УДК 004.49
DOI: 10.31673/2409-7292.2023.020002

Хавер А. В.

ПРИНЦИПИ ФУНКЦІОНУВАННЯ ТА ВИЯВЛЕННЯ НА ЦІЛЬОВІЙ СИСТЕМІ ІНСТРУМЕНТУ ПОДВІЙНОГО ПРИЗНАЧЕННЯ COBALT STRIKE

У статті проводиться дослідження природи функціонування інструменту подвійного призначення Cobalt Strike, яке в своєму арсеналі активно використовують APT (Advanced Persistent Threat) перш за все з метою отримання несанкціонованого доступу до інформаційних систем та їх інформаційних активів. Враховуючи масштаби поширення використання Cobalt Strike доцільно розглянути принцип його роботи та можливі заходи з протидії його проникненню в інформаційні системи об'єктів критичної інформаційної інфраструктури.

Ключові слова: програмні інструменти подвійного призначення, шкідливе програмне забезпечення, Cobalt Strike, бокове переміщення.

Вступ

В зв’язку зі змінами в сучасній геополітичній обстановці у світі, загостренням воєнних конфліктів між державами різних воєнно-політичних блоків та враховуючи роль і місце ведення активних наступальних операцій у кіберпросторі, в тому числі в ході військового протистояння між РФ та Україною, загрози щодо кібератак на об’єкти критичної інформаційної інфраструктури нашої держави посилилися та урізноманітнилися. Здебільшого суб’єктами таких загроз виступають хакерські угрупування спонсоровані державою-агресором та її союзниками. Серед них, з метою збору розвідданих, противник найчастіше використовує кібератаки з використанням шкідливого програмного забезпечення (ШПЗ).

Основна частина

За останній рік зросла тенденція до використання хакерськими групами інструментів подвійного призначення для здійснення кібератак через механізми віддаленого доступу. Кібератаки такого типу спрямовані на об’єкти критичної інформаційної інфраструктури (ОКІІ) здійснюються з метою шпигунства, викрадення облікових даних користувачів та подальшої компрометації інформаційних активів. Серед прикладів таких інструментів подвійного призначення можна назвати: Cobalt Strike, Sliver, Nighthawk, Brute Ratel C4, Havak та інші. Використання такого ПЗ з зловмисною метою отримало назву “living-off-the-land” — зловмисної тактики, яка набула значного поширення через її простоту застосування і гнучкість використання.

Ефективним засобом для реалізації етапу “Доставки” (Табл.1) на цільову систему залишається таргетований фішинг. Елементи соціальної інженерії застосовані в електронному повідомлені допомагають зловмисникам досягти поставленої мети цього етапу атаки.

Таблиця 1

Класична послідовність проведення атаки на цільову систему

№з/п	Назва етапу
	Проведення розвідки (Reconnaissance)
	Вибір ефективної тактики для проведення атаки (Weaponization)
	Доставка корисного навантаження (Delivery)
	Експлуатація (Exploitation)
	Установка (Installation)
	Підвищення привілеїв до рівня суперкористувача (Command&Control)
	Здійснення кінцевої мети (Action on Objective)

	Замітання слідів (Clean)

Розглянемо детальніше процес функціонування інструменту подвійного призначення на прикладі ПЗ Cobalt Strike. Cobalt Strike є комерційним ПЗ компанії “Help Systems”, призначене для проведення пентесту та здатне емулювати діяльність зловмисника, зокрема, спрямоване на імітацію тактик, прийомів і процедур суб’єктів загроз для перевірки стійкості цільової системи [1]. Також даний програмний інструмент дозволяє здійснювати такі корисні для проведення атаки функції як обфускацію, для обходу антивірусного програмного забезпечення (АВПЗ) та “бокове переміщення” (“lateral movement”).

Обфускація використовується зловмисниками для уникнення виявлення та аналізу ШПЗ, так як після її виконання початковий код (або виконуваний програмний код) приводиться до вигляду, який зберігає його функціональність, але ускладнює аналіз, розуміння алгоритму роботи, таким чином зберігаючи стійкість перед АВПЗ так як його ефективність в даному випадку є слабкою [2].

Також, “Cobalt Stricke” використовує спосіб обходу АВПЗ використовуючи так званий “безфайловий метод”. Метод базується на взаємодії ШПЗ і цільової системи через оперативну пам’ять. Наприклад, при початковому відвідуванні користувачем шкідливої веб-сторінки ШПЗ використовує вразливість у ПЗ та направляє завантажене ШПЗ в область оперативної пам’яті цільової системи де воно й виконується. Характерною особливістю такого методу є те, що безфайлові атаки не заражають системні файли, проте використовують “PowerShell.exe” або “wmic.exe” для свого виконання.

Техніка “бокового переміщення” дозволяє зловмиснику використовувати різні інструменти і методи для компрометації кількох пов’язаних систем і встановлення контролю над ними. Зазвичай метою використання цієї техніки є підвищення привілеїв в системі та викрадення конфіденційних даних. В “Cobalt Strike’ для “бокового переміщення” використовується протокол SMB. В ході здійснення атак зловмисниками безпосередньо ПЗ Cobalt Strike використовується після етапу експлуатації (Табл.1). Структурно ПЗ Cobalt Strike складається з серверної та клієнтської частини.

На цільову систему, зазвичай, клієнтська частина програми потрапляє через три найбільш поширені шляхи: через шкідливі вкладення в фішингових електронних листах (Рис. 1); через шкідливі посилання в фішингових листах; з завантаженим з відкритих джерел нелінцензійним ПЗ разом з дропером. Для експлуатації ж, зокрема, застосовуються програми дропери, такі як IcedID, ZLoader, Qbot, Ursnif, Hancitor, Bazar і TrickBot та інші.

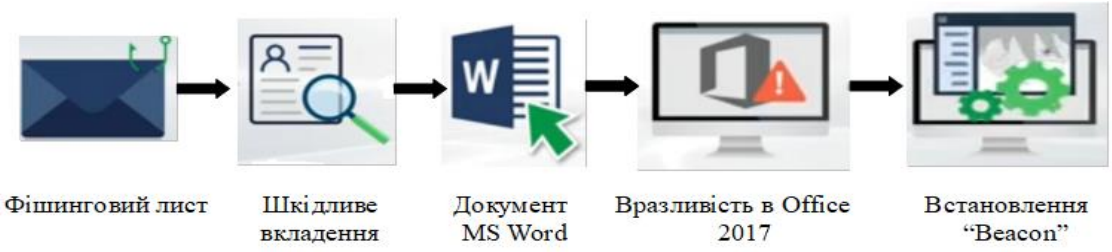

Рис. 1. Алгоритм проникнення Cobalt Strike “Beacon” на цільову систему

Дропер – це різновид троянської програми, яка призначена для “доставки” ШПЗ (вірусів, бекдорів, тощо) на цільову систему. Вони перешкоджають виявленню ШПЗ засобами АВПЗ на етапі завантаження до цільової системи. У більшості випадків дропери не виконують шкідливих функцій. Основна мета дропера — непомітно для користувача та засобів АВПЗ доставити на цільову систему так зване “корисне навантаження”. На відміну від завантажувача, який отримує необхідні компоненти з сервера зловмисників, дропер, зазвичай вже містить їх, проте в окремих випадках може завантажити ШПЗ вже після активації.

Найчастіше дропери маскуються під ПЗ, яке виглядає легітивним та несе цінні додаткові функції для користувача. Типовим прикладом є генератор ключів (або кейген) для піратської копії комерційного програмного забезпечення. Після запуску він витягує корисне навантаження та зберігає його в пам'яті цільового пристрою. Дропер також може запускати інсталятори шкідливих програм. Корисне навантаження дропера зазвичай включає декілька троянських програм. Таке ШПЗ не обов'язково пов'язане між собою і може використовуватися з різною метою. Дропер також може бути обфускованим. Механізм нейтралізації виявлення дропера залежить від типу цільової операційної системи. Наприклад, дропери для Windows зазвичай відключають контроль облікових записів користувачів (User Account Control), який сповіщає користувачів про будь-які спроби виконати дії, що впливають на критичні елементи системи.

Потрапляючи в оперативну пам'ять цільової системи клієнтська частина "Cobalt Stricke" встановлює своє корисне навантаження, що називається "Beacon"[3]. Клієнтська частина "Cobalt Stricke" може працювати на ОС Windows, Linux, MacOS, встановлена в зловмисних цілях на цільовій системі виконує функції бекдору. Cobalt Strike Team Server (сервер) може об'єднувати декілька операторів (зловмисників) та їхні хости в єдину Central Cobalt Strike Console. В такому разі усі вони будуть використовувати одні й ті ж сеанси зв'язку, зберігати отримані дані, ділитися захопленими файлами, вести спільні журнали подій. Серверна частина буде виконувати функції віддаленого Comand&Control (C2) сервера. Для здійснення віддаленого доступу до цільової системи в своїй інфраструктурі командні сервери зазвичай використовують редиректори (Рис. 2)

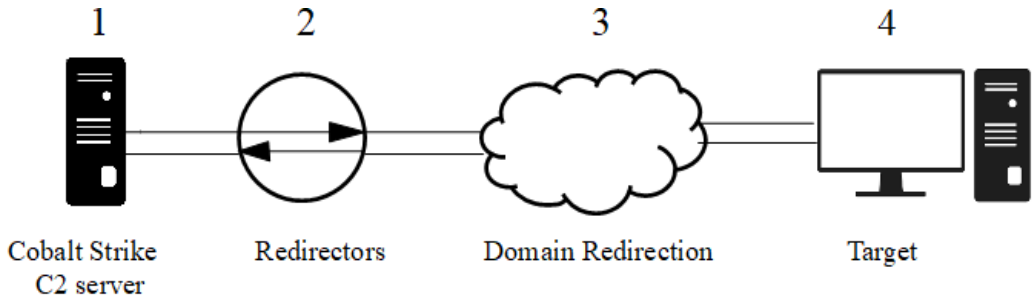

Рис. 2. Схема взаємодії С2 сервера з цільовою системою через редиректори

Редиректори – це хости, які виконують функцію перенаправлення трафіку на справжній сервер управління С2. Зловмисниками може використовуватися ціла ієрархія редиректорів, таким чином виявлення інфраструктури противника значно ускладнюється. Також, зв'язок через редиректори може організовуватися з С2 серверу з використанням утиліти "Socat" та через проксі сервери. "Socat" дозволяє здійснювати двонаправлений обмін даними між серверною та клієнтською частиною Cobalt Strike [4].

Одним з найважливіших компонентів "Beacon" є "Listeners", які допомагають "Beacon" зв'язуватися через редиректори з командним сервером. "Listeners" бувають чотирьох типів і відрізняються за протоколом зв'язку: http/https Beacon; DNS Beacon; SMB Beacon; TCP Beacon. Причому, SMB Beacon та TCP Beacon використовуються при вдалому здійснені "бокового переміщення" в межах локального сегменту мережі (Рис. 3).

Щоб замаскувати свою присутність в локальній мережі і приховати нелегітимний трафік від систем виявлення в Cobalt Strike передбаченена взаємодія між головною і підлеглою нодою (вузлом, хостом). З командним сервером відкрито взаємодіє лише головна нода, а підлеглі ноди між собою та з головною нодою взаємодіють за протоколом SMB (порт TCP 445).

Головна нода з командним сервером зазвичай взаємодіють за протоколом http/https (рідше DNS). Використовуючи саме ці протоколи є можливість приховування аномального трафіку в мережі, адже він імітує звичайний користувацький трафік, уникаючи виявлення

© Хавер, А. В. (2023). Принципи функціонування та виявлення на цільовій системі інструменту подвійного призначення Cobalt Strike. Сучасний захист інформації, 2(54), 13–18. https://doi.org/10.31673/2409-7292.2023.020002.

засобами моніторингу мережевого трафіку. Важливо відзначити, що “Beacon” може перебувати у стані так званого сну і не завжди бути активним, відтак його трафік не буде регулярним. Проте робота з Cobalt Strike в інтерактивному режимі генеруватиме значну кількість мережевих запитів, особливо з деякими “Beacon” (наприклад, DNS), коли відбувається завантаження файлів [5].

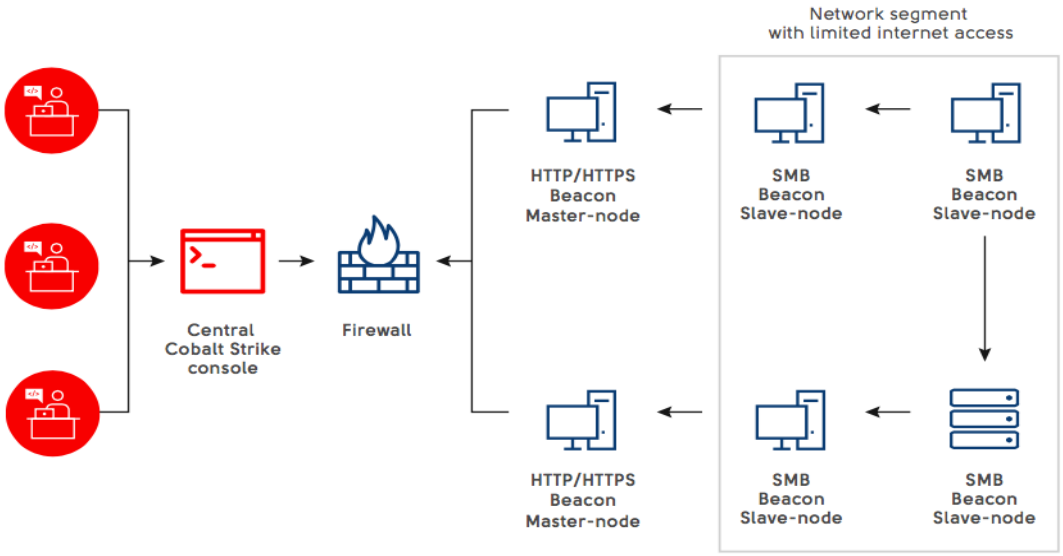

Рис.3 Схема взаємодії клієнт-сервер через “маяки” (Beacon) в Cobalt Strike

Для запобігання потрапляння даного інструменту подвійного призначення в систему рекомендовано перш за все інформувати користувачів стосовно імовірності проведення таргетованих фішингових атак; необхідності використання виключно ліцензійного програмного забезпечення на автоматизованих робочих місцях; регулярно оновлювати штатне програмне забезпечення задля уникнення експлуатації його вразливостей.

Весь процес ідентифікації ураження клієнтською частиною Cobalt Strike в мережі передбачає виявлення аномалій на певній ланці або ланках роботи кінцевої точки чи мережі. Тому засоби виявлення мають бути застосовані комплексно. Для ефективного виявлення адміністратором мережі можуть бути застосовані наступні заходи (Рис.4):

моніторинг використання командного рядка (PowerShell). Адміністратору необхідно використовувати ведення журналу активності PowerShell. Крім того адміністративно ввівши обмеження на використання цього засобу на користувацьких системах та заборонивши ініціювання PowerShell Remouting можна суттєво знизити ризики його використання зловмисниками;

сканування пам’яті, що передбачає аналіз оперативної пам’яті кінцевого пристрою, адже безфайлові атаки працюють саме з оперативною пам’яттю. Для її аналізу, зокрема, використовуються різноманітні інструменти для захисту кінцевих точок від складних загроз (EDR - Endpoint Detection and Response) [6]. Також для дослідження процесів пам’яті може бути використано програмний інструмент “Rekall”. Корисною практикою для періодичного аналізу процесів оперативної пам’яті є створення регулярних дампів пам’яті;

сканування відкритої мережевої інфраструктури, що передбачає використання спеціальних програмних засобів для контролю трафіку того сегменту мережі, який має безпосередній вихід в Інтернет, адже саме в цьому місці мережі можна виявити аномалії;

моніторинг статичного або динамічного двійкового коду передбачає сукупність двох видів дослідження, що здійснюється на кінцевих точках. Статичний аналіз — засобами АВПЗ на наявність сигнатур (індикаторів) та перевірку файлу на наявність рядків, які можуть

вказувати на завантажувані ним модулі та іншу інформацію таку як IP-адреси, URL-адреси, доменні імена і т.д., яку можна отримати із двійкового виконуваного файлу. Проте цей тип аналізу працює з виконуваним кодом який не проходив обфускацію. Якщо ж її було здійснено, необхідно використовувати додаткові програмні інструменти для здійснення подальшого аналізу (наприклад FLOSS – FireEye Labs Obfuscated String Solver). Проте, важливо зауважити, що зловмисники можуть навмисно розміщати всередині двійкових файлів URL-адреси, IP-адреси, імена хостів та іншу інформацію, яка не є дійсною. Це робиться з метою відслідковування, коли хтось взаємодіє і аналізує їх двійкові файл;

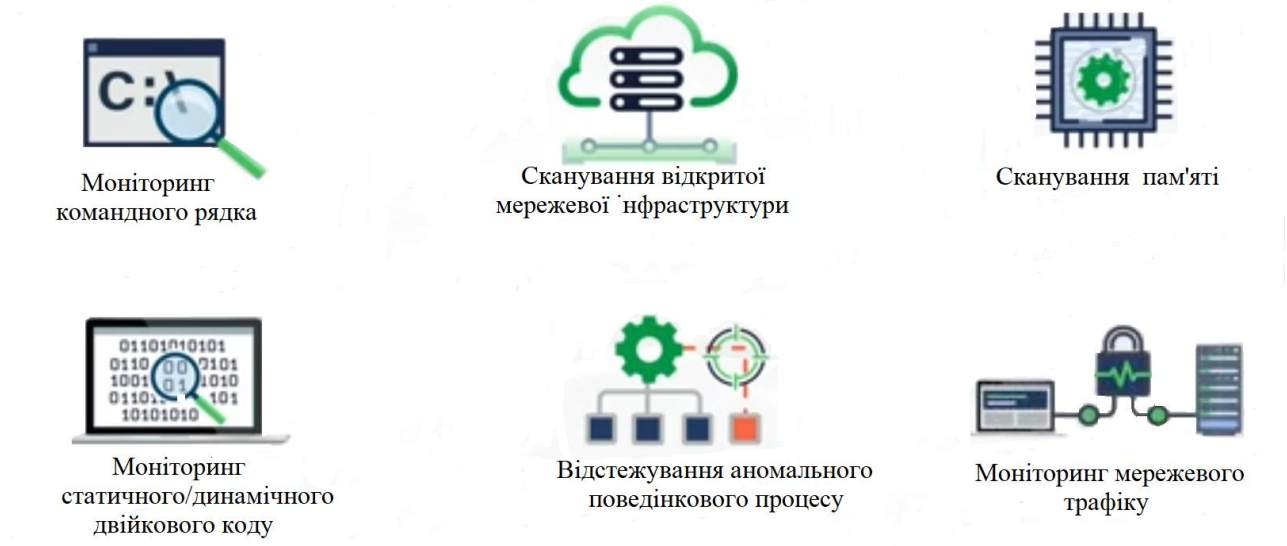

Рис.4 Заходи з виявлення Cobalt Strike в локальній мережі

динамічний аналіз дозволяє виявити як підозріла програма взаємодіє з системою на віртуальній машині з використанням автоматизованих систем для аналізу ШПЗ – sandbox. Хоча деякі зразки ШПЗ можуть визначати чи знаходяться вони в штучному середовищі sandbox, і якщо так, то не проявляти свої справжні шкідливі функції;

відстежування аномального поведінкового процесу, що передбачає ретельний аналіз адміністратором мережі, як активності кінцевих точок так і мережевої активності на основі знання “норми” в системі і таким чином виявлення відхилень або аномалій в ній;

моніторинг мережевого трафіку з використанням спеціалізованої системи моніторингу дозволяє виявити різні його види аномалій (наприклад через систему моніторингу Security Onion) [7].

Рекомендації щодо виявлення Cobalt Strike

Виявлення застосування порушником інструменту Cobalt Strike може бути складним завданням, оскільки цей інструмент має функції, що дозволяють приховувати його від спостереження. Однак, існують деякі ознаки, які можуть вказувати на застосування Cobalt Strike в атаках на систему. Ось деякі ознаки, на які можна звернути увагу при виявленні застосування Cobalt Strike:

1. Підозрілий мережевий трафік: Cobalt Strike може використовувати спеціальний протокол, який не звичайний для більшості легітимних програм і сервісів. Також, він може взаємодіяти зі специфічними портами, що зазвичай не використовуються для комунікації між комп'ютерами.

2. Наявність підозрілих процесів: Cobalt Strike може створювати підозрілі процеси, які не звичайні для легітимних програм та служб. Ці процеси можуть мати незвичайні атрибути, такі як високий рівень привілеїв або змінений час створення.

3. Дії з віддаленого доступу: Cobalt Strike може використовуватися для забезпечення віддаленого доступу до комп'ютера. Якщо виявлено дії з віддаленого доступу, які не були дозволені адміністратором системи, це може свідчити про застосування Cobalt Strike.

4. Дії зі шкідливим кодом: Cobalt Strike може використовуватися для розповсюдження шкідливого коду. Якщо виявлено дії зі шкідливим кодом, таким як відкривання файлів з підозрілими розширеннями або запуск невідомих програм, це може свідчити про застосування "Cobalt Strike".

5. Відсутність антивірусного захисту: Cobalt Strike може бути виявлений шляхом відсутності реакції антивірусного захисту на виконання підозрілих дій в системі. Оскільки "Cobalt Strike" є добре відомим інструментом в кіберзлочинців, багато антивірусних програм можуть реагувати на його застосування.

6. Використання знань з безпеки: Cobalt Strike може бути виявлений шляхом застосування в ньому певних методів та технік, що вимагають високого рівня знань з безпеки. Ці методи можуть бути виявлені шляхом моніторингу журналів системи та застосування вимог щодо встановлення паролів, захисту мереж та інших заходів безпеки.

7. Наявність підозрілих файлів: Cobalt Strike може бути виявлений шляхом пошуку підозрілих файлів на комп'ютері або в мережі. Ці файлі можуть мати підозрілі назви, розширення або містити підозрілий код.

Щоб виявити застосування Cobalt Strike, можна використовувати спеціальні програми та інструменти для моніторингу мережі та обмеження доступу до підозрілих портів. Також, можна проводити регулярний аудит безпеки системи та реагувати на будь-які підозрілі дії в мережі.

Висновок

Враховуючи можливі масштаби негативних наслідків для об’єктів критичної інформаційної інфраструктури від ураження інструментом подвійного призначення Cobalt Strike необхідно врахувати особливості його функціонування та виявлення під час здійснення заходів з підвищення рівня кібербезпеки та кіберстійкості у інформаційних системах об’єктів критичної інфраструктури.

Перелік посилань

1. User Guide “Cobalt Strike 4.5” - [Електрон. ресурс] /“Help Systems”. – Режим доступу: www.helpsystems.com;

2. “How cybercriminals try to bypass antivirus protection - [Електрон. ресурс] – Режим доступу:https://”www.kaspersky.com/resource-center/threats/combating-antivirus;

3. “What is Cobalt Strike and How Does It Work?” - [Електрон. ресурс] – Режим доступу: https://www.netsurion.com/videos/what-is-cobalt-strike;

4. “Hunting and detecting Cobalt Strike” - [Електрон. ресурс] – Режим доступу: https://log.sekoia.io/hunting-and-detecting-cobalt-strike/;

5. “Defining Cobalt Strike Components So You Can BEA-CONfident in Your Analysis” - [Електрон. ресурс] – Режим доступу: https://www.mandiant.com/resources/blog/defining-cobalt-strike-components;

6. “Що таке Endpoint Detection and Response” - [Електрон. ресурс] – Режим доступу: https://ua.softlist.com.ua/articles/chto-takoe-endpoint-detection/;

7. Steve Anson“Applied Icident Response”, “Wiley”, 2021, 435 p.

Надійшла: 01.02.2023 Рецензент: д.т.н., професор Гайдур Г.І.