DefCamp HackingVillage 2021

Author: <0x435446> - <mihai.cujba@yahoo.com>

Summary

DefCamp HackingVillage 2021 1
Summary 1
Challenge: unpac (<3120>) 4
<Q1> (<420>): <Malware> 4
Proof of Flag 4
Question 4
Proof of Solving 4
<Q2> (<430>): <Malware> 5
Proof of Flag 5
Question 5
Proof of Solving 5
<Q3> (<440>): <Malware> 5
Proof of Flag 5
Question 5
Proof of Solving 5
<Q4> (<460>): <Malware> 6
Proof of Flag 6
Question 6
Proof of Solving 6
<Q5> (<500, in caz ca ar conta) >): <Malware> 6
Proof of Flag 6
Question 6
Proof of Solving 7
<Q6> (<440>): <Malware> 7
Proof of Flag 7
Question 7

Proof of Solving 7
<Q7> (<430>): <Malware> 7
Proof of Flag 7
Question 7
Proof of Solving 7
Challenge: StepUp (<470>) 8
<Q1> (<470>): <Malware> 8
Proof of Flag 8
Question 8
Proof of Solving 8
Challenge: netlogmon (<5320>) 10
<Q1> (<430>): <Malware> 10
Proof of Flag 10
Question 10
Proof of Solving 10
<Q2> (<430>): <Malware> 11
Proof of Flag 11
Question 11
Proof of Solving 11
<Q3> (<440>): <Malware> 11
Proof of Flag 11
Question 11
Proof of Solving 12
<Q4> (<440>): <Malware> 12
Proof of Flag 12
Question 12
Proof of Solving 12
<Q5> (<460>): <Malware> 13
Proof of Flag 13
Question 13
Proof of Solving 13
<Q6> (<440>): <Malware> 14
Proof of Flag 14

Question 14
Proof of Solving 14
<Q7> (<440>): <Malware> 15
Proof of Flag 15
Question 15
Proof of Solving 15
<Q8> (<440>): <Malware> 15
Proof of Flag 15
Question 15
Proof of Solving 16
<Q9> (<460>): <Malware> 16
Proof of Flag 16
Question 16
Proof of Solving 16
<Q10> (<450>): <Malware> 17
Proof of Flag 17
Question 17
Proof of Solving 17
<Q11> (<450>): <Malware> 18
Proof of Flag 18
Question 18
Proof of Solving 18
<Q12> (<450>): <Malware> 19
Proof of Flag 19
Question 19
Proof of Solving 19

Challenge: unpac (<3120>)

<Q1> (<420>): <Malware>

Proof of Flag

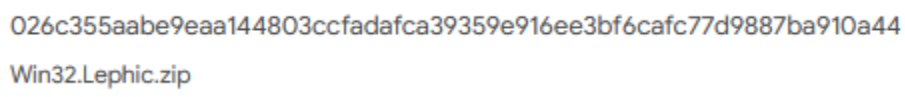
explorer.exe

Question

Into what process does the malware inject its code?

Proof of Solving

Pentru început voi explica pașii pentru a detecta despre ce malware este vorba. Primeam în descriere un sha256 (026c355aabe9eaa144803ccfadafca39359e916ee3bf6cafc77d9887ba910a44), cel al malware-ului, pe care l-am căutat pe virustotal și am găsit asta:



De aici am căutat malware-ul pe github și l-am găsit: https://github.com/0xBADBAC0N/malware/tree/master/Win32.Lephic

Am descărcat malware-ul și am făcut exact ce scria în primul hint de pe discord: unpac.me.

Am intrat pe https://unpac.me și am despachetat malware-ul (După multe încercări cu PEiD și alte unpackere).

Am folosit IDA pentru a analiza conținutul fișierului malițios.

Pe lângă IDA am folosit și un sandbox online, pentru a detona malware-ul și a vedea ce registrii se modifică.

Linia de cod din IDA care ne arată procesul injectat:

```
hProcess = sub_4013E0(aExplorerExe_0);
```

aExplorerExe face referire la un string din zona de date, “explorer.exe”.

<Q2> (<430>): <Malware>

Proof of Flag

S-1-5-21-0243556031-888888379-781863308-12986119

Question

What is the directory name the malware creates where it keeps its persistence? (format: S-.*-\d{8})

Proof of Solving

Pentru întrebarea aceasta am avut nevoie de VirusTotal, unde am reuploadat malware-ul, dar despachetat, iar SecondWrite a reușit să găsească numele folderului creat de către PE-ul infectat.
https://www.virustotal.com/gui/file/f95efe3ccbd55d03d56958d4518676f69385f43c102f41f700bbc784d6695c4a/behavior/SecondWrite

Files Written

C:\RECYCLER\S-1-5-21-0243556031-888888379-781863308-12986119\Desktop.ini

Files Deleted

C:\RECYCLER\S-1-5-21-0243556031-888888379-781863308-12986119\sjdbpro61.exe

<Q3> (<440>): <Malware>

Proof of Flag

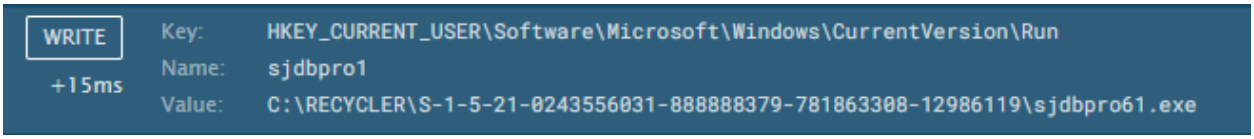
sjdbpro1

Question

The process does some operations with a system register. What is the value it saves on the register?

Proof of Solving

Aici m-am folosit de any.run, am detonat malware-ul în sandbox-ul lor și am văzut exact ce se întâmplă cu registrii după execuție.
Analiză: https://app.any.run/tasks/ce146459-dba4-4a9b-b483-eb29620b016e



<Q4> (<460>): <Malware>

Proof of Flag

sjdbpro

Question

The malware tests if it can inject data into a process. What is the data, until the first null byte, it injects at this test?

Proof of Solving

Pentru rezolvarea acestui task m-am folosit în continuare de IDA, iar această linie de cod are rolul de alocare de memorie + injectare.

```
*((_DWORD *)hMem + 68) = sub_4014A0(hProcess, aSjdbpro, 0x33u);
```

```
void *__stdcall sub_4014A0(HANDLE hProcess, LPCVOID lpBuffer, SIZE_T dwSize)
{
  void *lpBaseAddress; // [esp+0h] [ebp-4h]

  lpBaseAddress = VirtualAllocEx(hProcess, 0, dwSize, 0x1000u, 0x40u);
  if ( !lpBaseAddress )
    return 0;
  if ( WriteProcessMemory(hProcess, lpBaseAddress, lpBuffer, dwSize, 0) )
    return lpBaseAddress;
  return 0;
}
```

De aici putem verifica ce string este în memorie în locul variabiei aSjdbpro, respectiv sjdbpro.

<Q5> (<500, in caz ca ar conta 😋) >): <Malware>

Proof of Flag

Nope ☹

Question

After calling WaitForSingeObject, what is the next function call? Provide parameters too. (format: - ex: FunctionName("StRiNg",var,1234,var))

Proof of Solving

Am văzut în cod șirul de pointeri către funcțiile de sistem, am văzut Sleep-ul, dar chiar nu am găsit argumentul cu care era folosit ☹.

<Q6> (<440>): <Malware>

Proof of Flag

ws2_32.dll

Question

What DLL is loaded after the function identified at question 5? (format: name.dll)

Proof of Solving

Exact în același loc unde se găsea și sirul de pointeri către funcții se găsea și următoarea linie de cod: `v3 = LoadLibraryA(aWs232Dll);` , => ws2_32.dll

<Q7> (<430>): <Malware>

Proof of Flag

dq.sjdbproxies.ru

Question

What is the full domain of the command and control server? (format: www.example.com)

Proof of Solving

Erau așezate de IDA exact cum trebuie, parcă știa că o sa avem nevoie de ele :D

```
.data:00404000 aSjdbpro        db 'sjdbpro',0          ; DATA XREF: start+9F↑o
.data:00404008 aDqSjdbproxiesR db 'dq.sjdbproxies.ru',0
.data:0040401A aWs232Dll_0     db 'ws2_32.dll',0
```

Challenge: StepUp (<470>)

<Q1> (<470>): <Malware>

Proof of Flag

CTF{4723f900215592f81987a100423ff28da3ea2a00b422897e1276eb544e6f8bbe}

Question

What is the flag? (Scurt și cuprinzător 😊))

Proof of Solving

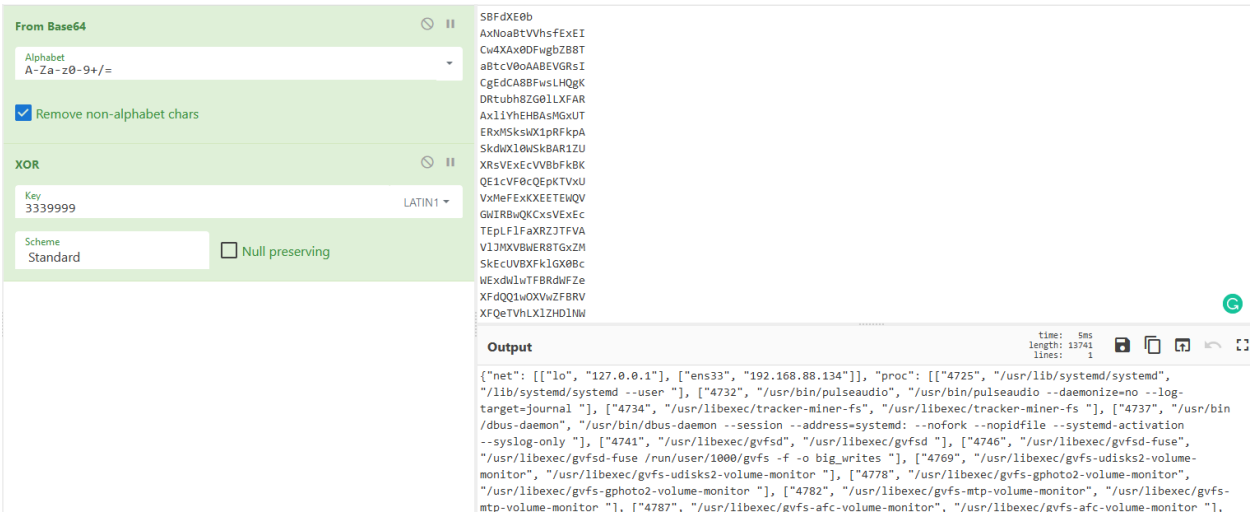
Pentru început am luat fișierul PCAP și am căutat să văd ce protocoale se găsesc în captura de trafic, iar de aici am ajuns la concluzia că toată acțiunea se petrecea în jurul a două pachete TCP. (Pachetele 1 și 5311)

De aici am dat follow la pachete și am văzut padding-ul de la base64 la jumătatea stream-ului, deci erau două mesaje acolo (din primul pachet și din ultimul).

Am luat prinul base64, l-am decodificat, iar de acolo am scos un fișier puc, pe care l-am decompilat folosind uncompyle6.

De aici am văzut mai multe comenzi de bash date, printre care și citirea unei chei de ssh (Nu am făcut ss la codul decompilat ☹), dar știu că la un moment dat în cod se citea /etc/passwd, fișierul de proc pentru cmdline si env (lucruri care nu apar în writeup-ul official).

Pe lângă aceste lucruri se putea observa și un XOR între datele citite de pe server și cheia “3339999”. Aceeași tehnică am văzut-o si la DAMCTF de acum câteva săptămâni, probabil de acolo este inspirat si challenge-ul (sneaky-script) (https://github.com/ab2pentest/ctfwriteups/blob/main/DamCTF/sneaky-script.md).



35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;
35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;
35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;
35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;
35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;
35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;
36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:",
"XDG_CURRENT_DESKTOP": "ubuntu:GNOME", "VTE_VERSION": "6003", "GNOME_TERMINAL_SCREEN": "/org/gnome/Terminal/screen
/20a1c576_0ae5_4a9f_9bed_162e06ba9032", "INVOCATION_ID": "b5c7562742e44663aa23b8d7ef58d4b7", "MANAGERPID": "4725",
"flag": "CTF{4723f900215592f81987a100423ff28da3ea2a00b422897e1276eb544e6f8bbe}", "GJS_DEBUG_OUTPUT": "stderr",
"LESSCLOSE": "/usr/bin/lesspipe %s %s", "XDG_SESSION_CLASS": "user", "TERM": "xterm-256color", "LESSOPEN": "|
/usr/bin/lesspipe %s", "USER": "kirk", "GNOME_TERMINAL_SERVICE": ":1.139", "DISPLAY": ":0", "SHLVL": "2",
"QT_IM_MODULE": "ibus", "XDG_RUNTIME_DIR": "/run/user/1000", "JOURNAL_STREAM": "8:110255", "XDG_DATA_DIRS":
"/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop", "PATH": "/usr/local/sbin:/usr/local
/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin", "GDMSESSION": "ubuntu",
"DBUS_SESSION_BUS_ADDRESS": "unix:path=/run/user/1000/bus", "OLDPWD": "/home/kirk/Desktop", "_": "/usr/bin

Având în vedere că am participat si la DAM CTF și mai văzusem asta și acolo, îmi dădusem seama de cheie din “strings” peste fișierul pyc, dar de dragul CTF_ului l-am decompilat și acum :D.

Challenge: netlogmon (<5320>)

<Q1> (<430>): <Malware>

Proof of Flag

ntlm.log

Question

Q1. Take a few minutes to familiarize yourself with Zeek log files. Go to the Discover Tab in Kibana and search for `log.file.path` in the "Available Fields" list from the left. Click on the field name to show its top five values. Click on "Visualize" to see them all.

Which log file contains the fewest records? *(filename.extension)*

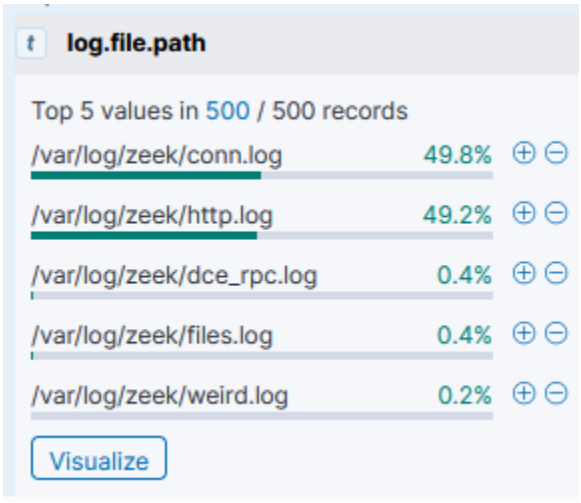
Proof of Solving

Pentru început am căutat să văd perioada în care a fost trafic și am găsit în perioada 28-29 Septembrie un număr considerabil de alerte.

De aici am urmat exact ce scria în cerință și am căutat după “log.file.path”

Filtru folosit: log.file.path : *

În partea stânfă, la Fileds am căutat de-asemenea log.file.path, am apăsat pe Visualize și am văzut un grafic cu intrările generate în fiecare logfile.



De aici se observă faptul că ntlm.log are cele mai puține intrări.

<Q2> (<430>): <Malware>

Proof of Flag

http://feedproxy.google.com/~r/zoziqddzgt/~3/SWLho3snQ0Y/chickadee.php

Question

Q2. As you enjoy your morning coffee, you come across a news article about how a group of attackers launch phishing campaigns using `feedproxy.google[.]com` links that once clicked will redirect users to URLs from new domains that will serve them OneDrive links to download macro-enabled Word documents.

Now that you've started to have some visibility into the organization's network traffic, you decide to perform a search to see if anyone has accessed `feedproxy.google[.]com` links. You quickly realize you're going to need more coffee because your search just returned some results.

What is the full URL that was accessed? *(http/s://www.example.com/index.html)*

Proof of Solving

Știam din cerință faptul că este vorba de feedproxy.google.com, așa că am filtrat dupa url.domain: feedproxy.google.com, iar la url.original se poate vedea path-ul accesat.

t	url.domain	feedproxy.google.com
t	url.original	/~r/zoziqddzgt/~3/SWLho3snQ0Y/chickadee.php

<Q3> (<440>): <Malware>

Proof of Flag

DESKTOP-71EBUL8.forgotmyhair.info

Question

Q3. You are onto something here so you decide to open a new case and start adding useful information.

What is the FQDN of the system that made the query to the previously discovered URL?
(myhostname.company.internal.domain)

Proof of Solving

Am căutat în singura intrare din fișierul de log-uri NTLM, iar aici am găsit asta:

t	zeek.ntlm.hostname	DESKTOP-71EBUL8
t	zeek.ntlm.server.name.dns	FORGOTMYHAIR-DC.forgotmyhair.info
t	zeek.ntlm.server.name.netbios	FORGOTMYHAIR-DC
t	zeek.ntlm.server.name.tree	forgotmyhair.info
◕	zeek.ntlm.success	true
t	zeek.ntlm.username	rosa.scott
t	zeek.session_id	CDAq9o3YmyOAHgMDue

De aici am încercat să văd dacă merge cumva hostname-ul de aici și Bingo!, a functionat.

<Q4> (<440>): <Malware>

Proof of Flag

51781

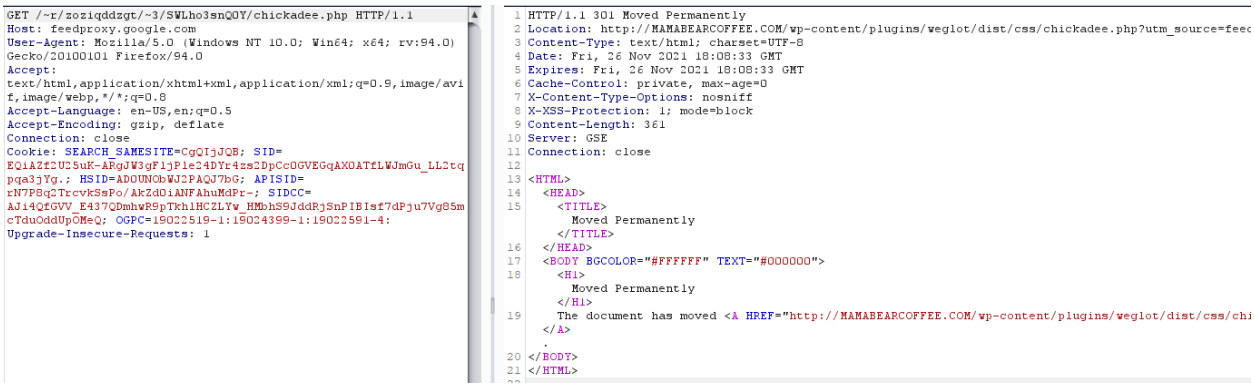
Question

Q4. You read in the article that users are redirected to another URL from a new domain once they click on the initial link from the email.

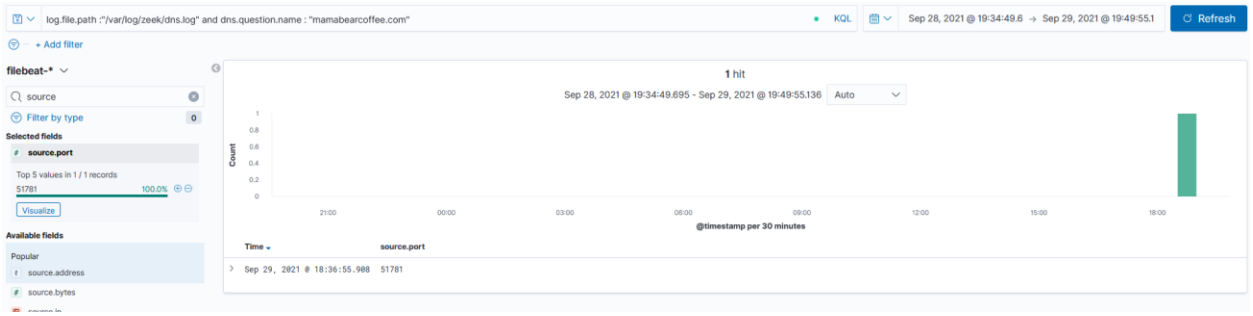
What is the source port of the DNS query performed for the new domain?

Proof of Solving

Aici am jucat puțin risky și am încercat să iau urma site-ului pe care l-am găsit la Q2. Pentru a fi sigur că nu o să intru pe site-ul redirectat am interceptat traficul cu Burp și nu am permis redirect-ul 😊), iar așa am văzut către ce site este trimis utilizatorul, respectiv pe MAMABEARCOFFEE.COM.



Mai departe am filtrat log-urile după fișierul de log-uri dns.log și query name-ul mamabearcoffee.com, iar ca filter am pus source.port și am scos răspunsul.



<Q5> (<460>): <Malware>

Proof of Flag

Sep 29, 2021 @ 18:38:39.510

Question

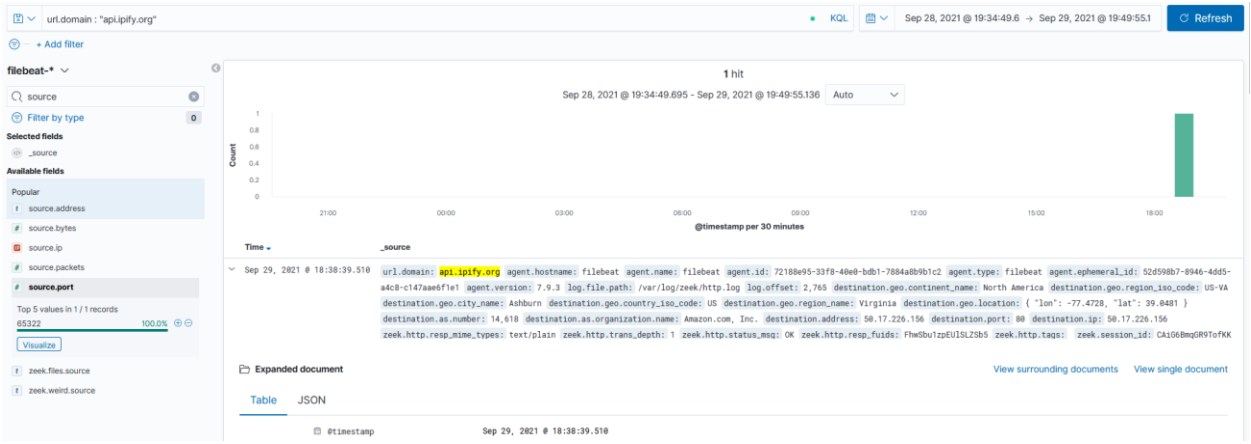
Q5. Next, users should be directed to OneDrive where they will download a Word document which upon opening and enabling macros, would execute code on the system.

Initially, the malware collects information about the infected host. This also includes a lookup of the external IP address using a legitimate public API service. Thus, the malware can check if it is running in a virtualized environment as it will not reach its command and control infrastructure unless it receives a successful response to this API call.

What is the exact time this lookup is performed? *(`timestamp` field value in Elastic)*

Proof of Solving

Aici am filtrat după url.domain: “api.ipify.org” și a apărut o singură alertă generat cu timestamp-ul Sep 29, 2021 @ 18:38:39.510.



<Q6> (<440>): <Malware>

Proof of Flag

http://forkineler.com/8/forum.php

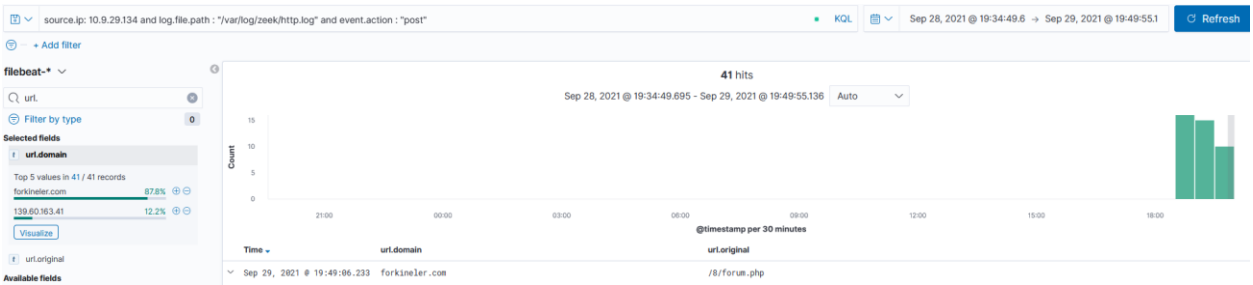
Question

Q6. The information just collected was sent to a command and control server using a POST request.

What URL was the malware using? *(http/s://www.example.com/index.html)*

Proof of Solving

Aveam IP-ul sursă de mai devreme (Din Q6 cel puțin), iar pe baza acestuia am căutat toate alertele cu IP Sursă 10.9.29.134, care se află în http.log și au ca event action “post”.



<Q7> (<440>): <Malware>

Proof of Flag

41.bin

Question

Q7. Over the next few moments, the malware tried to download more malware.

You may wonder why. Because that's how they roll! `Insert meme here.`

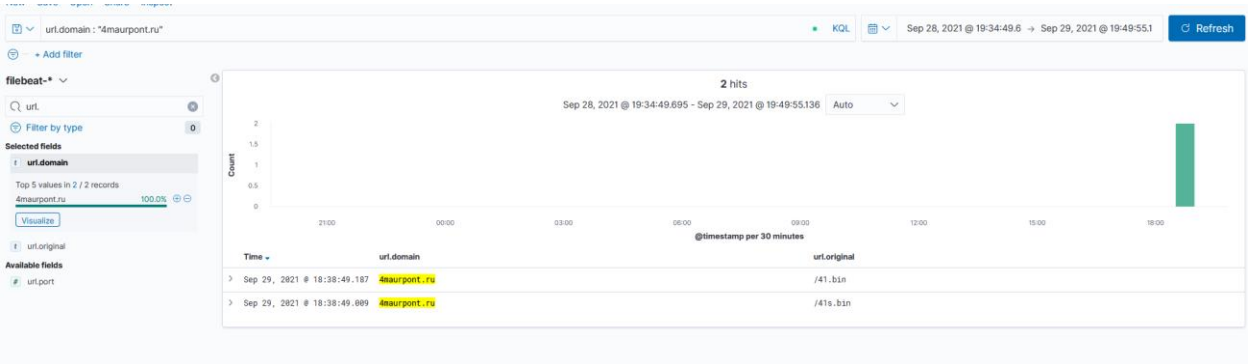
But the truth is that often the initial malware will attempt to download other payloads capable of extending both access and control over the infected host. The new malware could help download customized executables, scripts, or provide a means to run shell commands that could help infect the entire network and/or exfiltrate company data, which can then be sold by attackers or used against the victims.

What is the name of the second executable file downloaded? *(filename.extension)*

Proof of Solving

Aici am stat foarte mult să caut două fișiere prin log-uri și m-am decis să iau la rând URL-urile pentru a vedea dacă a fost vreo activitate suspectă pe unul dintre ele și așa am ajuns la 4maurpont.ru.

Cu filtrul deja setat de mai devreme (Q6) pentru url.domain și url.original, am văzut exact ce pagini au fost accesate, iar una dintre ele a fost exact malware-ul cerut.



<Q8> (<440>): <Malware>

Proof of Flag

139.60.163.41

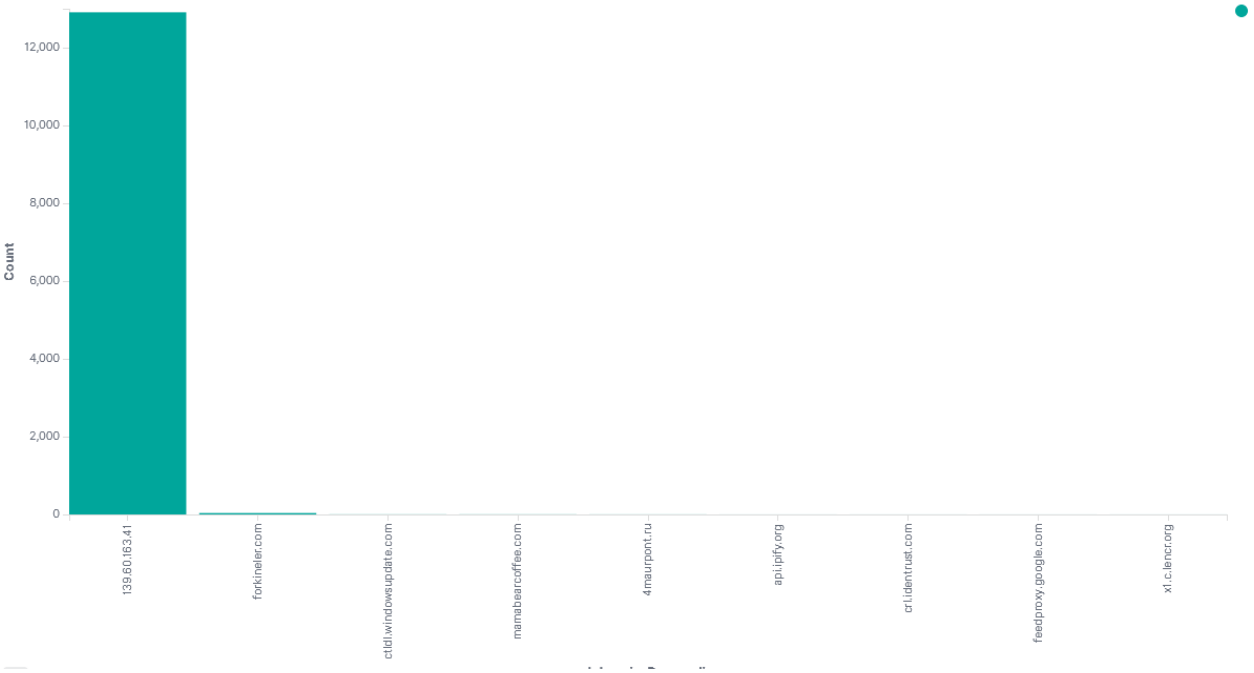
Question

Q8. After the new payloads have been downloaded and executed on the infected system, the malware will start beaconing to a second C2 server.

What is the IP address of the new C2 server?

Proof of Solving

Răspunsul la această întrebare l-am aflat prin verificarea ip-urilor destinație, iar acesta avea cele mai multe request-uri, iar restul erau ori verificate deja, ori domenii de certificate, așa că acesta a rămas cel vizat.



<Q9> (<460>): <Malware>

Proof of Flag

10.2

Question

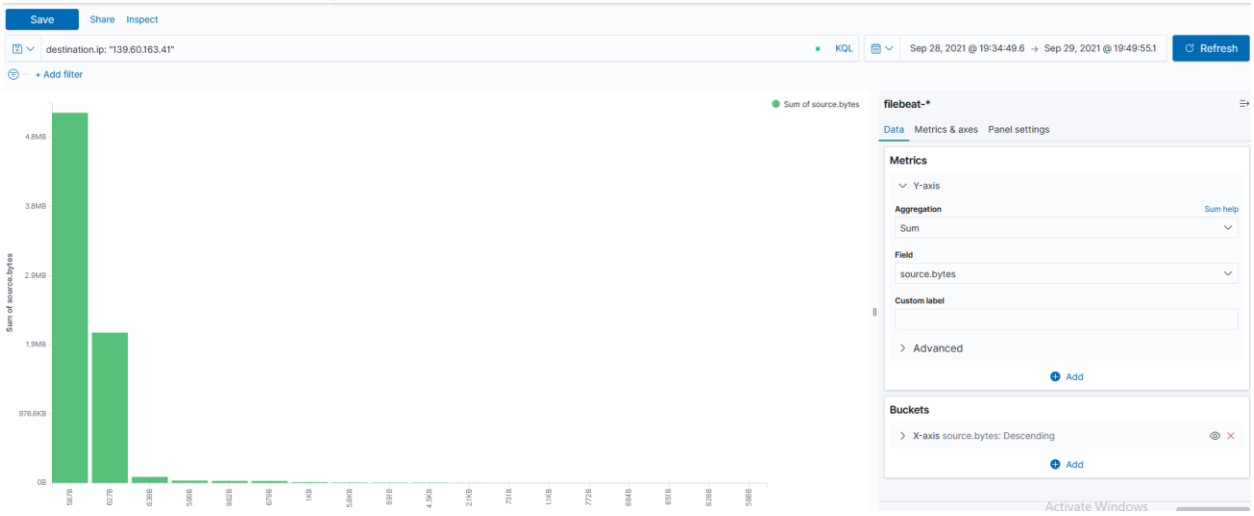
Q9. With so many beacons out there, it's important to check for signs of data exfiltration.

What is the total number of MB sent to this new C2 server? *(round to one decimal place)*

Proof of Solving

Aici am fost puțin indus în eroare de cerință, pentru ca am interpretat-o greșit și nu înțelegeam de ce nu dau un răspuns bun, dar eu trimiteam MB pe care îi primeam înapoi, nu pe cei care erau trimiși (am filtrat prost).

După ce am văzut că filtrasem dupa destination.bytes și nu după source.bytes am pus la search destionation.ipȘ 139.60.163.41, la filter source bytes și am verificat cu Visualize. De aici am făcut suma pentru fiecare camp din graphic și le-am adunat. Probabil este și o variant mai elegantă, dar de care nu știu.



Suma = 10.2

<Q10> (<450>): <Malware>

Proof of Flag

10.9.29.1,10.9.29.9 sau 10.9.29.9,10.9.29.1 (nu mai stiu exact ordinea, dar cred ca .1 era primul)

Question

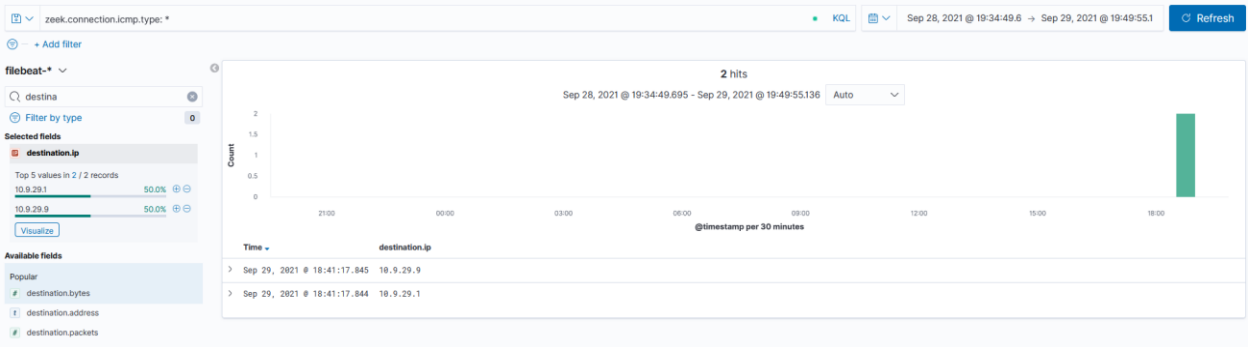
Q10. Now that the attacker has established his access and can send commands remotely, he will start to discover the environment in which he has landed in order to identify high-value targets to help him in fulfilling his mission.

The attacker tried to find the active hosts by pinging them.

What are the destination IP addresses to which this type of traffic was observed? *(enter comma separated values)*

Proof of Solving

În întrebare se specifică faptul că se dă ping, așa că am filtrat dupa ICMP, astfel: zeek.connection.icmp.type: * și am găsit două IP-uri.

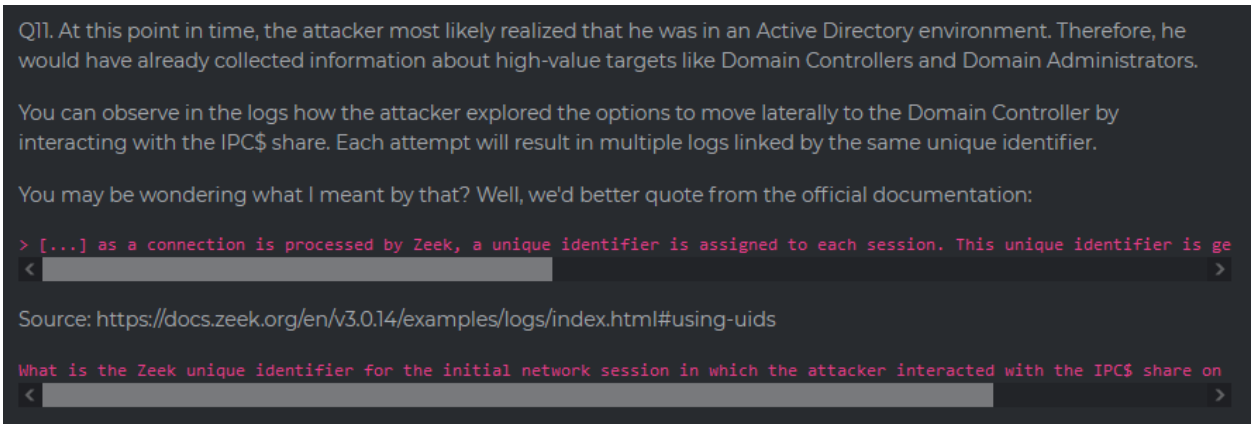


<Q11> (<450>): <Malware>

Proof of Flag

CDAq9o3YmyOAHgMDue

Question

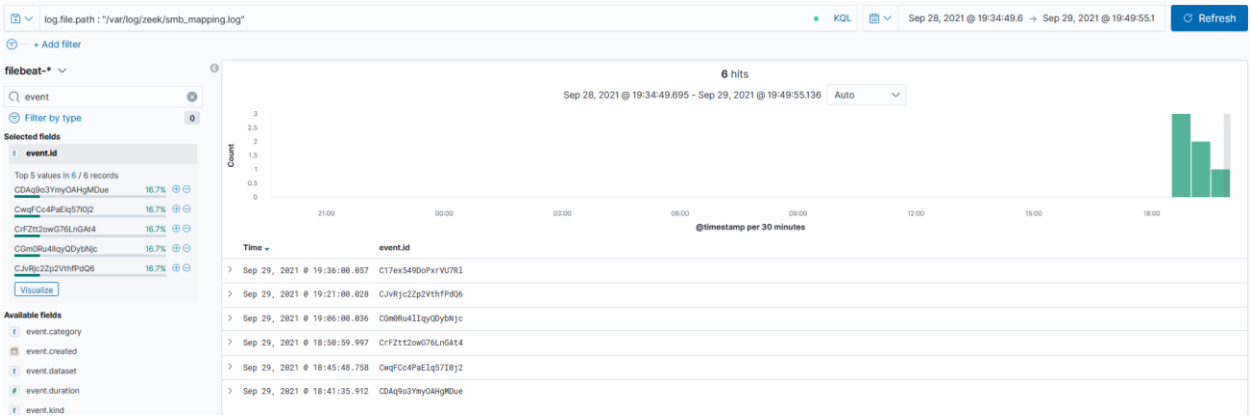


"What is the Zeek unique identifier for the initial network session in which the attacker interacted with the IPC$ share on the Domain Controller?"

Proof of Solving

Știind că este vorba de Domain Controller am filtrat după smb mapping, astfel: log.file.path : "/var/log/zeek/smb_mapping.log".

De aici m-am uitat la prima alertă generată, iar de aici am luat event id-ul.



<Q12> (<450>): <Malware>

Proof of Flag

Hancitor

Question

Q12. Based on the information discovered so far, what is the name of the malware used for initial access?

Proof of Solving

Aici am căutat exact după URL-ul “4maurpont.ru” și am intrat pe primul link, unde am găsit și restul de link-uri accesate de către programul malițios. (https://otx.alienvault.com/pulse/615fd9b5ca46f2842ca3ebd9)

TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
URL	http://yemodene.ru/8/forum.php	malware_hosting		Oct 8, 2021, 5:40:06 AM		1
URL	http://forkineler.com/8/forum.php	malware_hosting		Oct 8, 2021, 5:40:06 AM		1
URL	http://fordecits.ru/8/forum.php	malware_hosting		Oct 8, 2021, 5:40:06 AM		1
URL	http://4maurpont.ru/41s.bin	malware_hosting		Oct 8, 2021, 5:40:06 AM		1
URL	http://4maurpont.ru/41.bin	malware_hosting		Oct 8, 2021, 5:40:06 AM		1
URL	http://139.60.163.41:443/updates.rss	malware_hosting		Oct 8, 2021, 5:40:06 AM		1
URL	http://139.60.163.41:443/Nf5U	malware_hosting		Oct 8, 2021, 5:40:06 AM		1
URL	http://139.60.163.41:443	malware_hosting		Oct 8, 2021, 5:40:06 AM		0
URL	http://139.60.163.41/ptj	malware_hosting		Oct 8, 2021, 5:40:06 AM		2
URL	http://139.60.163.41/3Gvl	malware_hosting		Oct 8, 2021, 5:40:06 AM		1

De aici am intrat pe indicatorul generat de către http://forkineler.com/8/forum.php , iar la câmpul “Related Tags “ se găsea “hancitor”, exact numele malware-ului.