Сведения об авторах

Абусаид Манап* – магистрант, Astana IT University; Республика Казахстан, Астана; e-mail: abusaid.manap@gmail.com. ORCID: https://orcid.org/0009-0001-5353-4052

Гульнара Аскеровна Абитова – кандидат технических наук, доцент; Astana IT University; Республика Казахстан, Астана; e-mail: gulya.abitova@gmail.com. ORCID: https://orcid.org/0000-0003-3830-6905

Material received on 17.11.2023 г.

DOI: 10.53360/2788-7995-2023-4(12)-7

МРНТИ: 81.93.29

A.K. Shaikhanova, D.S. Kadyrov*
L.N. Gumilyov Eurasian National University,
010000, Republic of Kazakhstan, Astana, Satpayev Str., 2
*e-mail: 010422551083@enu.kz

A DEEP DIVE INTO COBALT STRIKE TOOL

Annotation: *Cobalt Strike is a popular commercial penetration testing tool that has also been widely used in cyber attacks. This paper provides a review of the Cobalt Strike and its use in cyber attacks, including an analysis of the tactics, techniques, and trends associated with its use. Conducted a literature review and data analysis of academic research, industry reports, and news articles on Cobalt Strike and its use in cyber attacks, as well as case studies of specific attacks involving Cobalt Strike. This research is based on cases in which Cobalt Strike has been used in a wide range of attacks: ransomware attacks, espionage campaigns, and advanced persistent threats. Attackers using Cobalt Strike tend to be highly sophisticated and motivated by a range of factors, including financial gain, political espionage, and cyber warfare. The tool's flexibility and adaptability make it a formidable threat to organizations seeking to defend against cyber attacks. Our research highlights key features and explains thoroughly the logical structure of the Cobalt Strike.*

Key words**:** *Command and Control (C2), penetration testing, post-exploitation, Cobalt Strike, network*

Introduction

In recent years the Cobalt Strike has been gaining significant recognition in the cybersecurity field as a highly valuable penetration testing tool. It is already considered the "swiss knife" of every red team engagement. While the tool was originally designed for legitimate security testing purposes, despite the fact that the company has strict criteria for selling its own product, it has also been widely used by threat actors in a variety of malicious activities. As a result, Cobalt Strike has become a major concern for organizations seeking to defend against cyber attacks.

This paper will provide a comprehensive review of the Cobalt Strike and its use in cyber attacks. Drawing on a combination of academic research, industry reports, and news articles, the research analyzes the tactics, techniques, and trends associated with Cobalt Strike-based attacks, and provides insights into the tool's key features and logical structure. Our research is based on a detailed review of the literature, as well as case studies of specific attacks that have used Cobalt Strike. Through this analysis, the main aim is to provide a deeper understanding of the key functionality and advanced options associated with the Cobalt Strike.

Overall, this research sheds light on the evolving threat landscape of cyber-attacks and highlights the need for organizations to develop proactive and resilient cybersecurity strategies. The bottom-up approach in this research the Cobalt Strike and its use by threat actors in different APTs, I hope to make a contribution to enhancing cybersecurity awareness in Command and Control framework aspect and cyberspace sustainability.

Brief history and development of Cobalt Strike

Cobalt Strike is a commercial penetration testing tool that was created and released by Raphael Mudge 2012, the founder of Armitage, another well-known penetration testing tool. Cobalt

Strike was designed to provide advanced capabilities beyond what Armitage offered, specifically focusing on advanced threat emulation, adversary simulation, and post-exploitation. Since its initial release, Cobalt Strike has undergone several updates and improvements to keep up with evolving threat landscapes and attacker techniques.

Key features and functionalities, including its intended use for penetration testing and its commercial availability

As described in Sinclair's (2022) article, Cobalt Strike offers a variety of features and functionalities to aid in penetration testing and adversary simulation, including but not limited to:

- Beacon payload for command-and-control (C2) communications
- Social engineering toolkit for crafting phishing emails
- Aggressor Script for customizing and automating post-exploitation actions
- Port forwarding and SOCKS proxy for network pivoting
- Integration with Metasploit Framework

While Cobalt Strike was initially developed for legitimate use in penetration testing, it is now also widely available commercially, and its use has expanded to include malicious activities such as ransomware attacks, espionage campaigns, and advanced persistent threats.

Differences between legitimate and malicious use of Cobalt Strike

The legitimate use of Cobalt Strike involves using the tool to identify vulnerabilities and improve an organization's security posture. "Cobalt Strike is a powerful and flexible tool that is designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors" (Help Systems, 2022, para. 1). On the other hand, malicious use of Cobalt Strike involves using the tool to compromise systems and steal data. Attackers can use Cobalt Strike to gain persistent access to a compromised network, exfiltrate data, or deploy ransomware.

One key difference between the legitimate and malicious use of Cobalt Strike is the presence of authorization and consent. Legitimate users of the tool obtain authorization from the organization being tested and follow a strict set of rules and guidelines. Malicious actors, on the other hand, use Cobalt Strike without authorization and for malicious purposes. It's important to note that while the tool itself is not inherently malicious, its misuse can have devastating consequences for targeted organizations.

Cobalt Strike-based attacks

Cobalt Strike has become a popular tool among cybercriminals for carrying out a wide range of attacks, including ransomware attacks, espionage campaigns, and advanced persistent threats (APTs). In ransomware attacks, attackers have been observed using Cobalt Strike to deploy the initial payload and establish a foothold in the victim's network before deploying the ransomware. This tactic allows attackers to bypass some of the victim's security measures and gain a deeper foothold in the network, enabling them to encrypt more files and demand a higher ransom.

In addition to ransomware attacks, Cobalt Strike has also been used in various espionage campaigns, including those carried out by nation-state-sponsored threat actors. Hinchliffe (2019) reported that a Chinese cyber espionage group known as PKPLUG utilized Cobalt Strike to deliver a complex malware strain in Operation Iron Tiger, which targeted victims in Southeast Asia. The malware was designed to steal sensitive information from the victims' networks and send it back to the attackers' command and control (C2) server.

APTs also commonly use Cobalt Strike in their attacks, often as a means of establishing a persistent presence on the victim's network. In the 2020 SolarWinds attack, for example, the attackers used Cobalt Strike to deliver a malware strain known as SUNBURST to their targets, as reported by CFCS (2021). The malware was designed to evade detection and establish a backdoor on the victim's network, allowing the attackers to maintain access and steal sensitive data over an extended period of time.

Comparative analysis of Cobalt Strike with open-source project

One significant drawback of Cobalt Strike lies in its susceptibility to detection by scanning mechanisms. As cybersecurity defenses continue to evolve, so too do the techniques employed by malicious actors and penetration testers alike. The inherent challenge arises from the distinct footprint that Cobalt Strike may leave behind during its operations, thereby making it susceptible to detection by advanced scanning tools.

In practical terms, security solutions have become adept at recognizing the behavioral patterns and characteristics associated with Cobalt Strike's activities. This heightened sensitivity may result in the premature identification of the tool, diminishing its efficacy in simulating real-world cyber threats. To address this concern, users are often compelled to employ additional measures, such as hiding behind proxies, to obfuscate the tool's presence and maintain its stealth capabilities.

Moreover, the need to employ such countermeasures introduces an additional layer of complexity to penetration testing activities, potentially impacting the tool's user-friendliness and accessibility. As organizations invest heavily in enhancing their threat detection capabilities, the cat-and-mouse game between security professionals and evolving scanning mechanisms continues to pose challenges for the sustained effectiveness of Cobalt Strike.

Another noteworthy limitation pertains to the financial implications associated with the acquisition of Cobalt Strike. Positioned as a commercial tool, Cobalt Strike comes with a considerable price tag, rendering it inaccessible to individuals and smaller organizations with limited budgets. The exorbitant cost of licensing may present a barrier for those seeking to leverage the tool for penetration testing purposes, potentially hindering the democratization of advanced cybersecurity capabilities.

Fortra, the company behind Cobalt Strike, maintains a stringent sales policy, limiting the availability of the tool to a select clientele. This exclusivity exacerbates the financial burden, as Fortra does not sell the product to anyone willing to purchase it. The restrictive nature of this sales approach may impede the diverse adoption of Cobalt Strike within the cybersecurity community, constraining the accessibility of a valuable tool for enhancing the security posture of diverse entities.

One standout advantage of the alternative penetration testing tool is its cost-effectiveness, setting it apart from premium, commercially available solutions like Cobalt Strike. Unlike the prohibitive pricing structures associated with some industry-leading tools, this alternative is freely available, making it an attractive option for individuals, small businesses, and cybersecurity enthusiasts operating within budget constraints.

The tool's open-source nature not only democratizes access to advanced cybersecurity capabilities but also fosters a more inclusive cybersecurity community. By eliminating financial barriers, it empowers a broader spectrum of users to engage in ethical hacking practices, contributing to the collective improvement of cybersecurity standards across various domains.

Stealth and Evasion of Recognizable Signatures:

In contrast to tools that may be easily detected by scanning mechanisms and signature-based defenses, the alternative penetration testing tool excels in maintaining a low profile during simulated cyber-attacks. Recognizing the evolving landscape of cybersecurity defenses, the tool is designed to evade detection by leveraging sophisticated evasion techniques and avoiding recognizable signatures.

The tool's developers prioritize staying ahead of detection mechanisms by regularly updating and refining its evasion capabilities. This commitment to continuous improvement ensures that the tool remains effective in emulating real-world cyber threats without triggering alarms within the target environment. As a result, security professionals can confidently deploy the tool in diverse scenarios, enhancing its utility for penetration testing activities.

As depicted in figure 1, in a comprehensive penetration testing framework, a plugin system facilitates extensibility through dynamically loadable modules. These plugins, created by users or the community, augment the tool's functionalities. A logging module captures and records pertinent events, providing a detailed audit trail for transparency and troubleshooting. An encryption module ensures secure communication between the command and control server and compromised systems, leveraging robust encryption algorithms and effective key management. The client interface, whether graphical or command-line, serves as the user's gateway to interact with the tool, executing commands and managing sessions seamlessly. The command and control server orchestrates communication, issuing commands to compromised systems and receiving their responses. Attack packages, comprising payload and post-exploitation modules, offer a diverse set of tools for simulating real-world cyber threats. The beacon payload, designed for stealth, maintains a low profile by evading recognizable signatures during communication. A listener component on the server side awaits incoming connections, establishing and managing sessions with compromised systems. Finally, a data exfiltration module enables the secure transfer of sensitive information from compromised systems to the operator-controlled infrastructure, completing the toolkit for comprehensive penetration testing activities.

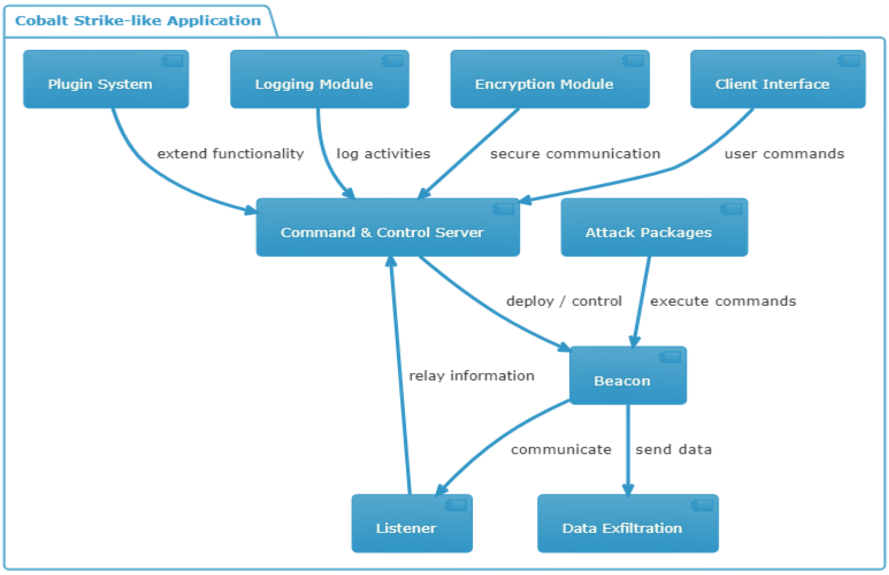

Figure 1 – Architecture of the developed application

Defense strategies

Cobalt Strike-based attacks are sophisticated and can be difficult to detect and prevent. In this section, we discuss several defense strategies that can help organizations protect against such attacks.

Technical controls are a critical part of an organization's defense against Cobalt Strike-based attacks. According to Sangvikar et al. (2022), intrusion detection and prevention systems can be used to detect and prevent attacks in real-time, while network segmentation can limit the potential impact of an attack. Regular patch management can also help to prevent known vulnerabilities from being exploited.

Organizational policies and procedures are also an essential defense against Cobalt Strike-based attacks. A culture of security can be fostered through security awareness training, which can help employees understand the risks and threats associated with the tool. Kruse and Heiser (2001) emphasize the importance of incident response plans in enabling organizations to respond promptly and efficiently to a security breach, thereby minimizing the potential impact on their operations. Vulnerability management, which involves regular assessments of an organization's infrastructure and systems, can help identify and address potential vulnerabilities before they are exploited.

User awareness and training are also critical components of a defense strategy against Cobalt Strike-based attacks. Dark, Epstein, Morales, Countermine, and Ali (2006) recommend that employees should receive education on identifying and reporting suspicious activity and being aware of the appropriate actions to take in the event of a security incident. This can include regular training sessions, simulated phishing attacks, and ongoing communication about the latest threats and trends. By promoting a culture of security and involving employees in the defense strategy, organizations can better protect themselves against Cobalt Strike-based attacks.

Future trends and research directions

As the threat of Cobalt Strike-based attacks continues to evolve, it is essential for organizations to stay abreast of emerging technologies and research in this area. This section discusses some potential future trends and research directions:

1. Emerging technologies and techniques for detecting and preventing Cobalt Strike-based attacks: With the increasing sophistication of attackers, new technologies and techniques are being developed to detect and prevent Cobalt Strike-based attacks. As investigated by Raghav, Mahmood, and Hasan (2011), artificial intelligence can be utilized to analyze network traffic and detect anomalous behavior that may indicate a security breach.

2. The evolving threat landscape: The threat landscape is constantly evolving, with new tactics, techniques, and procedures (TTPs) being developed by attackers. It is important for organizations to stay current with new developments in Cobalt Strike-based attacks to ensure their defense strategies remain effective.

3. Potential areas for future research: There are several potential areas for future research, including the effectiveness of defense strategies against Cobalt Strike-based attacks and the motivations and capabilities of attackers using Cobalt Strike. Additionally, as new developments arise, research into emerging technologies and their effectiveness in defending against Cobalt Strike-based attacks may be needed.

Conclusion

In conclusion, Cobalt Strike is a versatile and powerful penetration testing tool that has also become a popular choice for malicious actors in cyber attacks. Our research has provided an overview of the tool's history, key features and functionalities, and differences between legitimate and malicious use. We have also analyzed specific examples of how Cobalt Strike has been used in ransomware attacks, espionage campaigns, and advanced persistent threats.

To defend against Cobalt Strike and other red team tools, organizations should implement a wide range of technical controls together, such as intrusion detection and prevention systems, security information, event management, antiviruses, and others. Organizational policies and procedures, including security awareness training, incident response plans, and vulnerability management, can also help create a culture of security. User awareness and training are equally important in recognizing and reporting suspicious activity.

Finally, we have highlighted emerging technologies and techniques for detecting and preventing Cobalt Strike-based attacks, as well as potential areas for future research. As the threat landscape continues to evolve, it is critical for organizations to stay up-to-date with new developments in Cobalt Strike-based attacks and to continually refine their defense strategies. By taking these steps, organizations can better protect themselves and be prepared against the significant amount of risks related to information security

Based on the literature review and data analysis conducted in this research, the problem of Cobalt Strike being used in malicious cyber attacks was investigated. The findings reveal that Cobalt Strike, originally designed for legitimate penetration testing purposes, has been widely used by threat actors in various attacks such as ransomware attacks, espionage campaigns, and advanced persistent threats.

The research also emphasizes the differences between legitimate and malicious use of Cobalt Strike, with legitimate use involving authorization and consent, and malicious use involving unauthorized and malicious activities. The paper also highlighted specific use cases of Cobalt Strike in ransomware attacks and espionage campaigns carried out by nation-state-sponsored threat actors.

References

1. Navarrete C., Sangvikar D. Cobalt strike analysis and tutorial: Identifying beacon team servers in the wild [Электрон. ресурс]. – 2022. – URL: https://unit42.paloaltonetworks.com/cobalt-strike-team-server (дата обращения: 03.11.2023).
2. Hinchliffe A. PKPLUG: Chinese Cyber Espionage Group attacking Southeast Asia [Электрон. ресурс]. – 2019. – URL: https: //unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage _group_attacking_asia (дата обращения: 03.10.2023)
3. Sinclair G. Making cobalt strike harder for threat actors to abuse | google cloud blog [Электронный ресурс]. – 2022. – URL: https://cloud.google.com/blog/products/identity-security/making-cobalt-strike-harder-for-threat-actors-to-abuse (дата обращения: 18.11.2023).
4. CFCS. Investigation report: SolarWinds: State-sponsored global software supply chain attack [Электрон. ресурс]. – 2021 – URL: https://www.cfcs.dk/globalassets/cfcs/dokumenter/rapporter/en/CFCS-solarwinds-report-EN.pdf (дата обращения: 10.04.2023).
5. Fortra. Cobalt Strike User Guide [Электрон ресурс]. – 2023 – URL: https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/welcome_main.htm (дата обращения: 10.09.2023).
6. Dark, M., Epstein, R.A., Morales, L., Countermine, T.A., & Ali, M.Y. (2006). A Framework for Information Security Ethics Education. Center for Research and Education in Information Assurance and Security.
7. Hasan R. и др. Artificial intelligence based model for incident response // 2011 International Conference on Information Management, Innovation Management and Industrial Engineering. – 2011. – С. 91-93.

8. Kruse W.G., Heiser J.G. Computer forensics: Incident response essentials. – Boston: Addison-Wesley, 2008. – 416 с.

А.К. Шайханова, Д.С. Кадыров*
Л.Н. Гумилёв атындағы Еуразия ұлттық университеті,
010000, Қазақстан Республикасы, Астана қаласы, Сәтпаев көшесі, 2
*e-mail: 010422551083@enu.kz

COBALT STRIKE ҚҰРАЛЫН ЕГЖЕЙ-ТЕГЖЕЙЛІ ТАЛДАУ

Cobalt Strike-бұл кибершабуылдарда кеңінен қолданылатын танымал коммерциялық енуді тексеру құралы. Бұл құжатта Cobalt Strike және оның кибершабуылдарда қолданылуы, оның ішінде оны қолданумен байланысты тактика, әдістер мен тенденцияларды талдау туралы шолу берілген. Cobalt Strike және оның кибершабуылдарда қолданылуы туралы академиялық зерттеулердің деректері, салалық есептер мен жаңалықтар мақалалары, сондай-ақ Cobalt Strike көмегімен нақты шабуылдардың жағдайлық зерттеулері туралы әдебиеттерге шолу және талдау жүргізілді. Бұл зерттеу Cobalt Strike әртүрлі шабуылдарда қолданылған жағдайларға негізделген: ransomware шабуылдары, тыңшылық науқандар және күрделі тұрақты қауіптер. Cobalt Strike қолданатын зиянкестер қаржылық пайда, саяси тыңшылық және кибер соғыс сияқты бірқатар факторларға өте талғампаз және ынталы. Бұл құралдың икемділігі мен бейімделгіштігі оны кибершабуылдардан қорғанғысы келетін ұйымдар үшін үлкен қауіпке айналдырады. Біздің зерттеуіміз негізгі ерекшеліктерді бөліп көрсетеді және cobalt Strike логикалық құрылымын егжей-тегжейлі түсіндіреді.

***Түйін сөздер**: Инфраструктура управления и контроля (C2), тестирование на проникновение, пост-эксплуатация, Cobalt Strike, сеть.*

А.К. Шайханова, Д.С. Кадыров*
Евразийский национальный университет имени Л.Н. Гумилева,
010000, Республика Казахстан, г. Астана, ул. Сатбаева, 2
*e-mail: 010422551083@enu.kz

ДЕТАЛЬНЫЙ АНАЛИЗ ИНСТРУМЕНТА COBALT STRIKE

Cobalt Strike – популярный коммерческий инструмент для тестирования на проникновение, который также широко используется в кибератаках. В этом документе представлен обзор Cobalt Strike и его использования в кибератаках, включая анализ тактики, методов и тенденций, связанных с его использованием. Проведен обзор литературы и анализ данных академических исследований, отраслевых отчетов и новостных статей о Cobalt Strike и его использовании в кибератаках, а также тематических исследований конкретных атак с использованием Cobalt Strike. Это исследование основано на случаях, когда Cobalt Strike использовался в самых разных атаках: атаках программ-вымогателей, шпионских кампаниях и сложных постоянных угрозах. Злоумышленники, использующие Cobalt Strike, как правило, очень изощренны и мотивированы рядом факторов, включая финансовую выгоду, политический шпионаж и кибервойну. Гибкость и адаптируемость этого инструмента делают его серьезной угрозой для организаций, стремящихся защититься от кибератак. Наше исследование выделяет ключевые особенности и подробно объясняет логическую структуру Cobalt Strike.

***Ключевые слова**: Инфраструктура управления и контроля (C2), тестирование на проникновение, пост-эксплуатация, Cobalt Strike, сеть.*

Авторлар туралы мәліметтер

Дамир Серикович Кадыров* – 2 курс магистрант; ақпараттық қауіпсіздік мамандығы; Л.Н. Гумилёв атындағы Еуразия ұлттық университеті; Қазақстан Республикасы; e-mail: 010422551083@enu.kz. ORCID: https://orcid.org/0009-0003-5364-9903.

Айгуль Кайрулаевна Шайханова – ақпараттық қауіпсіздік кафедрасының профессор; Л.Н. Гумилёв атындағы Еуразия ұлттық университеті; Қазақстан Республикасы; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Information about the authors

Damir Serikovich Kadyrov* – 2st year master's degree; specialty of information security; Eurasian National University named after L.N. Gumilyov; The Republic of Kazakhstan; e-mail: 010422551083@enu.kz. ORCID: https://orcid.org/0009-0003-5364-9903

Aigul Kairulaevna Shaikhanova – professor of the department of Information Security; Eurasian National University named after L.N. Gumilyov; Republic of Kazakhstan; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813

Сведения об авторах

Дамир Серикович Кадыров* – магистрант 2-го курса; специальность инфорационной безопасности; Евразийский национальный университет имени Л.Н. Гумилева; Республика Казахстан; e-mail: 010422551083@enu.kz. ORCID: https://orcid.org/0009-0003-5364-9903.

Айгуль Кайрулаевна Шайханова – профессор кафедры «Информационной безопасности»; Евразийский национальный университет имени Л.Н. Гумилева; Республика Казахстан; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Material received on 05.12.2023 г.