

Kelompok:

2501981270 - AGUSTINUS LEONARDO DWITAMA

2501989550 - MUHAMAD DWI APRIYANTO


2502001864 - RAVI DEEVAN SATYAKI

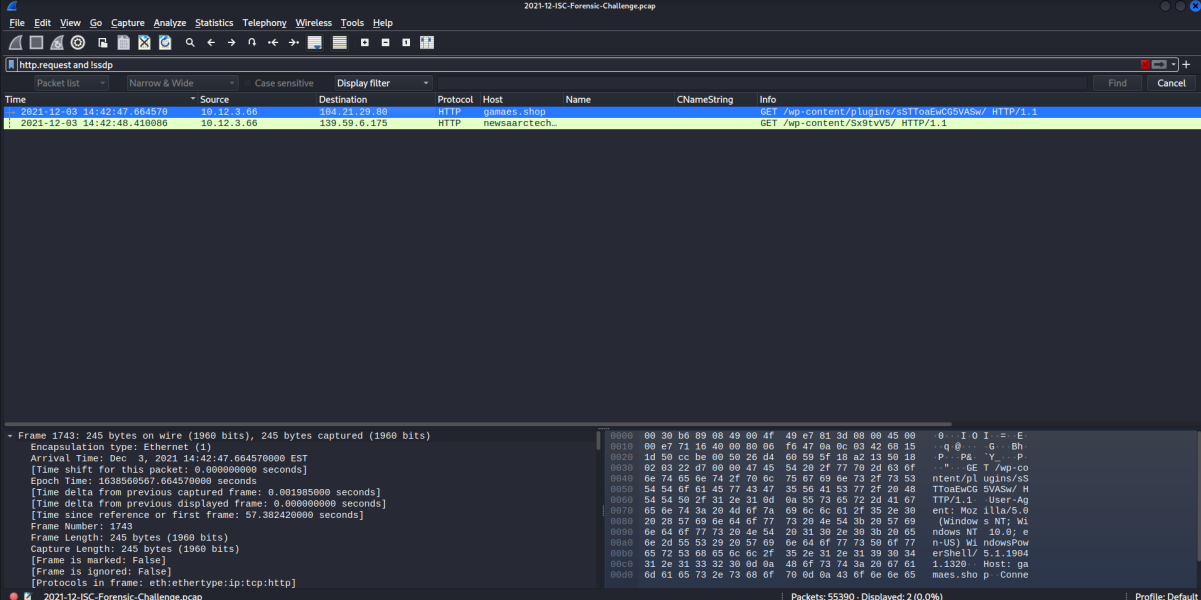
2501965052 - KEVIN MORRIS ARMANDO

2501983723 - NATANAEL FRANSISCO

Wireshark Forensics

2021-12-08 (WEDNESDAY) - PCAP FOR AN ISC DIARY (DECEMBER 2021 FORENSIC CHALLENGE)

Name	Date modified	Type	Size
 2021-12-ISC-Forensic-Challenge.pcap	08/12/2021 07:12	Wireshark capture file	32.203 KB



The image shows the Wireshark interface with the packet list pane displaying two HTTP GET requests. The first packet, at time 2021-12-03 14:42:47.664578, is a GET request to gmaaes.shop. The second packet, at time 2021-12-03 14:42:48.419086, is a GET request to newsaartech. The packet details pane shows the structure of the first packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.

Time	Source	Destination	Protocol	Host	Name	CNameString	Info
2021-12-03 14:42:47.664578	10.12.3.66	104.21.29.88	HTTP	gmaaes.shop			GET /wp-content/plugins/sstToaEwC5VASw/ HTTP/1.1
2021-12-03 14:42:48.419086	10.12.3.66	139.59.6.175	HTTP	newsaartech...			GET /wp-content/Sx9tvv5/ HTTP/1.1

Berdasarkan source yang kita dapat ini menyatakan **10.12.3.66** merupakan IP yang infected

Time	Source	Destination	Protocol	Host	Name	CNameString	Info
2021-12-03 14:41:56.361363	10.12.3.66	10.12.3.255	NBNS		DESKTOP-LUOABV1<2>		Registration NB DESKTOP-LUOABV1<2>
2021-12-03 14:41:56.736488	10.12.3.66	10.12.3.255	NBNS		DESKTOP-LUOABV1<0>		Registration NB DESKTOP-LUOABV1<0>
2021-12-03 14:41:56.736543	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<00>		Registration NB FARGREENTECH<00>
2021-12-03 14:41:56.124943	10.12.3.66	10.12.3.255	NBNS		DESKTOP-LUOABV1<2>		Registration NB DESKTOP-LUOABV1<2>
2021-12-03 14:41:56.489833	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<00>		Registration NB FARGREENTECH<00>
2021-12-03 14:41:56.489834	10.12.3.66	10.12.3.255	NBNS		DESKTOP-LUOABV1<0>		Registration NB DESKTOP-LUOABV1<0>
2021-12-03 14:41:56.878075	10.12.3.66	10.12.3.255	NBNS		DESKTOP-LUOABV1<2>		Registration NB DESKTOP-LUOABV1<2>
2021-12-03 14:41:56.254409	10.12.3.66	10.12.3.255	NBNS		DESKTOP-LUOABV1<0>		Registration NB DESKTOP-LUOABV1<0>
2021-12-03 14:41:56.254410	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<00>		Registration NB FARGREENTECH<00>
2021-12-03 14:41:56.647942	10.12.3.66	10.12.3.255	NBNS		DESKTOP-LUOABV1<2>		Registration NB DESKTOP-LUOABV1<2>
2021-12-03 14:41:56.025399	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<00>		Registration NB FARGREENTECH<00>
2021-12-03 14:41:56.025401	10.12.3.66	10.12.3.255	NBNS		DESKTOP-LUOABV1<0>		Registration NB DESKTOP-LUOABV1<0>
2021-12-03 14:41:56.456084	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1e>		Registration NB FARGREENTECH<1e>
2021-12-03 14:41:56.299333	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1e>		Registration NB FARGREENTECH<1e>
2021-12-03 14:41:56.696055	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1e>		Registration NB FARGREENTECH<1e>
2021-12-03 14:41:56.751429	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1e>		Registration NB FARGREENTECH<1e>
2021-12-03 14:41:56.545745	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1d>		Registration NB FARGREENTECH<1d>
2021-12-03 14:41:56.545952	10.12.3.3	10.12.3.66	NBNS		FARGREENTECH<1d>		Registration response, Name is owned by another node NB 10.12.3.3
2021-12-03 14:41:56.546627	10.12.3.66	10.12.3.255	NBNS		<01><02>_MSBROWSE_<02><01>		Name query NB <01><02>_MSBROWSE_<02><01>
2021-12-03 14:41:56.546832	10.12.3.3	10.12.3.66	NBNS		<01><02>_MSBROWSE_		Name query response NB 10.12.3.3
2021-12-03 14:41:56.656746	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH-DC<00>		Name query NB FARGREENTECH-DC<00>
2021-12-03 14:41:56.656941	10.12.3.3	10.12.3.66	NBNS		FARGREENTECH-DC<00>		Name query response NB 10.12.3.3
2021-12-03 14:41:56.658942	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH-DC<20>		Name query NB FARGREENTECH-DC<20>
2021-12-03 14:41:56.659091	10.12.3.3	10.12.3.66	NBNS		FARGREENTECH-DC<20>		Name query response NB 10.12.3.3
2021-12-03 14:41:56.660444	10.12.3.66	10.12.3.3	NBNS		DESKTOP-LUOABV1<2>		Name query response NB 10.12.3.66
2021-12-03 14:41:56.667931	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1d>		Registration NB FARGREENTECH<1d>
2021-12-03 14:41:56.668175	10.12.3.3	10.12.3.66	NBNS		FARGREENTECH<1d>		Registration response, Name is owned by another node NB 10.12.3.3
2021-12-03 14:41:56.669321	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1e>		Name query NB FARGREENTECH<1e>
2021-12-03 14:41:56.669473	10.12.3.3	10.12.3.66	NBNS		FARGREENTECH<1e>		Name query response NB 10.12.3.3
2021-12-03 14:41:56.669682	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1e>		Registration NB FARGREENTECH<1e>
2021-12-03 14:41:56.669880	10.12.3.38	10.12.3.66	NBNS		FARGREENTECH<1e>		Name query response NB 10.12.3.38
2021-12-03 14:41:56.670098	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1e>		Name query response NB 10.12.3.35
2021-12-03 14:41:57.415887	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1e>		Registration NB FARGREENTECH<1e>
2021-12-03 14:41:58.170356	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1e>		Registration NB FARGREENTECH<1e>
2021-12-03 14:41:58.241158	10.12.3.66	10.12.3.255	NBNS		FARGREENTECH<1e>		Registration NB FARGREENTECH<1e>

Kita dapat menggunakan command nbns untuk mendapatkan data network traffic netbios name service yang dimana kita bisa melihat juga hostname yang dari IP tersebut yang infected yaitu **DESKTOP-LUOABV1**

Time	Source	Destination	Protocol	Host	Name	CNameString	Info
2021-12-03 14:42:08.999587	10.12.3.66	10.12.3.3	KRB5		darin.figueroa AS-REQ		
2021-12-03 14:42:08.918139	10.12.3.66	10.12.3.3	KRB5		darin.figueroa AS-REQ		
2021-12-03 14:42:08.919743	10.12.3.3	10.12.3.66	KRB5		darin.figueroa AS-REP		
2021-12-03 14:42:08.923123	10.12.3.66	10.12.3.3	KRB5		darin.figueroa TGS-REP		
2021-12-03 14:42:08.915939	10.12.3.3	10.12.3.66	KRB5		darin.figueroa TGS-REP		
2021-12-03 14:42:08.9181757	10.12.3.3	10.12.3.66	KRB5		darin.figueroa TGS-REP		
2021-12-03 14:42:08.9183276	10.12.3.3	10.12.3.66	KRB5		darin.figueroa TGS-REP		

```

0000  10 08 36 b9 41 7c 00 4f 49 47 81 3d 08 00 45 00  6 A| O I = E
0010  81 08 d9 5a 40 00 80 06 05 db 0a 0c 03 42 0a 0c  ZB|...B
0020  03 03 cc aa 00 58 03 f2 bd 04 a9 09 04 cc 50 18  ...X...d 1 P
0030  02 01 de c1 09 00 00 01 3a 6a 02 01 30 30 92    ...: 3| 66
0040  01 32 a1 03 02 01 05 a2 03 02 01 0a a3 03 30 61  2|...cBa
0050  30 4c a1 03 02 01 02 a2 45 04 43 30 41 a0 03 02  0L|...E CBA
0060  01 12 a2 3a 04 38 7e 58 12 4e 4b 04 f0 15 0c 30  :| B:P NH| 0
0070  9f 03 bf b9 b9 05 65 c7 f4 d6 bd d7 f5 bd 06 4b  :|e...K
0080  ff 3c 43 20 22 ca dd a7 24 88 0a 33 ae c1 8a fa  -C|...$ 3
0090  0c 5f 72 03 a0 5d 02 b5 c9 0b 01 0a bf 02 30 11  V|...0 0
00a0  a1 04 02 02 00 80 a2 09 04 07 30 05 a0 03 01 01  8|...0 d
00b0  ff 44 01 08 38 81 bd a0 07 03 05 00 40 01 00 19  -|...0
00c0  61 1b 30 19 a0 03 02 01 01 01 12 30 19 10 0e 04  8|...0
00d0  61 72 69 6e 2e 66 69 67 75 65 72 6f 61 a2 0e 1b  arin.figueroa
00e0  0c 46 41 52 47 52 45 45 4e 54 45 43 46 a3 21 30  FARGREE NTECH 1B
00f0  1f a0 03 02 01 02 a1 15 30 1b 06 0b 72 02 74    0 Krb
0100  67 74 1b 0c 46 41 52 47 52 45 45 4e 54 45 43 48  gt_ FARG REENTECH
0110  a5 11 19 0f 32 30 33 37 30 39 31 33 00 52 34 38  -2037 09130248
0120  30 35 5a a0 11 1b 0f 32 30 33 37 30 39 31 33 30  052 2 03709130
0130  32 34 38 30 35 5a a7 06 02 04 56 76 e6 64 a8 15  248052 Vv d
0140  30 13 02 01 12 02 01 11 02 01 17 02 01 18 02 02  0
0150  ff 79 02 01 03 a9 1d 38 1b 36 19 a0 03 02 01 14  y...0
0160  a1 12 04 19 44 45 53 4b 54 4f 50 2d 4c 55 4f 41  DESK TOP-LUOA
0170  42 56 31 20  BV1
  
```

Selanjutnya, kita bisa lanjut mencari user account name dari windows komputer yang infected. Hal ini dapat dilakukan dengan memfilter network traffic yang memiliki protokol KRB5 atau kerberos yang merupakan protokol autentikasi user. Jika kita lihat CNameString valuenya maka kita akan dapat nama user accountnya adalah **darin.figueroa**

2021-12-ISC-Forensic-Challenge.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request and isdp

Time	Source	Destination	Protocol	Length	Host	Info
2021-12-03 14:42:48.410866	10.12.3.66	139.59.6.175	HTTP	234	newsaarctech.com	GET /wp-content/Sx9tvV5/ HTTP/1.1
2021-12-03 14:42:47.664570	10.12.3.66	104.21.29.80	HTTP	245	gamaes.shop	GET /wp-content/plugins/sSTToaEwCG5VASw/ HTTP/1.1

Jika melihat melalui http request ini dan kita mencoba download filenya.

Source	Destination	Protocol	Length	Host	Info
10.12.3.66	139.59.6.175	HTTP	234	newsaarctech.com	GET /wp-content/Sx9tvV5/ HTTP/1.1
10.12.3.66	104.21.29.80	HTTP	245	gamaes.shop	GET /wp-content/plugins/sSTToaEwCG5VASw/ HTTP/1.1

Wireshark - Export - HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
1752	gamaes.shop	text/html	4,334 bytes	sSTToaEwCG5VASw
11107			798 bytes	
11117			1,361 bytes	
11119			1,132 bytes	
11124			1,361 bytes	
11125			1,361 bytes	
11132			1,361 bytes	
11134			1,361 bytes	

Proses download malware hanya berhasil pada hostname gamaes.shop . Mari kita cek filenya lebih lanjut.

← → ↺ https://urlhaus.abuse.ch/browse.php?search=gamaes.shop

For quick access, place your bookmarks here on the bookmarks toolbar: [Manage bookmarks...](#) Other Bookmarks

URLhaus by ABUSE[CH] Browse API Feeds Statistics About

There are **2'702'775** malicious URLs tracked on URLhaus. The queue size is **12**.

Submit a URL

In order to submit a URL to URLhaus, you need to login with your [abuse.ch](#) account

Browse Database

domain, url, md5, sha256, tag:SocGholish, filetype:doc or url_status:online

Search

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2021-12-02 12:09:23	http://gamaes.shop/wp-content/plugins/sSTToaEwC...	Offline	dll emotet epoch4 heodo	waga_tw
2021-12-01 14:10:16	http://gamaes.shop/qss7r/BsfX/	Offline	emotet epoch4 redir-appinstaller	sugimu_sec

Previous Next

© abuse.ch 2023

Disini dari web urlhaus, kita bisa melihat bahwa isi dari file yang di download ini merupakan malware bernama **emotet**.

2021-12-08 (WEDNESDAY) - PCAP FOR AN ISC DIARY (DECEMBER 2021 FORENSIC CHALLENGE)

Questions & Answers

What was the IP address of the infected Windows computer?

10.12.3.66

What was the host name of the infected Windows computer?

DESKTOP-LUOABV1

What was the user account names from the infected Windows computer? (should be "name" not "names")

darin.figueroa

What was the date and time the infection activity began?

Dec 3, 2021 14:42:47.664570000 EST -> sesuai dengan kapan emotet didownload dari gamaes.shop

What was the family of malware that caused this infection.

emotet.