuous testing (to see how many products detected their malware as bad), but also for their own internal security.

A chat between Conti upper manager “**Reshaev**” and subordinate “**Pin**” on Aug. 8, 2021 shows Reshaev ordering Pin to quietly check on the activity of the Conti network administrators once a week — to ensure they're not doing anything to undermine the integrity or security of the group's operation. Reshaev tells Pin to install endpoint detection and response (EDR) tools on every administrator's computer.

“Check admins' activity on servers each week,” Reshaev said. “Install EDR on every computer (for example, Sentinel, Cylance, CrowdStrike); set up more complex storage system; protect LSAS dump on all computers; have only 1 active accounts; install latest security updates; install firewall on all network.”

Conti managers were hyper aware that their employees handled incredibly sensitive and invaluable data stolen from companies, information that would sell like hotcakes on the underground cybercrime forums. But in a company run by crooks, trust doesn't come easily.

“You check on me all the time, don't you trust me?,” asked mid-level Conti member “**Bio**” of “**Tramp**” (a.k.a. “**Trump**”), a top Conti overlord. Bio was handling a large bitcoin transfer from a victim ransom payment, and Bio detected that Trump was monitoring him.

“When that kind of money and people from the street come in who have never seen that kind of money, how can you trust them 1,000%?” Trump replied. “I've been working here for more than 15 years and haven't seen anything else.”

OSINT

Conti budgeted heavily for what it called “OSINT,” or open-source intelligence tools. For example, it subscribed to numerous services that can help determine who or what is behind a specific Internet Protocol (IP) address, or whether a given IP is tied to a known virtual private networking

(VPN) service. On an average day, Conti had access to tens of thousands of hacked PCs, and these services helped the gang focus solely on infected systems thought to be situated within large corporate networks.

Conti's OSINT activities also involved abusing commercial services that could help the group gain the upper hand in ransom negotiations with victims. Conti often set its ransom demands as a percentage of a victim's annual revenues, and the gang was known to harass board members of and investors in companies that refused to engage or negotiate.

In October 2021, Conti underling "**Bloodrush**" told his manager "**Bentley**" that the group urgently needed to purchase subscriptions to **Crunchbase Pro** and **Zoominfo**, noting that the services provide detailed information on millions of companies, such as how much insurance a company maintains; their latest earnings estimates; and contact information of executive officers and board members.

In a months-long project last year, Conti invested \$60,000 in acquiring a valid license to **Cobalt Strike**, a commercial network penetration testing and reconnaissance tool that is sold only to vetted partners. But stolen or ill-gotten "Coba" licenses are frequently abused by cybercriminal gangs to help lay the groundwork for the installation of ransomware on a victim network. It appears \$30,000 of that investment went to cover the actual cost of a Cobalt Strike license, while the other half was paid to a legitimate company that secretly purchased the license on Conti's behalf.

Likewise, Conti's Human Resources Department budgeted thousands of dollars each month toward employer subscriptions to numerous job-hunting websites, where Conti HR employees would sift through resumes for potential hires. In a note to Conti taskmaster "**Stern**" explaining the group's paid access on one employment platform, Conti HR employee "**Salamandra**" says their workers have already viewed 25-30 percent of all relevant CVs available on the platform.

"About 25% of resumes will be free for you, as they are already opened by other managers of our company some CVs are already open for you, over time their number will be 30-35%," Salamandra wrote. "Out of 10 CVs, approximately 3 will already be available."

Another organizational unit within Conti with its own budget allocations — called the "**Reversers**" — was responsible for finding and exploiting new security vulnerabilities in widely used hardware, software and cloud-based services. On July 7, 2021, Stern ordered reverser "**Kaktus**" to start focusing the department's attention on **Windows 11**, Microsoft's newest operating system.

"Win11 is coming out soon, we should be ready for this and start studying it," Stern said. "The beta is already online, you can officially download and work."

BY HOOK OR BY CROOK

The chats from the Conti organization include numerous internal deliberations over how much different ransomware victims should be made to pay. And on this front, Conti appears to have

sought assistance from multiple third parties.

Milwaukee-based cyber intelligence firm Hold Security this week posted a screenshot on Twitter of a conversation in which one Conti member claims to have a journalist on their payroll who can be hired to write articles that put pressure on victim companies to pay a ransom demand.

“There is a journalist who will help intimidate them for 5 percent of the payout,” wrote Conti member “**Alarm**,” on March 30, 2021.

The Conti team also had decent working relationships with multiple people who worked at companies that helped ransomware victims navigate paying an extortion demand in virtual currency. One friendly negotiator even had his own nickname within the group — “**The Spaniard**” — who according to Conti mid-level manager **Mango** is a Romanian man who works for a large ransomware recovery firm in Canada.

“We have a partner here in the same panel who has been working with this negotiator for a long time, like you can quickly negotiate,” Trump says to Bio on Dec. 12, 2021, in regards to their ransomware negotiations with **LeMans Corp.**, a large Wisconsin-based distributor of powersports equipment [LeMans declined to comment for this story].

Trump soon after posts a response from their negotiator friend:

“They are willing to pay \$1KK [\$1 million] quickly. Need decryptors. The board is willing to go to a maximum of \$1KK, which is what I provided to you. Hopefully, they will understand. The company revenue is under \$100KK [\$100 million]. This is not a large organization. Let me know what you can do. But if you have information about their cyber insurance and maybe they have a lot of money in their account, I need a bank payout, then I can bargain. I’ll be online by 21-00 Moscow time. For now, take a look at the documents and see if there is insurance and bank statements.”

In a different ransom discussion, the negotiator urges Conti to reconsider such a hefty demand.

“My client only has a max of \$200,000 to pay and only wants the data,” the negotiator wrote on Oct. 7, 2021. “See what you can do or this deal will not happen.”

Many organizations now hold cyber insurance to cover the losses associated with a ransomware attack. The logs indicate Conti was ambivalent about working with these victims. For one thing, the insurers seemed to limit their ability to demand astronomical ransom amounts. On the other hand, insured victims usually paid out, with a minimum of hassle or protracted back-and-forth negotiations.

“They are insured for cyber risks, so what are we waiting for?” asks Conti upper manager “**Revers**,” in a conversation on Sept. 14, 2021.

“There will be trades with the insurance company?” asks Conti employee “**Grant.**”

“That’s not how it works,” Revers replied. “They have a coverage budget. We just take it and that’s it.”

Conti was an early adopter of the ransomware best practice of “double extortion,” which involves charging the victim two separate ransom demands: One in exchange for a digital key needed to unlock infected systems, and another to secure a promise that any stolen data will not be published or sold, and will be destroyed. Indeed, some variation of the message “need decryptors, deletion logs” can be seen throughout the chats following the gang’s receipt of payment from a victim.

Conti victims were directed to a page on the dark web that included a countdown timer. Victims who failed to negotiate a payment before the timer expired could expect to see their internal data automatically published on Conti’s victim shaming blog.

The beauty of the double extortion approach is that even when victims refuse to pay for a decryption key — perhaps because they’re confident they can restore systems from backups — they might still pay to keep the breach quiet.

“Hello [victim company redacted],” the gang wrote in January 2022. “We are Conti Group. We want to inform that your company local network have been hacked and encrypted. We downloaded from your network more than 180GB of sensitive data. – Shared HR – Shared_Accounting – Corporate Debt – Departments. You can see your page in the our blog here [dark web link]. Your page is hidden. But it will be published if you do not go to the negotiations.”

“We came to an agreement before the New Year,” Conti member “**Skippy**” wrote later in a message to the victim company. “You got a lot of time, more than enough to find any sum and fulfill your part of this agreement. However, you now ask for additional time, additional proofs, etc. Seems like you are preparing to break the agreement and flee, or just to decrease the sum. Moreover, it is a very strange request and explanation. A lot of companies pay such amounts without any problems. So, our answer: We are waiting for the above mentioned sum until 5 February. We keep our words. If we see no payment and you continue to add any conditions, we begin to upload data. That is all.”

And a reputation for keeping their word is what makes groups like Conti so feared. But some may come to question the group’s competence, and whether it may now be too risky to work with them.

On Mar. 3, a new Twitter account called “Trickbotleaks” began posting the names, photos and personal information of what the account claimed were top Trickbot administrators, including information on many of the Conti nicknames mentioned throughout this story. The Trickbotleaks Twitter account was suspended less than 24 hours later.

On Mar. 2, the Twitter account that originally leaked the Conti chat (a.k.a. “jabber”) records posted fresh logs from the Conti chat room, proving the infiltrator still had access and that Conti hadn’t

figured out how they'd been had.

“Ukraine will rise!,” the account tweeted. “Fresh jabber logs.”

If you liked this story, check out Part IV: Cryptocrime, which explores different schemes that Conti pursued to invest in and steal cryptocurrencies.

This entry was posted on Friday 4th of March 2022 03:20 PM

NE'ER-DO-WELL NEWS

RANSOMWARE

RUSSIA'S WAR ON UKRAINE

ALARM BENTLEY BIO BLOODRUSH CHAINALYSIS COBALT STRIKE CONTI GRANT KAKTUS LEMANS CORPORATION PIN RANSOMWARE RESHAEV REVERS SALAMANDRA SKIPPY THE SPANIARD TRAMP TRICKBOTLEAKS TRUMP

23 thoughts on “Conti Ransomware Group Diaries, Part III: Weaponry”

JamminJ

March 4, 2022

“Tramp” (a.k.a. “Trump”), a top Conti overlord.

Says it all

Klaus

March 8, 2022

Clinton was thought to have been shot down by Fancy Bear, not Conti. Are you suggesting that Tramp/Trump was a former Fancy Bear member?

Well, perhaps the pay is better for a Conti overlord than in a state-funded group, but what would the FSB (Федеральная служба безопасности Российской Федерации) say about such a move?

Dennis Hunter

March 8, 2022

I like your comments. Don't stop

The Sunshine State

March 5, 2022

Part 4 ?

JamminJ touches kids

March 5, 2022

JamminJ, do you still bitch and moan about George Bush too? Jesus Christ, get over it and take your political hot garbage elsewhere.

thegreyfoxx

-
March 5, 2022

Yeah, I'm real tired of his pontifications too. he needs to create his own rant blog. someone might follow him, but he sure is an arrogant 'know it all' nuisance here.

Readership1

-
March 6, 2022

You are free not to comment or even read the comments if you wish. Whether wrong, right or just an opinion at least JamminJ has something to say. Do you have anything at all to add?

factoid

-
March 8, 2022

It's more that he repeats what others are saying as if he is coming up with it. Over and over and over. People who require attention are annoying. Oh well.

maruchan

-
March 7, 2022

Worse is when he repeats what someone else said as if fixing it. Some people have no filter for indulgent self-involvement.

Readership1

-
March 8, 2022

Where do you see JamminJ repeating what others are saying? His was the first comment here. It's more likely that he's just triggering people who support Trump. Just being a know it all doesn't invite such vitriol. But politics is certainly divisive enough.

The fact that the first response was to accuse pedophilia suggests a political motive against JamminJ and not one based on just being annoying. Very similar attacks that we see from Q Anon believers.

maruchan

-
March 15, 2022

Excellent obfuscation, or you think this is his first comment? My observation has nothing to do with pedophilia nor politics, nor Trump, nor Q-Anon, so maybe read more carefully or not.

Readership1

-
March 16, 2022

That was his first comment here, yes. Regardless of your claimed observation, I don't see any problem with JamminJ comments on

this article. You say it has nothing to do with pedophilia or politics but you are replying to and agreeing with a comment that accused both. I read carefully and so should you. Read the comments that you are replying to and agreeing with. The only explanation for all these replies trying to pile on, is that its politically motivated.

hypocrite magats

March 6, 2022

Moaning about trump 14 months after he left office isn't the same as moaning about Bush after 14 years.

And Trump supporters are still bitching about Clinton after all. Their default accusation seems to be to call someone a pedo. Sounds like you would storm into a non-existent pizzeria basement.

History is showing maga cultists to be hypocrites and traitors to the county. Reagan wouldn't have sided with Putin, and it's pathetic that any self respecting Republican would defend Russia here.

This is political of course. Russian kleptocrats love Trump and Trump loves them. So it makes sense that one of Conti's criminals takes the name Trump.

Ed

March 5, 2022

What I don't understand is that if these high \$ value extortions are true, then why have these thieves have not been the subject of those that specialize in private sector wet work. It doesn't make sense that this industry is permitted to thrive. The only explanation is that there are bigger, more powerful benefactors and sponsors involved.

Eugene Craine

March 5, 2022

Many of the Conti group live in Russia which is so corrupt that any and all information is available for the right price. Because nothing happens in Russia without the FSB permission it should be fairly straight forward to find a source in local law enforcement or FSB who would sell the identities of the Conti group. Police salaries in Russia are not exhorbitant and corruption is endemic. You can buy databases on street corners in Moscow. Then it's a simple matter of sending the right people to their homes to persuade them to cease and desist. It would be a lot cheaper than handing over a seven figure ransom. There are thousands of ex military in Russia with the right skills and the willingness to do the job. Most Russians are not well off with yachts and mansions.

ReadandShare

March 5, 2022

I did not realize that conti revenues are so much higher than all the rest!

Kenar

March 5, 2022

These crooks are all trading in crypto to me it could be regulated out of existence with good regulations.

Cristian

March 7, 2022

En español: <https://blog.segu-info.com.ar/2022/03/diarios-del-grupo-ransomware-conti-iii.html>

Cached Comments

March 7, 2022

The reason why users don't see new comments (even after moderator approved) and engagement has been so low.

At some point earlier this year, W3TC memcached was turned on. Not sure if this was intentional to prevent Layer 7 DOS attacks on the site, or if Brian is aware that comments are also cached.

Source of the page:

Performance optimized by W3 Total Cache. Learn more: <https://www.boldgrid.com/w3-total-cache/>

Object Caching 174/175 objects using memcached

Page Caching using memcached

Database Caching 13/18 queries in 0.005 seconds using memcached

Served from: krebsonsecurity.com @ 2022-03-06 17:03:42 by W3 Total Cache

That's almost 24 hours ago.

A WP blog with an active comment section should not be so heavily cached.

SeymourB

-

March 7, 2022

Maybe everyone's tired of criminals posting nonsense to Krebs comment threads and that's why they're not being approved anymore.

Stop looking for complex conspiracies when a much simpler explanation will do.

Appsec1

-

March 8, 2022

He's not talking about comments being approved or denied by the moderator.

He's talking about comments that are approved not awaiting moderator and are actually posted. These comments are there but they are still not always visible for up to 24 hours because the entire page is cached from a previous version.

It's not a conspiracy. It's plain text right there in the source page. Look for yourself.

Henry

-

March 8, 2022

I see the source code too. It's a commented out note from W3 Total Cache.

That explains why comments seem to show up and disappear randomly when refreshing the page. Thanks.

Mainline

March 8, 2022

Seems inevitable that Conti and many other Russian based ransomware gangs will be sanctioned by the US government and NATO allies.

This is going to have a profound effect on the economics. Victim businesses will no longer be able to pay these ransoms. Cybersecurity insurance can still cover losses and recovery costs, but decryptors and promises to keep Conti from posting the data won't be legal anymore.

I know, many people who argue against making ransomware payments illegal say that companies will just stop reporting breaches.

But I disagree. Companies avoid reporting all kinds of breaches. Most breaches do not involve paying ransomware. They are just damaging to reputation, so they don't report. Paying large sums of money is something that corporations usually cannot hide. Publicly traded companies absolutely cannot just hide a ransomware payment, they risk way more than their reputation for cooking the books. Even private companies can be audited by the IRS and easily show a large payment made to buy cryptocurrency.

So if a victim company doesn't want to report a breach, that's still legal, but making a million dollar purchase of bitcoin to send to an overseas wallet owned by Russian cyber criminals... that's something the government can and should sanction.

"Russia is the world's largest exporter of decryptors". It's a billion dollar industry, with Conti as the largest share. Conti has already sided with Putin. Time to sanction those exports and cut off their funding. North American and European businesses should not be funding Conti, Putin, or his oligarchs.

Comments are closed.

© Krebs on Security - Mastodon

EXHIBIT 4

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 the trend of increasing use of hacking tools as more threat actors adopt hacking tools in their operations.

How can I help you today?

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.

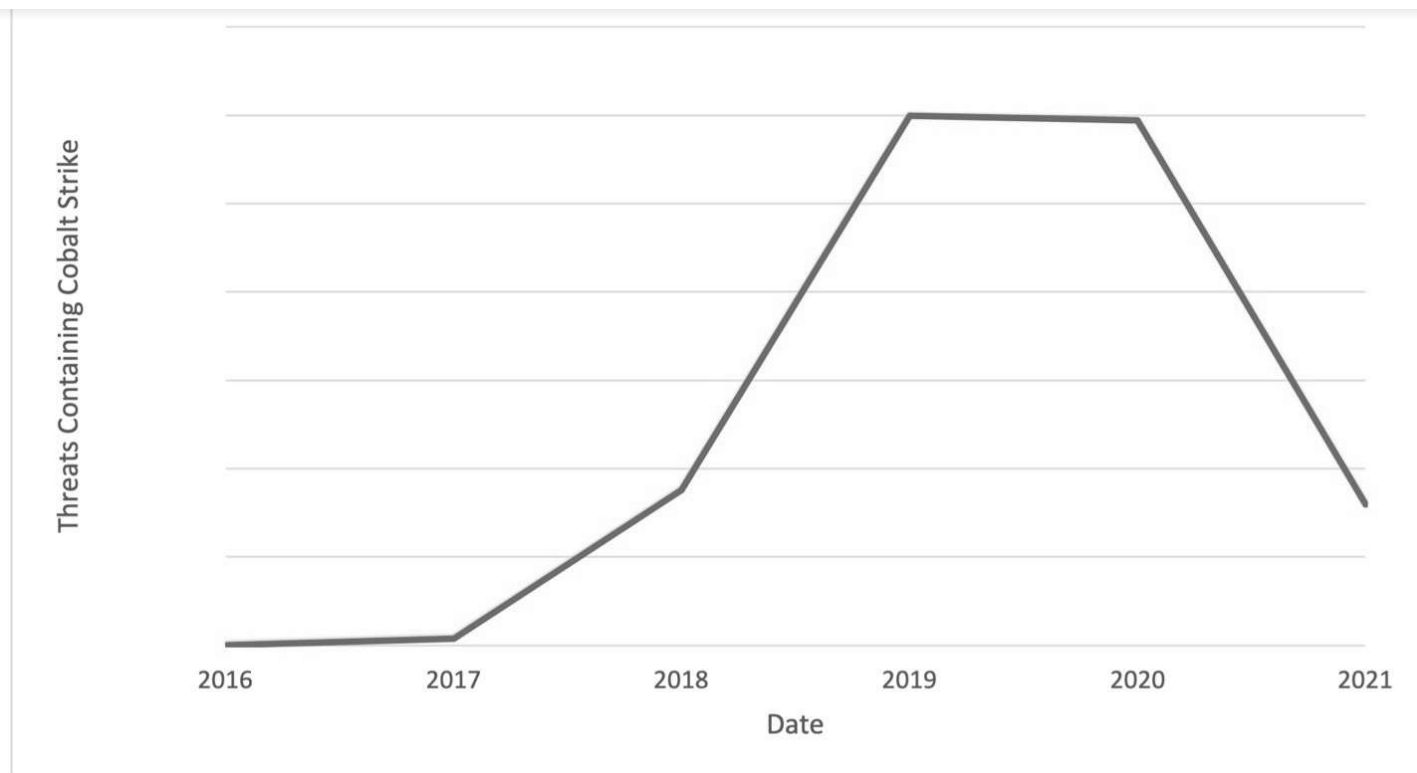


Figure 1: Number of email messages associated with a Cobalt Strike payload observed over time. Note: 2021 figures include data through May 2021.

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.

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

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.

BRIEF TIMELINE OF COBALT STRIKE THREATS

COBALT STRIKE USE IN CYBERATTACKS IS INCREASING. THE FOLLOWING HIGH-PROFILE EVENTS INCLUDED COBALT STRIKE USE.

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

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.

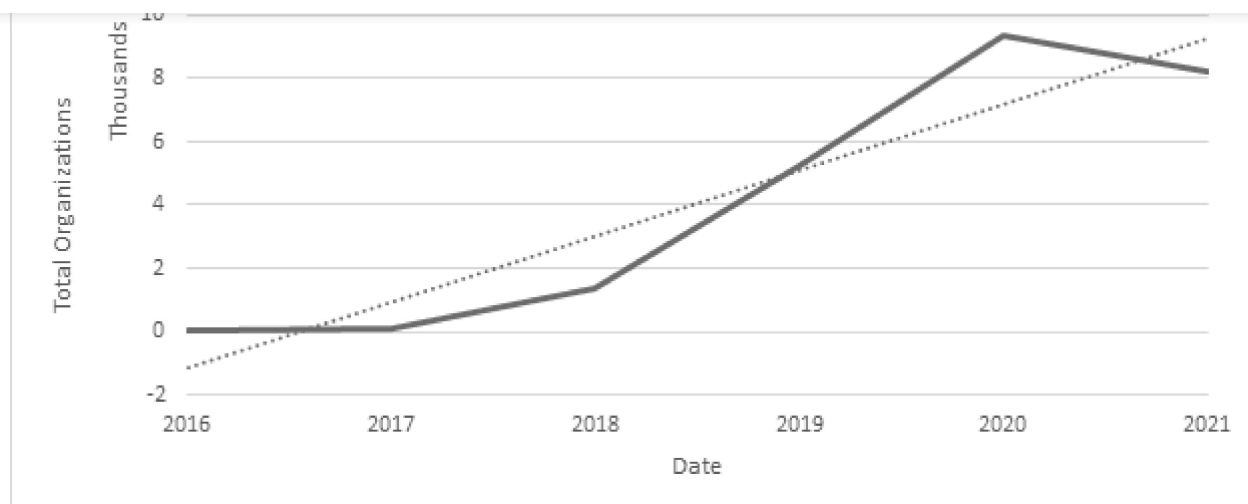


Figure 3: Number of customers targeted by threats using Cobalt Strike

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

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

Blog Interest:

Submit

About

- Overview
- Why Proofpoint
- Careers
- Leadership Team
- News Center
- Nexus Platform
- Privacy and Trust

Threat Center

- Threat Hub
- Cybersecurity Awareness Hub
- Ransomware Hub
- Threat Glossary
- Threat Blog
- Daily Ruleset

Products

- Email Security & Protection
- Advanced Threat Protection
- Security Awareness Training
- Cloud Security
- Archive & Compliance

Resources

- White Papers
- Webinars
- Data Sheets
- Events
- Customer Stories

Product Bundles

Connect

+1-408-517-4710

Contact Us

Office Locations

Request a Demo

Support

Support Login

Support Services

IP Address Blocked?



© 2023. All rights reserved.

Terms and conditions

Privacy Policy

Sitemap

EXHIBIT 5

Cybercrime , Fraud Management & Cybercrime , Fraud Risk Management

Attackers Increasingly Using Cobalt Strike

Report: Pen Testing Tool a Favorite Among Lower-Level Threat Groups

Doug Olenick (🐦DougOlenick) • June 30, 2021 

The solid blue line tracks the number of organizations Proofpoint saw being targeted by attackers using Cobalt Strike. (Source: Proofpoint)

The legitimate security penetration testing tool Cobalt Strike is increasingly being used by threat groups, especially those that are less technically proficient, according to a Proofpoint report released Tuesday.


See Also: LIVE Webinar | Stop, Drop (a Table) & Roll: An SQL Highlight Discussion

Researchers at the security firm say the number of attacks using Cobalt Strike increased 161% between 2019 and 2020, and the tool remains a high-volume threat in 2021. It's been used in a wide variety of attacks - including the SolarWinds supply chain attack - and for cyberespionage campaigns, leading Proofpoint to conclude that it's a favorite tool of advanced persistence threat groups.

"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," Proofpoint says.

Why Attackers Like Cobalt Strike

Some of the tool's useful features for an attacker are its user-friendliness, its obfuscation capabilities and its ability to be used as either a first- or second-stage downloader.

Proofpoint notes that as Cobalt Strike has been updated over the years, it has moved from 

being used almost exclusively by well-resourced crime groups - such as FIN7, the APT group Leviathan and APT40 - to becoming more mainstream for a broader range of criminals.

One reason for that is that Cobalt Strike is easy to obtain. An attacker can attempt to buy it legitimately from the developer, although there's a verification process in place to ensure the tool does not fall into the hands of a cybercriminal. And the tool is also widely available for purchase on the darknet, including a cracked version of the latest Cobalt Strike 4.0, Proofpoint says.

The software is highly customizable and can be removed without leaving any evidence behind. It can help enable an attacker to exfiltrate data, drop a second payload and essentially behave as if it belongs inside a system.

"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," Proofpoint says.

HelpSystems, which developed Cobalt Strike, did not immediately reply to a request for comment on the Proofpoint report.

Groups Using Cobalt Strike as Malware

"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," according to Proofpoint. "For example, APT29 frequently uses custom Cobalt Strike Beacon loaders to blend in with legitimate traffic or evade analysis," the security firm says.

Another group known to use Cobalt Strike is the crime gang TA800, which specializes in banking malware attacks. TA800 recently underwent a shift in how it delivers Cobalt Strike. Starting in 2019, after gaining initial entry, the gang would inject BazaLoader, which downloads Cobalt Strike. In February, the group reversed this process, distributing Cobalt Strike as a first-stage payload via malicious URLs.

Also in February, TA547, which uses banking Trojans, began distributing Cobalt Strike as a second-stage payload to establish command and control, Proofpoint says.

Our website uses cookies. Cookies enable us to provide the best experience possible and help us understand how visitors use our website. By clicking "Accept", you consent to our use of cookies.

Barium, also known as APT41 and TA415, used Cobalt Strike in several campaigns in 2020. This group is believed to be associated with the People's Republic of China's Ministry of State Security, Proofpoint says.

Cobalt Strike and SolarWinds

The group behind the SolarWinds supply chain attack, which the U.S. government believes to be Russian and which Microsoft named Nobelium, extensively used Cobalt Strike. A Microsoft analysis of the attack released in January showed the attackers used Cobalt Strike to maintain persistence and remain hidden to give them time to fully penetrate systems, move laterally through networks and exfiltrate data in follow-on attacks.

When activating the second stage of an attack, Microsoft said, the hackers "went out of their way" to ensure that the backdoor they initially installed in the SolarWinds' Orion network monitoring platform was separated "as much as possible" from Cobalt Strike loader implants they used to escalate the attack, paving the way for exfiltrating data.

Microsoft says the attackers apparently believed that this approach meant that if Cobalt Strike - a legitimate penetration testing tool - was detected in an infected system, the victim would not notice the connection to the SolarWinds Orion backdoor.

Defending Against Cobalt Strike

Sherrod DeGrippe, senior director of threat research and detection with Proofpoint, says organizations can take steps to spot an illegitimate use of Cobalt Strike.

Email security tools can block first-stage delivery of Cobalt Strike, and threat detection tools can identify a generic instance of Cobalt Strike in a company network that is not associated with another legitimate process, she says.

"Defenders can look at network communications to identify unusual activity, disallow communications to unrecognized IP addresses or domains, etc. It can be difficult to detect/defend against the tool, however, there are multiple resources available for defenders," DeGrippe says.

Our website uses cookies. Cookies enable us to provide the best experience possible and help us understand how visitors use our website. By browsing bankinfosecurity.com, you agree to our use of cookies.

Other Legitimate Tools Being Used for No Good

Proofpoint's researchers note that malicious actors are using other legitimate red team tools - including Mythic, Meterpreter and the Veil Framework - to ply their trade.

"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," Proofpoint says.

About the Author



Doug Olenick

Former News Editor, ISMG

Olenick has covered the cybersecurity and computer technology sectors for more than 25 years. Prior to his stint as ISMG as news editor, Olenick was online editor for SC Media, where he covered every aspect of the cybersecurity industry and managed the brand's online presence. Earlier, he worked at TWICE - This Week in Consumer Electronics - for 15 years. He also has contributed to Forbes.com, TheStreet and Mainstreet.



Our website uses cookies. Cookies enable us to provide the best experience possible and help us understand how visitors use our website. By browsing [bankinfosecurity.com](https://www.bankinfosecurity.com/), you agree to our use of cookies.

EXHIBIT 6

InformationWeek
IT NETWORK

Network Computing

Dark Reading

[Advertise](#)

[About Us](#)

SECTIONS



-
-
-
-
-
-
-
-
-
-

- [Perimeter](#)
- [Physical Security](#)
- [Risk](#)
- [Operations](#)
- [Analytics](#)
- [Vulns/Threats](#)
- [Threat Intelligence](#)
- [Careers and People](#)
- [IoT](#)
- [Security Now](#)
- [Omdia](#)



[Login to your account](#)

[Register](#)

[About Us](#)

[Advertise](#)

-
-
-
-



Search Dark Reading



-
-
-
-

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

[RSS](#)

Search Dark Reading

Follow DR:

- [Authors](#)
- [Slideshows](#)
- [Video](#)

Search Dark Reading

- [THE EDGE](#)
- [Analytics](#)
- [Attacks / Breaches](#)
- [App Sec](#)
- [Cloud](#)
- [Endpoint](#)
- [IoT](#)
- [Operations](#)



This site uses cookies to provide you with the best user experience possible. By using Dark Reading, you accept [our use of cookies](#).



[Calendar](#)
[Black Hat News](#)
[Omdia Research](#)

[Threat Intelligence](#)
[Vulns / Threats](#)

[Attacks/Breaches](#)

5/19/2021 05:35 PM
Cobalt Strike Becomes a Preferred Hacking Tool by Cybercrime, APT Groups

[End of Biblio RCM includes -->](#)



Incident response cases and research show how the red-team tool has become a go-to for attackers.

Kelly Jackson Higgins News
Connect Directly:
0 comments
Comment

RSA CONFERENCE 2021 - For nearly two decades, the open source Metasploit hacking platform has garnered a mix of enthusiasm and frustration by security teams that both need the tools to test their own networks but also fear cybercriminals or other bad actors could use it against them in attacks.

Now Like Tweet Share
Metasploit remains popular today among good and bad hackers, but another red-team tool, Cobalt Strike, is increasingly playing a major role in attacks. Attackers are weaponizing the tool for the second stage of attacks to carry payloads (including Metasploit exploits) once they have penetrated the victim's network using customized, cloned, or even purchased versions of Cobalt Strike.

The threat-emulation software suite for penetration testing was created by researcher Raphael Mudge in 2012 and was acquired last year by HelpSystems. Its most popular component by nefarious hackers is Beacon, a payload that operates like an attacker, running PowerShell scripts, logging keystrokes, snapping screenshots, stealing files, and dropping other payloads or malware.

HelpSystems declined to comment for this article.

New data from Sophos that cataloged attacker behavior, tools,

Related Content:
[How to Identify Cobalt Strike on Your Network](#)



Editors' Choice
Subscribe to Newsletters

Live Events

White Papers

[Discover More From Informa Tech](#)

Webinars

[Empower Digital Transformation](#)

[The Smart Way to Shift Left](#)

[Working With Us](#)

[The Importance of Bespoke Security v2.0](#)

[Follow DarkReading On Social](#)

[How Firewalls Fit With Modern Enterprise Security](#)

[What Elite Threat Hunters See that Others Miss](#)

[Webinar Archives](#)

[The 2022 State of Cloud Security Report](#)

[Transform Your Security Strategy](#)

[More White Papers](#)

[Video](#) [Cartoon](#) [Current Issue](#)

threat hunters and incident responders last year and through the first part of 2021 shows that Cobalt Strike is one of the top five tools used by attackers. It's also a key element when attackers employ PowerShell commands to camouflage their activity on a victim's network. Nearly 60% of PowerShell exploits employ Cobalt Strike, and some 12% of attacks use a combination of Cobalt Strike and Microsoft Windows tools PowerShell and PsExec. It's also paired with PsExec in nearly a third of attacks, according to Sophos's new "[Active Adversary Playbook 2021](#)" report.

New From The Edge: How to Get Employees to Care About Security.

"Cobalt Strike lends itself to being deployed by PowerShell" and PsExec, says John Shier, senior security advisor at Sophos. "The code [Cobalt Strike] was leaked online a long time ago, [attackers] know how to use it, and it's an evasion technology" to remain under the radar as an attack escalates and spreads.

In one of its more high-profile uses by attackers, the Russian GRU hacking team behind the [SolarWinds supply-chain attack](#) campaign built custom shellcode loaders that dropped Cobalt Strike payloads: the Teardrop and Raindrop malware components of the attack.

Researchers and incident responders at Intel 471 say the malicious use of Cobalt Strike correlates with ransomware's rise in recent years, but it's also used for dropping other types of malware and for stealing data. Among the malware groups using Cobalt Strike: Trickbot, Hancitor, Qbot, SystemBC, Smokeloader, and Bazar. The researchers today published indicators of compromise that indicate Cobalt Strike is in play with these malware families.

Brandon Hoffman, CISO at Intel 471, says attackers appear to like the features of Cobalt Strike, specifically the Beacon component. "It has so many features built into it from a post-exploit tool perspective; it's a perfect fit for second-stage attack and instead of picking and choosing different pieces of malware, you just drop this tool and all of its features in it," he says.



Managing system vulnerabilities is one of the oldest - and most frustrating - security challenges that enterprise defenders face. Every software application and hardware device ships with intrinsic flaws - flaws that, if critical enough, attackers can exploit from anywhere in the world. It's crucial that defenders take stock of what areas of the tech stack have the most emerging, and critical, vulnerabilities they must manage. It's not just zero day vulnerabilities. Consider that CISA's Known Exploited Vulnerabilities (KEV) catalog lists vulnerabilities in widely used applications that are "actively exploited," and most of them are flaws that were discovered several years ago and have been fixed. There are also emerging vulnerabilities in 5G networks, cloud infrastructure, Edge applications, and firmwares

Latest Comment: I've heard of people walking right out the front door with entire servers...

[Download This Issue!](#)

[Back Issues](#) | [Must Reads](#)

Report

Dark Reading

Enterprise Vulnerabilities From Twitter's Source Code Leak on GitHub. CERT's National Vulnerability Database

bit.ly/3FRsaYT #Twitter

CVE-2023-1142

PUBLISHED: 2023-03-27

darkreading.com

Twitter's Source Code Leak on GitHub a Potential Cyber Nightmare

Electronics InfraSuite

How Data Breaches Affect the Enterprise

0 comments



different threat actor group. "Malleable C2 lets you mimic behavior or make C2 traffic look like almost any legitimate service," he says. So if an organization allows users to stream Pandora, for example, a Malleable C2 could be disguised as Pandora traffic in the victim's network, he says.

"That makes it extremely difficult" to spot an attack, Hoffman says. "Beacon is so customizable."

Even so, there are ways to spot malicious abuse of Cobalt Strike, experts say. Aside from bad guys making mistakes and leaving behind clues or breadcrumbs, you can spot a Cobalt Strike-borne attack unfold if you're monitoring activity: "Because Cobalt Strike is not generally used at the first attack vector, in the middle of an incident response [case] if you see something come in from one of the command-and-control servers it could potentially be Beacon," Hoffman explains. And if you create Yara rules for certain malicious scripts, that can detect it as well.

"Where we saw Cobalt Strike in the wild, some folks had repurposed it for the same malware family," says Hoffman, whose team today published its findings on cybercrime groups deploying Cobalt Strike (including indicators of compromise).

Ransomware Thread

"We've seen a correlation between the rise of Cobalt Strike use [by adversaries] and a rise in ransomware. We're not saying Cobalt Strike is fueling" ransomware, Hoffman says. It's more that ransomware is dropped at the later stages of an attack chain. "Before they get to the ransomware, attackers first have to deploy something like this [Cobalt Strike]." So, spotting that activity before ransomware is installed can save a lot of headache.

Speaking of ransomware, Sophos' IR and threat-hunting data found ransomware in more than 80% of the incidents they investigated. "Ransomware is noisy, it needs to grab attention," which is why those cases were flagged for an investigation, Sophos' Shier says. "[In] a lot of the attacks we stopped, we noticed there had been Cobalt Strike activity" as well, he says.

for to
responding 10.5,
to an
ransomware
attacker
Not could
sure/double
know. URL
decoding
to
retrieve
system All Polls
files,
credentials,
and
bypass
authentication
resulting
in
privilege
escalation.

Submit

CVE-2023-1143
PUBLISHED:
2023-03-27
In
Delta
Electronics
InfraSuite
Device
Master
versions
prior
to
1.0.5,
an
attacker
could
use
Lua
scripts,
which
could
allow
an
attacker
to
remotely
execute
arbitrary
code.

CVE-2023-1144
PUBLISHED:
2023-03-27
Delta
Electronics
InfraSuite
Device

payment card theft and ransomware campaigns. They described incidents where attackers using Bazar malware used Cobalt Strike payloads in advance of their dropping Ryuk ransomware on the victim, all within a two-hour window.

"Cobalt Strike is so common and reliable that adversaries create their own custom tooling to simply deploy the payloads, knowing that they will likely succeed if they can just get the payload past security controls. This capability demonstrates how Cobalt Strike fits into the threat model for nearly any organization," according to [Red Canary's report](#), which includes details on ways to detect malicious Cobalt Strike activity.

Kelly Jackson Higgins is the Executive Editor of Dark Reading. She is an award-winning veteran technology and business journalist with more than two decades of experience in reporting and editing for various publications, including Network Computing, Secure Enterprise ... [View Full Bio](#)

to
1.0.5
contains
an
improper
access
control
vulnerability
in
which
an
attacker
can
use
the
Device-
Gateway
service
and
bypass
authorization,
which
could
result
in
privilege
escalation.

CVE-
2023-
1145
PUBLISHED:

Comment | Email This | Print | RSS

More Insights

Webcasts

The Biggest Network Security Threats of 2023 & How to Combat Them

ITSM Guide to Evaluation and Selection

More Webcasts

White Papers

The Essential Guide to Secure Web Gateway

Enable and Protect Your Remote Workforce

More White Papers

Reports

Automate IT: Modernizing IT Service Management in Healthcare

10 Hot Talks From Black Hat USA 2022

More Reports

//Comments

~~Newest First~~ | ~~Oldest First~~ |

Threaded View

[Be the first to post a comment regarding this story.](#)

2023-
03-
27
Delta
Electronics
InfraSuite
Device
Master
versions
prior
to
1.0.5
are
affected
by
a
deserialization
vulnerability
targeting
the
Device-
DataCollect
service,
which
could
allow
deserialization
of
requests
prior
to
authentication,
resulting
in



CVE-
2023-
1655

PUBLISHED:

2023-
03-
27

Heap-
based
Buffer
Overflow
in
GitHub
repository
gpac/gpac
prior
to
2.4.0.

Interop

InformationWeek

Network Computing

ITPro Today

Data Center Knowledge

Black Hat

Contact us

About Us

Advertise

Reprints

[Home](#)

[Cookies](#)

[CCPA: Do not sell my personal info](#)

[Privacy](#)

[Terms](#)

Copyright © 2023 Informa PLC Informa UK Limited is a company registered in England and Wales with company number 1072954 whose registered office is 5 Howick Place, London, SW1P 1WG.

This site uses cookies to provide you with the best user experience possible. By using Dark Reading, you accept [our use of cookies](#).



EXHIBIT 7

Security Boulevard

POWERED BY Techstrong | Group

Home ▾ Security Bloggers Network ▾ Webinars ▾

Events ▾ Chat ▾ Library Related Sites ▾ About Us

Sponsor Techstrong Group

ANALYTICS APPSEC CISO

THREATS / BREACHES MORE

Container Journal

DevOps.com

Security Boulevard

Techstrong Research

Techstrong TV

Techstrong.tv Podcast

Techstrong.tv - Twitch

Devops Chat

DevOps Dozen

DevOps TV

IDENTITY INCIDENT RESPONSE IOT / ICS 🔍

Home » Security Bloggers Network » Cobalt Strike: The New Favorite Among Thieves



Cobalt Strike: The New Favorite Among Thieves

by Virginia Satrom on Security Boulevard

By Chris Gerritz

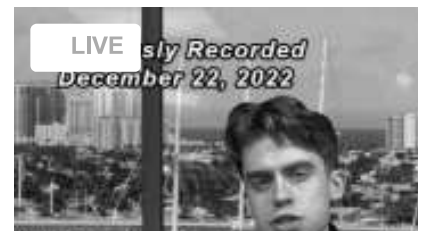
Since 2012, Cobalt Strike has been utilized as a proactive way of testing network defenses against advanced threat actor tools, tactics, and procedures (TTPs). The aim, of course, is to mimic the most malicious threat actors and their techniques to test your security posture and practice response procedures. Unfortunately, like most things in security, tools and knowledge meant to help security teams can also be used maliciously by criminals.

Though this is debated in some circles, offensive security research and offensive simulation tools like Cobalt Strike, are in my opinion, a net positive for the security community. A tool like Cobalt Strike is simply

Favorite

ite

Techstrong TV – Live



Click full-screen to enable volume control

Watch latest episodes and shows



Subscribe to our

simulating tactics and techniques already being used by hackers in the wild. Security teams need access to these tools in order to test against them.

Historically, penetration testing and simulation software had not been popular with competent cybercriminals due to the ubiquity of their use and familiarity to defenders — hackers usually relied on dark web exploit kits like Angler and Blackhole. This has flipped in recent years due to two reasons:

1. The availability of stable exploit kits on the dark web has reduced dramatically due to law enforcement actions against exploit kit authors.
2. Cobalt Strike has gotten good; real good.

Cobalt Strike – The Swiss Army Hacker Framework

Over the last two years, malicious threat actors have managed to crack fully-featured versions of Cobalt Strike and made them widely available within dark web marketplaces and forums. For instance, on March 22 this year, the latest version of the tool was cracked and provided to hackers. Infocyte has seen it widely used to infiltrate and laterally move through networks, and depending on what value is placed on a given company's data, ransomware is dropped. Infocyte has noticed a consistent upward trend of this cracked version as a primary methodology by threat actors since early 2019 to present.

Cobalt Strike is a favorite because it's stable and highly flexible. It can be repurposed to deploy all manner of payloads, like ransomware or keylogger, to the compromised network. It's well organized and provides a framework to manage compromised assets. Essentially, this tool helps the 'B list' act like 'A list' hackers.

While Cobalt Strike's author has implemented many protections and licensing schemes to keep the code out of the wrong hands, the cracked versions appear to utilize the entire framework of the solution. This means that threat actors have access to networks, are able to pivot, and then laterally move within the network. Implants called "beacons" support this lateral movement from system to system without even connecting to the internet. Only one of these beacons actually needs to

Newsletters

Get breaking news, free eBooks and upcoming events delivered to your inbox.

Enter your email address*

[View Security Boulevard Privacy Policy](#)

Subscribe Now

Most Read on the Boulevard

[Business Email Compromise Threats Soar Past Phishing Risks](#)

[AI/ML's Role in Software Supply Chain Security](#)

[ChatGPT Less Convincing Than Human Social Engineers in Phishing Attacks](#)

[Survey Surfaces Need to Change SecOps Priorities](#)

[Zoom Taps Okta to Bring Zero-Trust Cybersecurity to Videoconferences](#)

Upcoming Webinars »

APR [Key Strategies for a Secure and Productive Hybrid Workforce](#)

connect to the internet (the “beachhead”), making it more difficult to detect at the network layer.

A feature called “Maleable C2” enables hackers to easily modify their network signature with relative ease, while Maleable PE enables the same stealthy flexibility to the implants that are injected into system processes.

Cobalt Strike also utilizes modern staged delivery. Once within the network, numerous stages trigger as part of gaining access to the network and executing the hacker’s final agenda. Essentially, one stage will trigger, then the next stage. What makes this difficult to detect is that each stage is simple and can even be a single line of code. Alone, any one stage might not look malicious or throw any alarms. Even worse, when it finally enters the final stage, the earlier stages disappear, leaving nothing on disk.

Lateral movement is a huge part of Cobalt Strike. The laterally communicating beacons enable the attacker to worm their way into more valuable parts of the network. The objective is often to find a domain administrator and take over their account. Using this account, they can instruct the domain controllers to stage ransomware throughout the entire network prior to execution — this technique gives almost no time for defenders to react once the final trigger is initiated.

Infocyte has observed that this methodology can take a couple hours or up to two full weeks from the initial entry to executing the ransom demand.

Stopping a Ransom Before It’s Demanded

In a recent case, the Infocyte support team was engaged with a large healthcare provider that was investigating a strange alert. Their antivirus and other detection tools missed everything, but their application control luckily stopped one of the ransomware stages from executing something from a temp folder (this turned out to be the ransomware encryptor that had been scheduled to kick-off early on a Sunday morning). Infocyte was used to investigate these alerts and triage the network for any other signs of compromise. Within the first hour of deployment, we found:

04 April 4 @ 1:00 pm - 2:00 pm

AP
R
05 **Securing Kubernetes With SentinelOne and AWS**

April 5 @ 1:00 pm - 2:00 pm

AP
R
05 **From Vulnerable to Invincible: The Five-Step Journey to Complete Cloud Security**

April 5 @ 3:00 pm - 4:00 pm

AP
R
12 **The State of Cloud-Native Security 2023**

April 12 @ 1:00 pm - 2:00 pm

AP
R
13 **Case Study: Improving Code Security With Continuous Software Modernization**

April 13 @ 11:00 am - 12:00 pm

AP
R
20 **Lessons From a Live Hack: Secure Your Cloud From the Inside**

April 20 @ 3:00 pm - 4:00 pm

AP
R
24 **Securing Open Source**

April 24 @ 1:00 pm - 2:00 pm

M
AY
03 **[https://webinars.securityboulevard.com/ciso-panel-tips-for-optimizing-cloud-native-security-stack-in-2023?](https://webinars.securityboulevard.com/ciso-panel-tips-for-optimizing-cloud-native-security-stack-in-2023?utm_campaign=2023.05.03_Aqua_Webinar_SB&utm_source=BMRegister)**

utm_campaign=2023.05.03_Aqua_Webinar_SB&utm_source=BMRegister

May 3 @ 3:00 pm - 4:00 pm

1. Memory-resident Cobalt Strike beacons on three of their critical servers
2. Malicious powershell commands downloading additional malware from a Los Angeles IP address
3. The compromised account being exploited was a doctor's account who has been assigned overly permissive administrator privileges to the network
4. The ransomware loader (technically a non-malicious file on it's own) staged on thousands of workstations, servers, and medical devices.

Based on the scoping of the incident using triage data and conclusions provided by Infocyte, our support team recommended immediate action to purge the malicious actor from the network:

1. IP Blocks were made at the firewall for the address found by Infocyte
2. The compromised doctor's account was disabled
3. The servers infected with Cobalt Strike beacons were rebooted to clear their memory footprint and validation scans performed to ensure no persistence remained. (Infocyte has a button for this)
4. Infocyte removed the ransomware loaders and other artifacts from every system in the network
5. All domain admins underwent password resets
6. Following these initial containment actions, the organization retained an Infocyte partner to take over the full investigation and remaining cleanup actions.

These swift actions by the organization's IT and security teams, supported by Infocyte, purged the actor, stopped further Cobalt Strike spread, and prevented an in-progress second attempt to lock out and ransom this critical healthcare provider. These actions, from triage to containment, happened within the same evening. Without a detection and response capability and support, it could have been a very different story.

Initial Response Support Is Most Critical

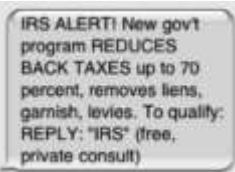
Most organizations spend a majority of their time and resources putting controls and protections in place to prevent these attacks from ever occurring. When such controls fail, detection and response expertise and capabilities are essential in the FIRST HOUR if you plan to mitigate an attack like this healthcare provider did. Too often we see organizations stumble in the first hour due to not understanding the scope and severity of an attack (lack of visibility) and not knowing what needs to get done first (lack of response experience and practice).

M **Ransomware**
 AY May 22 @ 1:00 pm - 2:00 pm
 22

Download Free eBook



Industry Spotlight »



FINALL
 Y! FCC
 Acts on
 SMS
 Scam-

Spam — But Will It Work?



White
 House
 to
 Regulat
 e Cloud

Security: Good Luck With
 That

'Extraordinary, Egregious'
 Data Breach at House and

Infocyte's Model: Our Customers Don't Go Through an Incident Alone

Infocyte is a Software-as-a-Service provider focusing on detection and response. We license our software to security teams and partner with MSSPs and security service providers to enable threat hunting, response and full scoped managed detection and response (MDR) services for organizations that have limited security manpower.

We are more than a product. Every member of Infocyte's support team is trained in incident response (IR) procedures and how to best use the Infocyte to find answers and take action. We often guide both end users in addition to acting as a backstop for our IR partners navigating these uncertain situations. For the most complex incidents, Infocyte has the ability to elevate to some of the most experienced and talented incident responders in the world—both on staff and in our partner network. We don't let our customers go through an incident alone.

Final Advice

Based on the tactics and methodology we've observed in the latest ransomware cases, we recommend that if your team encounters ransomware, the remediation and response shouldn't stop at the ransomware. It is very likely that there are hidden beacons within your network that have been missed: hiding in memory. Even if your endpoint protection stops the ransom, the perpetrator could still be inside with access to try again. Fully triaging and scoping an incident is essential to containment: you'll need a tool like Infocyte and a team to support your effort to ensure that all of the malicious code is remediated.

If you're interested in learning more, reach out to our sales team or request a demo.

The post Cobalt Strike: The New Favorite Among Thieves appeared first on Infocyte.

Recent Articles By Author

- [Hunting for SolarWinds Orion Compromises](#)
- [Simplifying O365 Security with Infocyte – Coming Fall 2020](#)



Senate

Top Stories »



Skyhawk
k
Security
Taps
Chat

GPT to Augment Threat
Detection



The
Chasm
Between
n
Cybers

Security Confidence and
Actual Ability



ChatGP
T Less
Convinc
ing
Than

Human Social Engineers in
Phishing Attacks

Security Humor »

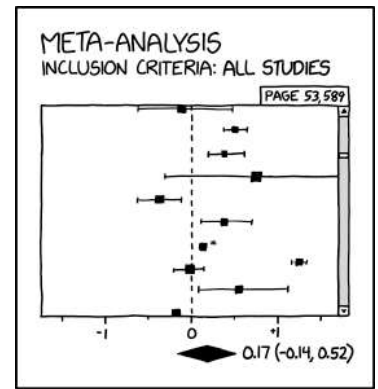
- Infocyte Announces Click-to-Remediate Enabling Remote and Distributed Workforces to Operate More Safely



More from Virginia Satrom

*** This is a Security Bloggers Network syndicated blog from Blog – Infocyte authored by Virginia Satrom. Read the original post at: <https://www.infocyte.com/blog/2020/09/02/cobalt-strike-the-new-favorite-among-thieves/>

📌 Blog, case-study, Cobalt Strike, Cyber Security, Cybersecurity, research, use case



BAD NEWS: THEY FINALLY DID A META-ANALYSIS OF ALL OF SCIENCE, AND IT TURNS OUT IT'S NOT SIGNIFICANT.

Randall Munroe's XKCD 'Effect Size'

← Akamai, CISA, and CIS Join Forces to Improve SLTT Cyber Defenses

Parsing NY-DFS' First Cybersecurity Case →

Join the Community

Add your blog to Security Bloggers Network

Write for Security Boulevard

Bloggers Meetup and Awards

Ask a Question

Email: info@securityboulevard.com

Useful Links

About

Media Kit

Sponsor Info

Copyright

TOS

DMCA Compliance Statement

Privacy Policy

Related Sites

Techstrong Group

Container Journal

DevOps.com

Digital CxO

Techstrong Research

Techstrong TV

Techstrong.tv Podcast

DevOps Chat

DevOps Dozen

DevOps TV






Copyright © 2023 Techstrong Group Inc. All rights reserved.

EXHIBIT 8

If you purchase via links on our site, we may receive **affiliate commissions**.

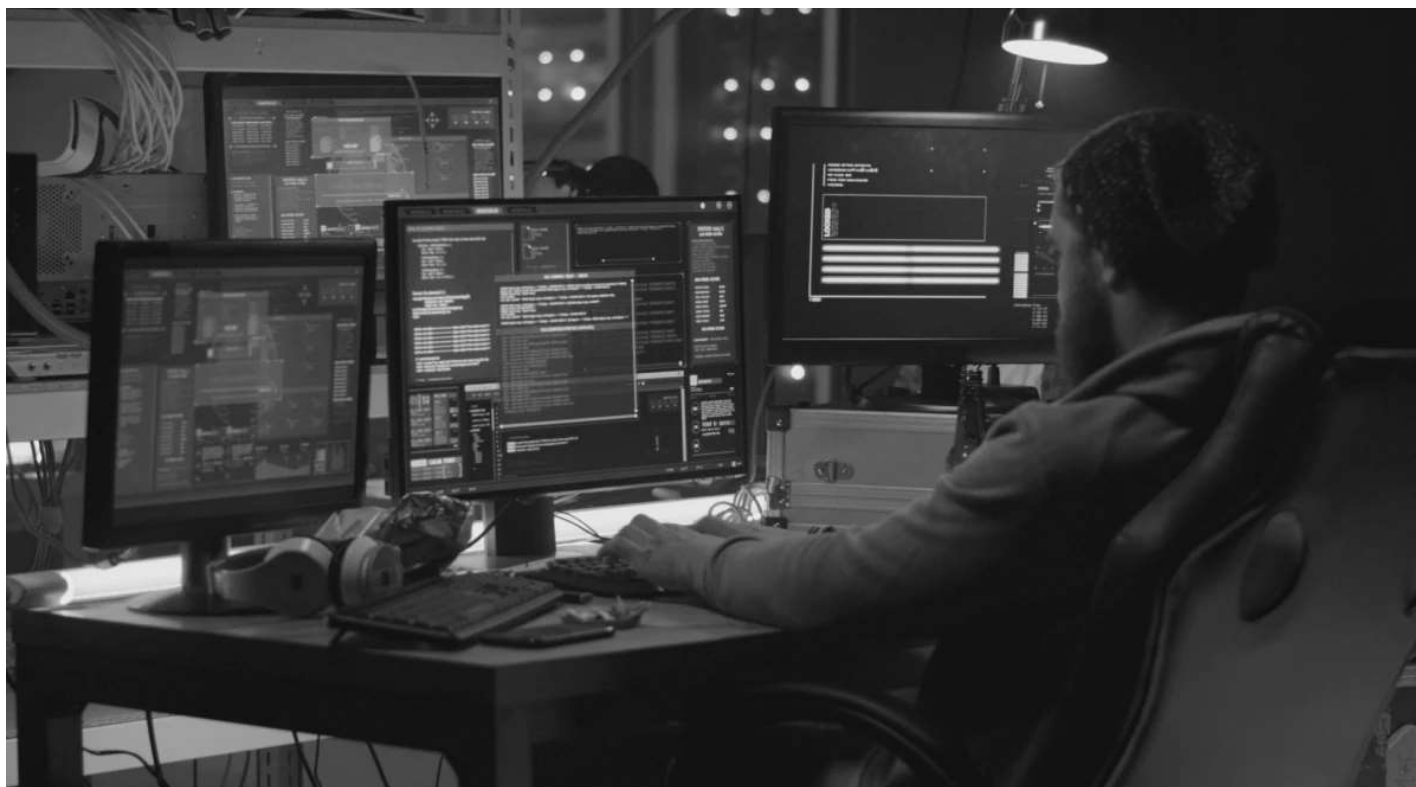
[Home](#) » [Editorial](#)

Cobalt Strike may be a double-edged sword but pentesting tools are invaluable, says expert

Updated on: 02 March 2023 



Damien Black, Senior Journalist



By Shutterstock



This website uses cookies. By continuing to use this website you are giving consent to cookies being used. Visit our [Privacy Policy](#) .

I Agree

criminals, staging an assault on a client company's defenses, with their permission, to assess their strengths and weaknesses.

To do this they have to simulate a cyberattack, sniffing around an organization's setup to probe it for blindspots a genuine criminal might use. To help the "white-hat hackers" do this, many useful tools have been developed – such as Cobalt Strike, designed by cybersecurity tech wiz Raphael Mudge in 2012, or BloodHound, an open-source tool readily available on the developer platform GitHub.

Unfortunately, just as many reports have surfaced in recent years of threat actors picking up these weapons and turning them against the 'good guys.' Perhaps the most notorious example of this was the [SolarWinds](#) hack, which reportedly involved the use of [Cobalt Strike](#).

So, are these red team pentester tools doing more harm than good? To find out more, I reached out to Greg Hatcher, the founder of cybersecurity firm White Knight Labs who cut his teeth working for the US military's Special Forces.

While Hatcher acknowledges that such tools can constitute a "double-edged sword," he still believes they are worth keeping around for the inevitable showdown with ransom-hungry crooks online. In this exclusive Cybernews interview, he explains why.

Cobalt Strike, Metasploit, BloodHound, sqlmap, Burp Suite, and Nmap are the names I've heard mentioned of pentester tools that are popular with threat actors. Are these tools worth it, and of the ones I've named are there any you would say are better or worse in this regard?

So for starters, I think BloodHound is an incredible tool for finding misconfigurations in Active Directory [a tool that allows for comprehensive management of computing systems and their users]. It's used by attackers and defenders just as much, so I would not say that it is a tool that should be shut down due to illicit purposes. Burp Suite is pretty much the number-one web application security-testing commercial software on the planet, so that's definitely a good tool.

Is it going to be used by threat actors that are trying to do attacks against web and mobile applications? Absolutely. But it's sort of like a knife, right? Whoever is holding the knife is going to be the one that decides whether they're going to use it for good intent or bad.

"Because it is so heavily used, default Cobalt Strike out of the box without modification is heavily signatored. Script kiddles [...] trying to use it [...] they're getting caught quickly."

Greg Hatcher, founder of White Knight Labs

[designed by Mudge to help cybersecurity professionals use Metasploit] as a paid-for tool, and now it's extremely cost-prohibitive, I think about \$6,000 for one license. The thing is, because it is so heavily used, default Cobalt Strike out of the box without modification is heavily signed. So you have these attackers that are script kiddies: they're trying to use it out of the box, and they're getting caught quickly.

But that being said, it's still in the hands of people that know what they're doing. You have apex predators that are software developers that can actually write custom loaders, and get around a lot of your products. So Cobalt Strike is more of a double-edged sword, whereas all the other tools that you mentioned are definitely OK to be in the hands of everybody, in my opinion.

I saw research from a few years ago that suggested the most common open-source tools adopted by criminals were memory-injection libraries and remote-access Trojans (RATs). Is that still the case, or has the trend shifted?

Once you actually have an implant at a Windows machine – the vast majority of enterprise environments are comprised of Windows machines – you may actually need a remote access tool to get some kind of functionality, whether you want to dump credentials out of memory or create some kind of process injection.

But you need to set persistence, so you can't just have a dumb tool: you need a fully functioning implant. I would say that has not changed whatsoever, that RATs are definitely still highly available, open-source, some of the top ones on the market. Cobalt Strike is not free, it's very much a paid-for tool, but we've had very good luck with Mythic, which you can just go to GitHub and download. Another good one, Sliver by Bishop Fox [designed as an alternative to Cobalt Strike] is an excellent tool, which has a fully functioning implant.

The other one we were talking about was memory or process injection and, yes, that is still very common today. There actually was a new process-injection technique released at Black Hat [hacker conference] last year called Dirty Vanity. So it's still very much an area of research and it really depends who is using the tool. Mythic, Havoc, Sliver, these are all command-and-control (C2) frameworks that can be used by red teamers, penetration testers, or criminals – because anyone can go to GitHub and pull them down. So like I said before, it really depends on the intent.

Going back to what's been reported previously, is it still the case that cybercriminals are stripping code from pentesting tools and incorporating it in their own malware?

on red team engagements. It's a huge timesaver.

Who do you see dual-purposing tools the most, is it mainly state-backed groups or is it more towards the script-kiddie end, or both?

We see a lot of illicit use coming out of China, but it really is all over the place. Even a criminal organization could just set up a shell company and purchase Cobalt Strike. There are certain export laws that forger has to follow when selling Cobalt Strike, but those can be subverted either way. So it really is everybody across the board, even for the white-hat hackers. The biggest barrier to entry is going to be the cost. It's kind of unfortunate: the black-hat hackers have the money, the white-hat hackers don't sometimes.

"There's a lot of things I learned in Special Forces, like contingency planning, that I implement in cybersecurity."

Greg Hatcher, founder of White Knight Labs

Has the reverse ever happened? I mean a threat group coming up with a tool that the white-hat guys look at and say, 'Oh, that's quite useful. We can use that in our own red teaming exercises.'

Not so much. A lot of it is ransomware, and there's free and open source. For instance, White Knight Labs does a ransomware simulation, but we're not going to go use Emotet ransomware. We have our own ransomware that we wrote by hand, we know exactly what it's doing. That being said, if you're going to do an adversarial emulation for a client, you do have to emulate those types of criminal or that advanced persistent threat (APT). It's more emulating TTPs [techniques, tactics and procedures] as opposed to using the exact same code. Sometimes criminals and APTs, they'll write their own C2 frameworks, which you'll never have access to.

You have a military background with Special Forces. Does that alter your perspective of the cyber landscape, in terms of digital weapons being used and counter-used? Because in the military sphere, that's probably something you see daily.

For the most part, the everyday American citizen underestimates the threat. There's a lot of things that I learned in Special Forces, like contingency planning, that I implement in cybersecurity. So if one attack doesn't work, I'll have something else ready to go. I'll have a primary means of entry, an alternate, and a contingent. But I have found most people in the private sector don't actually think like that.

authentication] for critical accounts, long passwords, updating your operating system whenever patches come out, those can take you really far and put you ahead of the curve – because an attacker, if they're lazy and you're a hard target, is just going to go around you to an easier one.

How much do developments in areas such as artificial intelligence, machine learning, and quantum computing worry you going forward, in terms of how they impact the toolkits that are available to both the 'good' and 'bad' guys? Is that something you give a lot of thought to?

Absolutely. At White Knight Labs we use ChatGPT: we have the paid-for chatbot, just because it really helps with report-writing. I think our AI is going to lower the barrier to entry for writing malware. We've already seen this.

It's not good at writing software right now: if you go on YouTube and look at the videos and Chat trying to write code, it's pretty terrible actually. But that being said, GPT is in its infancy, right? Because they worked for seven years in darkrooms to make this thing: this is just the beginning. Who knows how fast this thing is going to learn and where it is going to be in two to three years: to be able to write undetectable malware, or find a kernel of vulnerability in the Windows operating system. It's definitely an area where it's going to be able to learn faster than any human being, that's for sure.



[Cobalt Strike malware cannot be stopped with a single line of defense, analyst warns](#)

[Signal to pull out of UK ahead of digital bill](#)

[Twitter was down after layoffs](#)

[Netflix digs in: don't force us to skimp on content](#)

[Don't get fooled by Russian propaganda, Ukraine warns journalists](#)

Subscribe to our [newsletter](#)



Editor's choice

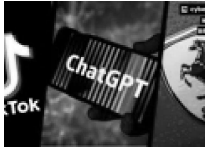


TECH

Lush takes stand against Google – what does this mean for Big Tech?

by Neil C. Hughes ⌚ 27 March 2023

The cosmetics brand recently revealed its Super Mario-themed bath bombs – while dropping truth bombs about Big Tech with the declaration that it would slash Google Ads spending by millions



Cybernews weekly briefing: more crazy innovations as the tech war rages

🕒 24 March 2023



A million at risk from user data leak at Korean beauty platform

🕒 23 March 2023

Lionsgate streaming platform with 37m subscribers leaks user data

🕒 21 March 2023

TikTok showdown with White House showcases Chinese-owned app's controversial history

🕒 23 March 2023

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Email *

Privacy Policy Agreement *

I agree to the [Terms & Conditions](#) and [Privacy Policy](#).

Post comment

CATEGORIES

- News
- Editorial
- Security
- Privacy
- Crypto
- Cloud
- Tech

REVIEWS

- Antivirus Software
- Password Managers
- Best VPNs
- Best VPN for iPhone
- Secure Email Providers
- Website Builders
- Best Web Hosting Services

TOOLS

- Password generator
- Personal data leak checker
- Password leak checker
- Website security checker
- VPN speed test
- Coupon codes

ENGAGE

- About Us
- Send Us a Tip
- Careers



[About Us](#) [Contact](#) [Send Us a Tip](#) [Privacy Policy](#) [Terms & Conditions](#) [Vulnerability Disclosure](#)

© 2023 Cybernews – Latest Cybersecurity and Tech News, Research & Analysis.

EXHIBIT 9

Healthcare , Industry Specific , Next-Generation Technologies & Secure Development

Feds Warn Healthcare Over Cobalt Strike Infections

Red-Teaming Tool Poses Ongoing Risks When Used by Hackers, HHS Warns

Marianne Kolbasuk McGee (HealthInfoSec) • October 10, 2022

The Department of Health and Human Services' Office of Information Security's HC3 unit says attackers are weaponizing legitimate security tools.

If every second hack seems to involve malicious use of penetration testing tool Cobalt Strike, it's not just your imagination.

See Also: LIVE Webinar | Stop, Drop (a Table) & Roll: An SQL Highlight Discussion

Russian hackers deployed Cobalt Strike's command-and-control function during their attack against SolarWinds' network management software. Hackers who earlier this year got into Cisco corporate IT infrastructure used the tool. The first thing the threat actor behind the Emotet malware does after an initial infection is to download Cobalt Strike onto compromised endpoints.

The number of organizations affected by a hack involving Cobalt Strike now number in the tens of thousands each year, says the Department of Health and Human Services in a new warning to the healthcare sector.

The Conti ransomware group values access to Cobalt Strike so much that it paid a legitimate company \$30,000 to secretly buy licenses for it, cybersecurity reporter Brian Krebs wrote in March.

The red-teaming application - licenses for which currently run nearly \$6,000 per user - wasn't designed for hackers and malicious activity isn't its purpose (see: *Attackers Increasingly Using Cobalt Strike*).

Our website uses cookies. Cookies enable us to provide the best experience possible and help us understand how visitors use our website. By browsing bankinfosecurity.com, you agree to our [page of cookies](#).



The company did not immediately respond to Information Security Media Group's request for comment, but its popularity among hackers is no secret. "Its built-in capabilities enable it to be quickly deployed and operationalized regardless of actor sophistication or access to human or financial resources," said cybersecurity company Proofpoint in a 2021 report.

The penetration testing tool, whose legitimate user base consists of white hat hackers, is being abused "with increasing frequency" against many industries, including the healthcare and public health sector, by ransomware operators and various advanced persistent threat groups, HC3 writes.

"Cobalt Strike is used maliciously by several state-sponsored actors and cybercriminal groups, many of whom pose a significant threat to the health sector," the threat brief says.

Among the governments that the HHS's Health Sector Cybersecurity Coordination Center lists as likely making use of Cobalt Strike for state-sponsored hacking are China, Russia, Iran and Vietnam.

Companies aren't helpless, says Sherrod DeGrippo, vice president of threat research and detection at Proofpoint.

Cobalt Strike and similar tools are "noisy" within an environment and can be detected by security tools such as anti-malware and intrusion prevention/detection systems, DeGrippo tells ISMG.

Detection should lead to quick action, says Keith Fricke, principal consultant at privacy and security consultancy tw-Security.

Cobalt Strike and other red-teaming tools are "'legitimate' in the sense that they can be used by red teamers, but are offensive security tools," he says.

Should defenders spot them, "they should be very concerned as they are not used for legitimate business purposes outside of security testing."

HHS HC3 recommends entities reduce their attack surfaces against common infection vectors such as phishing, known vulnerabilities and remote access capabilities.

Our website uses cookies. Cookies enable us to provide the best experience possible and help us understand how visitors use our website. By browsing bankinfosecurity.com, you agree to our use of cookies.

About the Author



Marianne Kolbasuk McGee

Executive Editor, HealthcareInfoSecurity, ISMG

McGee is executive editor of Information Security Media Group's HealthcareInfoSecurity.com media site. She has about 30 years of IT journalism experience, with a focus on healthcare information technology issues for more than 15 years. Before joining ISMG in 2012, she was a reporter at InformationWeek magazine and news site and played a lead role in the launch of InformationWeek's healthcare IT media site.

© 2023 Information Security Media Group, Corp.

<https://www.bankinfosecurity.com/>

Toll Free: (800) 944-0401



Our website uses cookies. Cookies enable us to provide the best experience possible and help us understand how visitors use our website. By browsing [bankinfosecurity.com](https://www.bankinfosecurity.com/), you agree to our use of cookies.

EXHIBIT 10

Home / Tech / Security

Ukrainian organizations warned of hacking attempts using CredoMap malware, Cobalt Strike beacons

Russian hackers continue their attempts to break into the systems of Ukrainian organisations, this time with phishing and fake emails.



Written by **Charlie Osborne**, Contributing Writer on June 22, 2022





Image: Getty

Ukrainian organizations have been subjected to new hacking attempts tailored to drop malware and malicious Cobalt Strike beacons onto their networks.

On June 20, the Computer Emergency Response Team for Ukraine (CERT-UA) published two advisories on the hacking incidents, suspected of being the work of threat groups APT28 -- also known as Fancy Bear -- and UAC-0098.

/ security

Cyber security 101: Protect your privacy from hackers, spies, and the government

Simple steps can make the difference between losing your online accounts or maintaining what is now a precious commodity: Your privacy.

Read now →

The phishing campaign, conducted by Russian advanced persistent threat (APT) APT28, sees it attempting to spread a malicious document titled, "Nuclear Terrorism A Very Real Threat". Distribution is suspected of being carried out on June 10.

SEE: Ransomware attacks: This is the data that cyber criminals really want to steal

UAC-0098's hacking attempts also begins with a malicious email. The phishing messages have a malware document attached, "Imposition of penalties.docx," and its distribution has been described as "persistent" with an original compilation date of June 16.

This document is also spread through a password-protected archive, fraudulently passed off as communication from Ukraine's tax office, with the subject line: "Notice of non-payment of tax."

When opened, both documents automatically download an HTML file that initiates malicious JavaScript code containing an exploit [for CVE-2022-30190](#).

Issued a CVSS severity score of 7.8, [CVE-2022-30190](#) is a remote code execution (RCE) vulnerability in the Microsoft Windows Support Diagnostic Tool (MSDT). The vulnerability, patched but exploited in the wild, [first emerged](#) as a zero-day flaw in May.

If the target system has not been protected, victims of Fancy Bear's attacks will find their systems infected with the CredoMap malware.

According to [Malwarebytes](#), CredoMap is an information stealer able to exfiltrate browser data, cookies, and account credentials. Older variants of the malware have previously [been used](#) by APT28 against Ukrainian targets.

The tax-related doc, however, deploys Cobalt Strike beacons. [Cobalt Strike](#) is a legitimate, commercial penetration-testing tool that has, unfortunately, been abused for malicious purposes by cyber attackers for many years. The tool's beacon functionality can facilitate remote connections and can be used for the deployment of shellcode and malware.

Since Russia's invasion of Ukraine began, CERT-UA has pivoted its focus to warning against cyber threats impacting both Ukrainian businesses and residents. Many campaigns are trying to take advantage of the situation, whether on behalf of the Russian state or just as run-of-the-mill attackers trying to make a profit.

[SEE: Cloud computing security: Five things you are probably doing wrong](#)

The agency has previously warned organizations of [Ghostwriter](#) phishing campaigns, [Invisimole activities](#) tied to the Russian APT Gamaredon, and frequent [misinformation schemes](#) targeting Ukraine's residents.

CERT-UA has also alerted Ukrainian media agencies to phishing campaigns, potentially conducted by the Russian Sandworm hacking group, intended to spread the CrescentImp malware.

Previous and related coverage

- [Ukraine security agencies warn of Ghostwriter threat activity, phishing campaigns](#)
- [Ukraine warns of InvisiMole attacks tied to state-sponsored Russian hackers](#)
- [Cyberattacks and misinformation activity against Ukraine continues say security researchers](#)

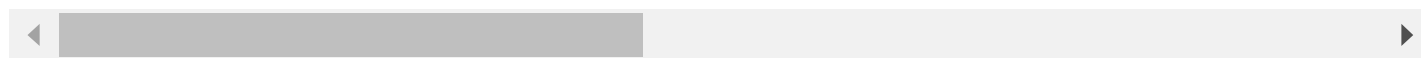
Have a tip? Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0

/ security

These experts are racing to protect AI from hackers. Time is running out

Fraudsters are using machine learning to help write scam emails in different languages

How to 1 your ph



 **Editorial standards**

show comments ↓

we equip you to harness the power of disruptive innovation, at work and at home.

topics

galleries

videos

do not sell or share my personal information

about ZDNET

meet the team

sitemap

reprint policy

join | log in

newsletters

site assistance

licensing

© 2023 ZDNET, A Red Ventures company. All rights reserved. [Privacy Policy](#) | [Cookie Settings](#) | [Advertise](#) | [Terms of Use](#)

EXHIBIT 11

Google Identifies 34 Cracked Versions of Popular Cobalt Strike Hacking Toolkit in the Wild

📅 Nov 21, 2022 👤 Ravie Lakshmanan



Google Cloud last week disclosed that it identified 34 different hacked release versions of the Cobalt Strike tool in the wild, the earliest of which shipped in November 2012.

The versions, spanning 1.44 to 4.7, add up to a total of 275 unique JAR files, according to findings from the Google Cloud Threat Intelligence (GCTI) team. The latest version of Cobalt Strike is version 4.7.2.

Cobalt Strike, developed by Fortra (née HelpSystems), is a popular adversarial framework used by red teams to simulate attack scenarios and test the resilience of their cyber defenses.

It comprises a Team Server that acts as the command-and-control (C2) hub to remotely commandeer infected devices and a stager that's designed to deliver a next-stage payload called the Beacon, a fully-featured implant that reports back to the C2 server.

Given its wide-ranging suite of features, unauthorized versions of the software have been increasingly weaponized by many a threat actor to advance their post-exploitation activities.

"While the intention of Cobalt Strike is to emulate a real cyber threat, malicious actors have latched on to its capabilities, and use it as a robust tool for lateral movement in their victim's network as part of their second-stage attack payload," Greg Sinclair, a reverse engineer at Google's Chronicle subsidiary, said.

In a bid to tackle this abuse, GCTI has released a set of open source YARA Rules to flag different variants of the software used by malicious hacking groups.

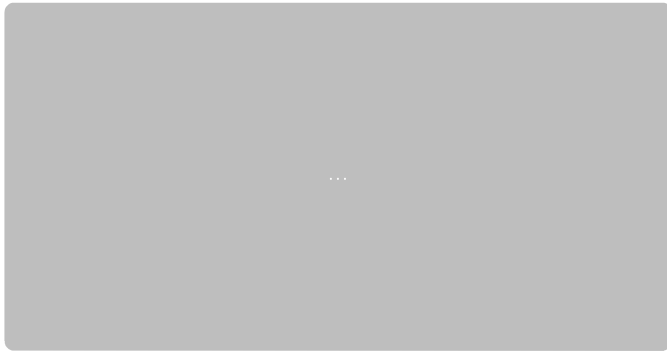
The idea is to "excise the bad versions while leaving the legitimate ones untouched," Sinclair said, adding "our intention is to move the tool back to the domain of legitimate red teams and make it harder for bad guys to abuse."

Found this article interesting? Follow us on Twitter  and LinkedIn to read more exclusive content we post.

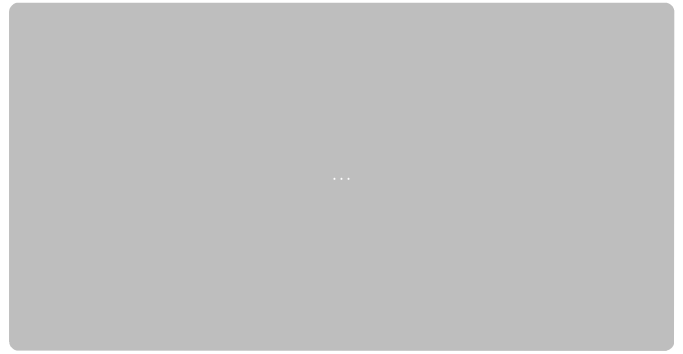
 Tweet  Share  Share

Breaking News

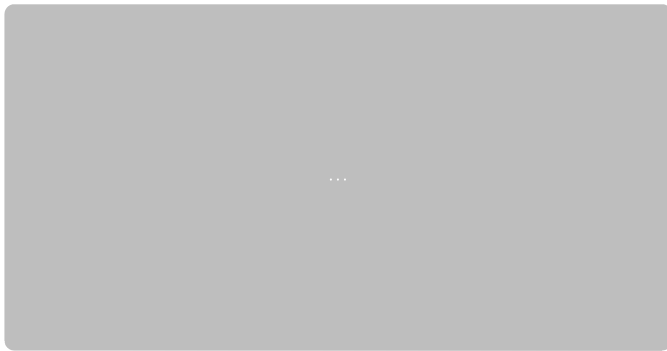
Cybersecurity Resources



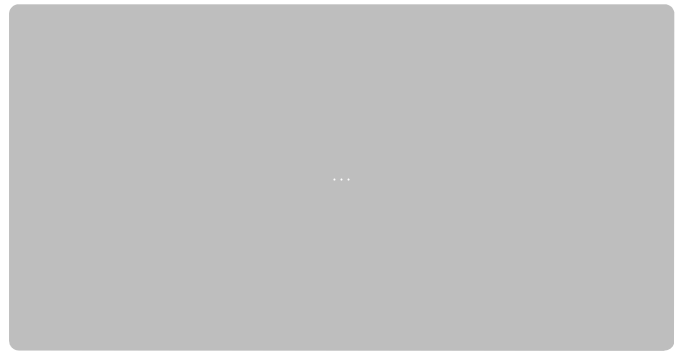
Save Time on Network Security With This Guide



Watch This to Learn How to Safeguard Against 3rd-Party SaaS App Breaches



eBook: 4 Steps To Comprehensive Service Account Security



A to Z Cybersecurity Certification Courses

Join 100,000+ Professionals

Sign up for free and start receiving your daily dose of cybersecurity news, insights and tips.

Your e-mail address

Connect with us!



Company

[About THN](#)

[Advertise with us](#)

[Contact](#)

Pages

[Deals Store](#)

[Privacy Policy](#)

[Jobs](#)



[Contact Us](#)

© The Hacker News, 2023. All Rights Reserved.