Cobalt Strike Hunting — simple PCAP and Beacon Analysis

By Michael Koczwara

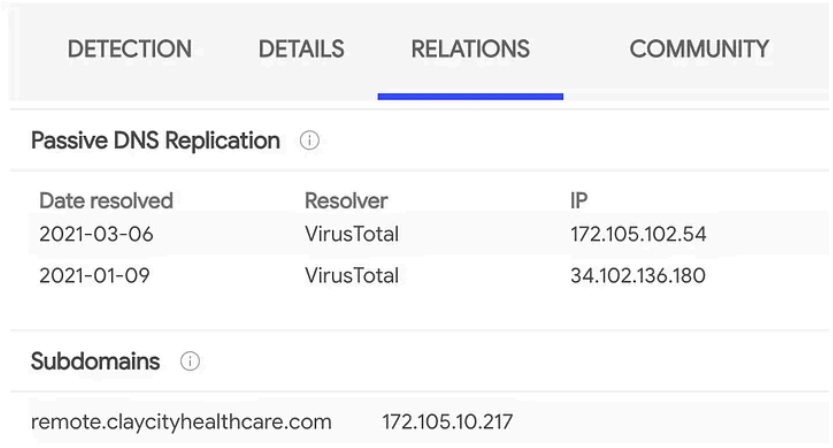
Published: 2021-08-08 · Archived: 2026-04-05 22:27:07 UTC

Threat Actors TTP's — hiding Cobalt Strike in claycityhealthcare[.]com subdomain.

Let's investigate subdomains using Shodan and VirusTotal.

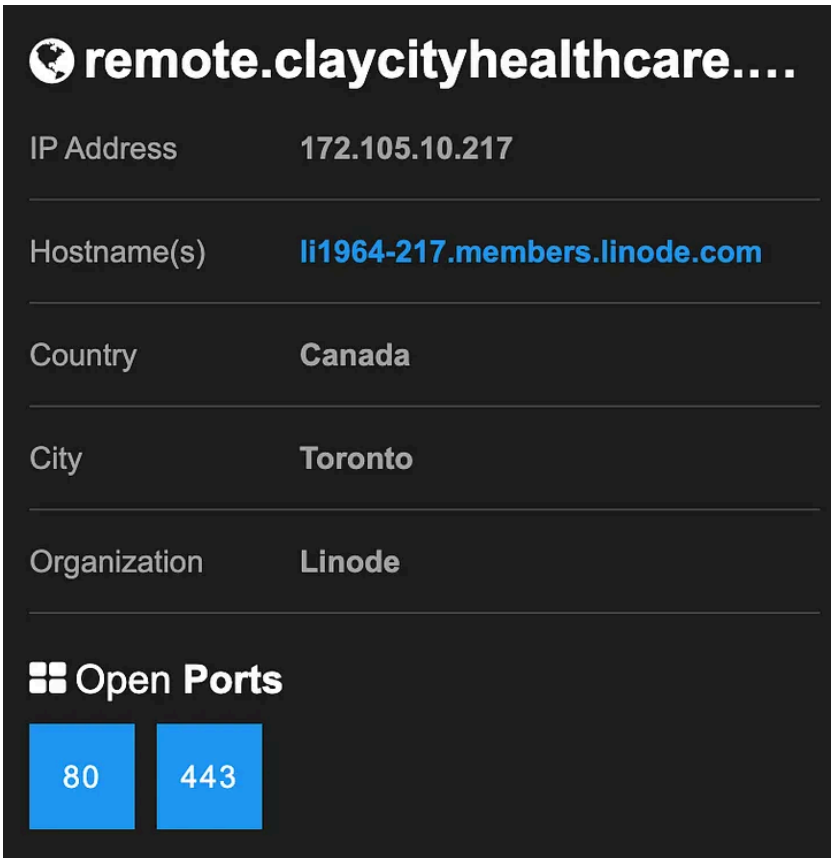
Quick Virus Total and Shodan check.

Press enter or click to view image in full size



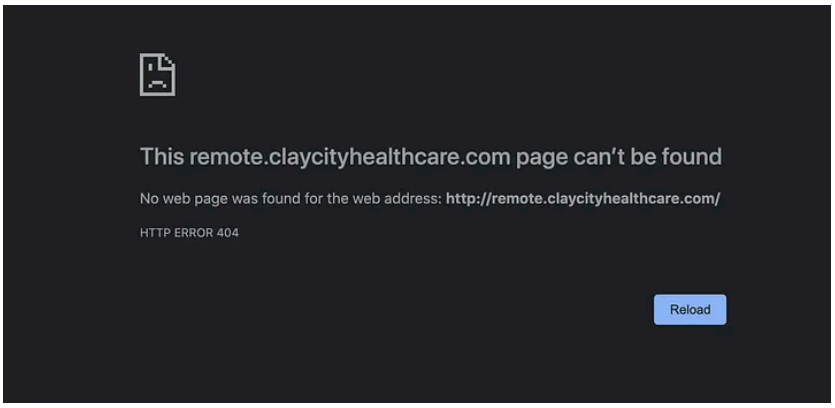
Shodan check.

Press enter or click to view image in full size

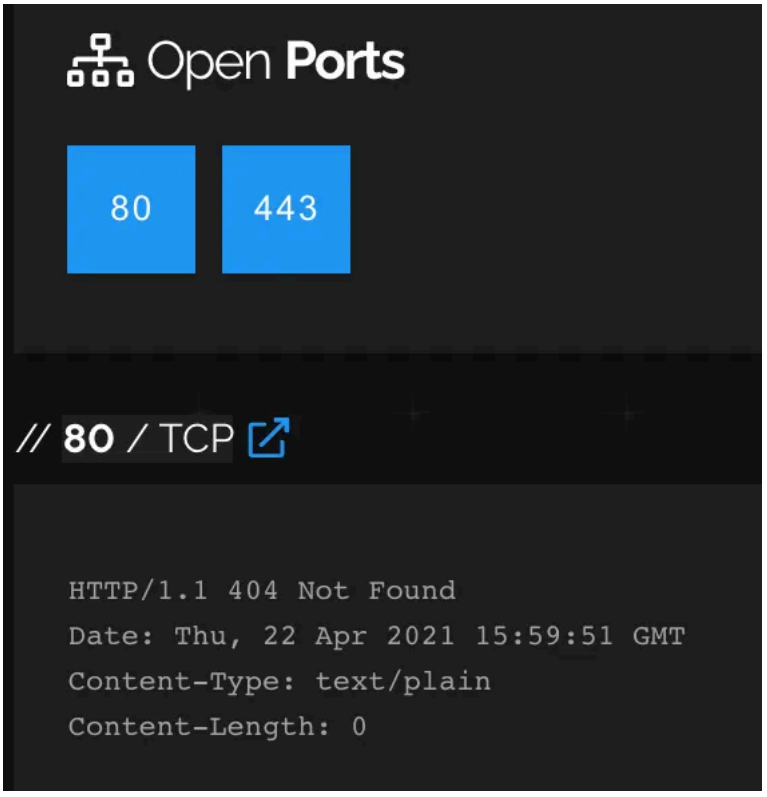


When you go to remote.claycityhealthcare[.]com the browser will display HTTP Error 404 page.

Press enter or click to view image in full size



Subdomain with two ports opened 80 and 443.



HTTP/1.1 404 Not Found and Content-Type: text/plain Content-Length:0 is always suspicious to me.

Press enter or click to view image in full size

Right, so now let's scan the subdomain using Nmap script to identify potential Cobalt Strike/C2.

What is interesting in this one is **Malleable profile**

remote.claycityhealthcare.com/**CWoNaJLBo/VTNeWw11212**

Get Michael Koczwara's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

A Malleable C2 is a way for an attacker to blend in command and control traffic (beacons between victim and server) with the goal of avoiding detection. Malleable C2 Profiles can be customized.

If you don't know about Comfoo, this is a good read.

Beacon analysis

Let's quickly analyze the Beacon and clarify the most interesting info.

{
“BeaconType”: [
“HTTP”
],
“MD5”: “9773d90443383e04c171c5b3e3017740”,
“Filename”: “cshell/a36fbae6e4c3e98560fc0f90ce075fb0d65ca926fdcfebea11a1b90445374c82.decoded”,
“Port”: 80,
“SleepTime”: 30000,

(0.5 minute) time when beacon will call home, 60000 is a default one.

“MaxGetSize”: 1048576,
“Jitter”: 20,

Beacon will vary each of its check in times by the random percentage you specify as a jitter factor from 0 -99.

“MaxDNS”: “Not Found”,
“PublicKey”:

“MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4P4BXSFMmJsHj3ePkNMOVGRsqJFQngo2QAFX0spN5orR8gltRgIcI0cseMS9BE2iPX

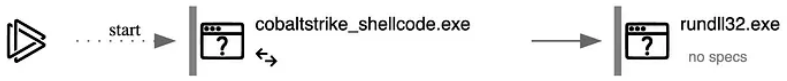
“C2Server”: “remote.claycityhealthcare.com,/CWoNaJLBo/VTNeWw11212/”,

“UserAgent”: “Not Found”,
“HttpPostUri”: “/CWoNaJLBo/VTNeWw11213/”,
“HttpGet_Metadata”: “Not Found”,
“HttpPost_Metadata”: “Not Found”,
“SpawnTo”: “Sm5rsPpaNgDLmwgX+eatPw==”,
“PipeName”: “Not Found”,
“DNS_Idle”: “Not Found”,
“DNS_Sleep”: “Not Found”,
“SSH_Host”: “Not Found”,
“SSH_Port”: “Not Found”,
“SSH_Username”: “Not Found”,
“SSH_Password_Plaintext”: “Not Found”,
“SSH_Password_Pubkey”: “Not Found”,
“HttpGet_Verb”: “GET”,
“HttpPost_Verb”: “POST”,
“HttpPostChunk”: 0,

“Spawnto_x86”: “%windir%\\syswow64\\rundll32.exe”,
“Spawnto_x64”: “%windir%\\sysnative\\rundll32.exe”,

This is where Cobalt Strike shellcode would spawn.

Press enter or click to view image in full size



rundll32.exe it is a default one.

“CryptoScheme”: 0,
“Proxy_Config”: “Not Found”,
“Proxy_User”: “Not Found”,
“Proxy_Password”: “Not Found”,
“Proxy_Behavior”: “Use IE settings”,

“Watermark”: 2005485734,

Watermark is unique to a customer and sometimes could be assigned and attributed to specific threat actors.

“bStageCleanup”: “False”,
“bCFGCaution”: “False”,
“KillDate”: “2099–01–01”,
“bProcInject_StartRWX”: “True”,
“bProcInject_UseRWX”: “True”,
“bProcInject_MinAllocSize”: 0,
“ProcInject_PrependAppend_x86”: “Empty”,
“ProcInject_PrependAppend_x64”: “Empty”,
“ProcInject_Execute”: [
“CreateThread”,
“SetThreadContext”,
“CreateRemoteThread”,
“RtlCreateUserThread”
],
“ProcInject_AllocationMethod”: “VirtualAllocEx”,
“bUsesCookies”: “False”,
“HostHeader”: “”

References:
