



PCAP CHALLENGE

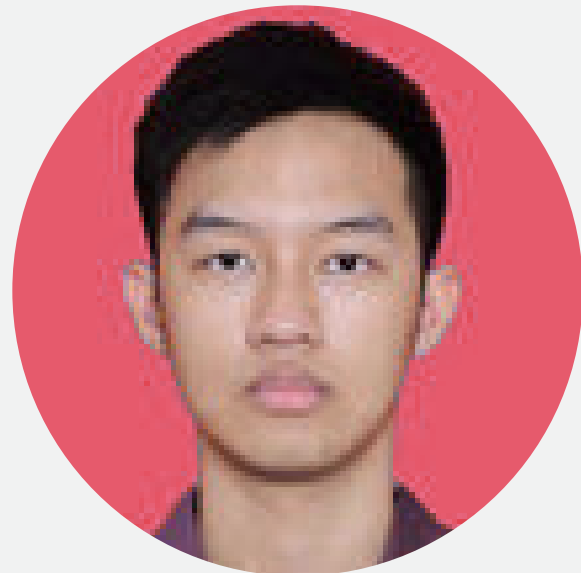


Computer Forensic | PCAP CHALLENGE

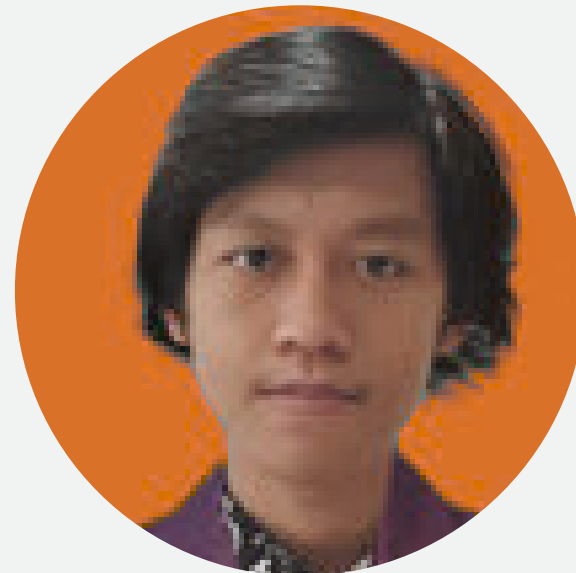
ANGGOTA KELOMPOK



CHRISTINA
2502004235



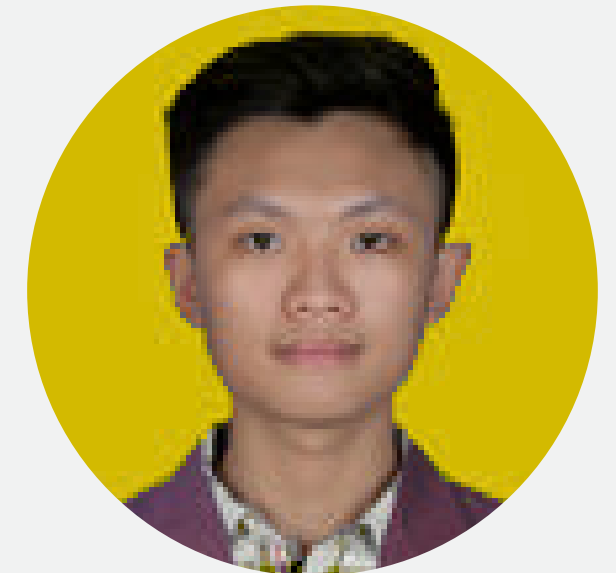
HUGO
2501997016



MADE
2502005723



JONATHAN
2501986611



MAX
2502011360

QUESTION

1. What was the IP address of the infected Windows computer?
2. What was the host name of the infected Windows computer?
3. What was the user account names from the infected Windows computer?
(should be "name" not "names")
4. What was the date and time the infection activity began?
5. What was the family of malware that caused this infection.

WHAT WAS THE IP ADDRESS OF THE INFECTED WINDOWS COMPUTER?

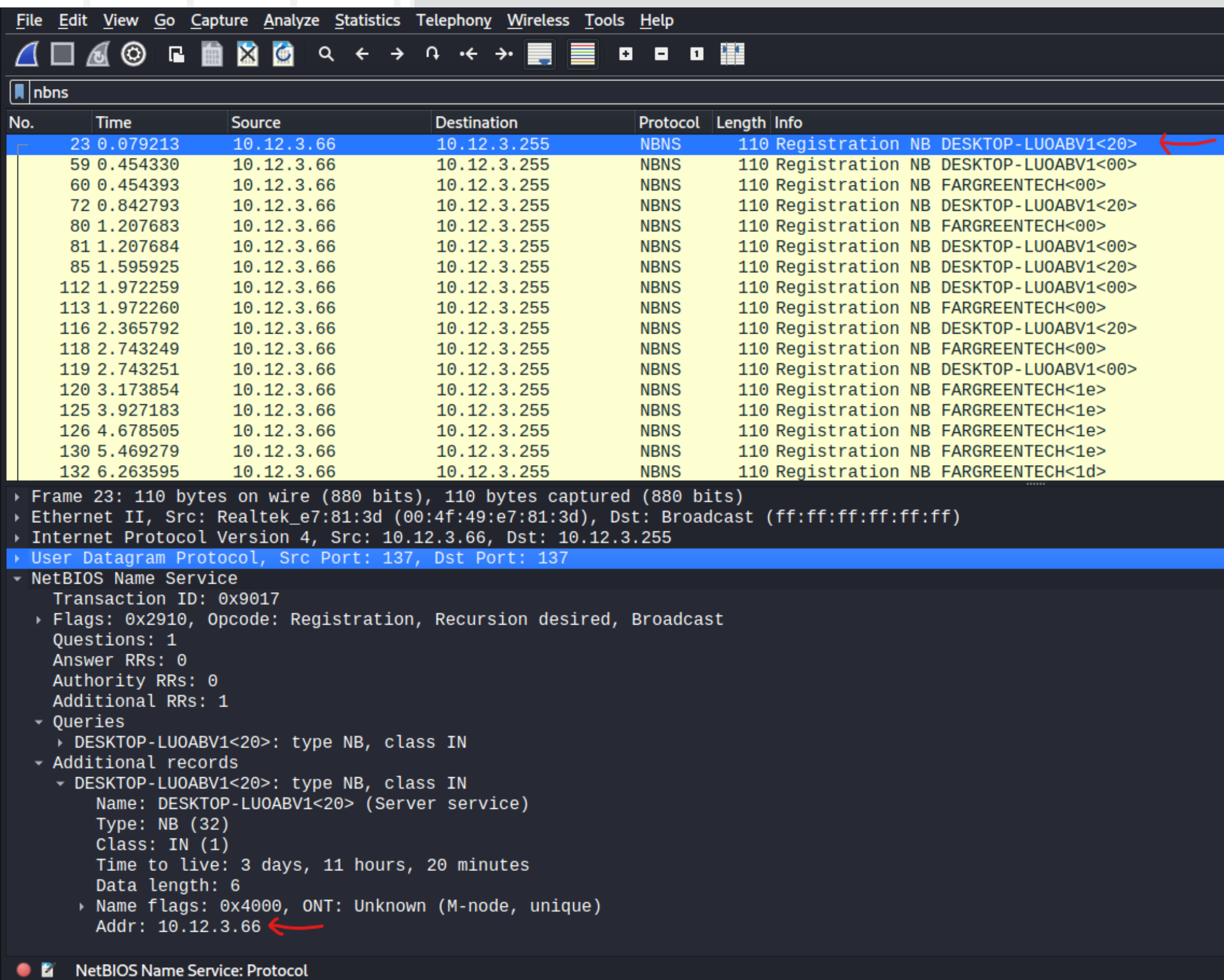
The image shows a Wireshark packet capture of a NetBIOS Name Service (NBNS) registration packet. The packet list on the left shows a series of registration packets from 10.12.3.66 to 10.12.3.255. The selected packet (No. 23) is a registration for 'DESKTOP-LU0ABV1<20>' from source 10.12.3.66 to destination 10.12.3.255. The packet details pane on the right shows the 'User Datagram Protocol' section with source port 137 and destination port 137. The 'NetBIOS Name Service' section shows the transaction ID 0x9017, flags for registration and broadcast, and a list of queries. The first query is for 'DESKTOP-LU0ABV1<20>' with type NB, class IN, and a time to live of 3 days, 11 hours, and 20 minutes. The packet bytes pane on the right shows the raw data of the packet, with the source IP address 10.12.3.66 highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
23	0.079213	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LU0ABV1<20>
59	0.454330	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LU0ABV1<00>
60	0.454393	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<00>
72	0.842793	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LU0ABV1<20>
80	1.207683	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<00>
81	1.207684	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LU0ABV1<00>
85	1.595925	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LU0ABV1<20>
112	1.972259	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LU0ABV1<00>
113	1.972260	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<00>
116	2.365792	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LU0ABV1<20>
118	2.743249	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<00>
119	2.743251	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LU0ABV1<00>
120	3.173854	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<1e>
125	3.927183	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<1e>
126	4.678505	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<1e>
130	5.469279	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<1e>
132	6.263595	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<1d>

Frame 23: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
Ethernet II, Src: Realtek_e7:81:3d (00:4f:49:e7:81:3d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.12.3.66, Dst: 10.12.3.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
Transaction ID: 0x9017
Flags: 0x2910, Opcode: Registration, Recursion desired, Broadcast
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
DESKTOP-LU0ABV1<20>: type NB, class IN
Additional records
DESKTOP-LU0ABV1<20>: type NB, class IN
Name: DESKTOP-LU0ABV1<20> (Server service)
Type: NB (32)
Class: IN (1)
Time to live: 3 days, 11 hours, 20 minutes
Data length: 6
Name flags: 0x4000, ONT: Unknown (M-node, unique)
Addr: 10.12.3.66

- **Answer:** The IP Address of the infected windows computer is “**10.12.3.66**”. You can see in the wireshark, the only windows machine is the IP “10.12.3.66”.

WHAT WAS THE HOST NAME OF THE INFECTED WINDOWS COMPUTER?



No.	Time	Source	Destination	Protocol	Length	Info
23	0.079213	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LUOABV1<20>
59	0.454330	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LUOABV1<00>
60	0.454393	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<00>
72	0.842793	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LUOABV1<20>
80	1.207683	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<00>
81	1.207684	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LUOABV1<00>
85	1.595925	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LUOABV1<20>
112	1.972259	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LUOABV1<00>
113	1.972260	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<00>
116	2.365792	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LUOABV1<20>
118	2.743249	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<00>
119	2.743251	10.12.3.66	10.12.3.255	NBNS	110	Registration NB DESKTOP-LUOABV1<00>
120	3.173854	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<1e>
125	3.927183	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<1e>
126	4.678505	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<1e>
130	5.469279	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<1e>
132	6.263595	10.12.3.66	10.12.3.255	NBNS	110	Registration NB FARGREENTECH<1d>

Frame 23: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: Realtek_e7:81:3d (00:4f:49:e7:81:3d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.12.3.66, Dst: 10.12.3.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
Transaction ID: 0x9017
Flags: 0x2910, Opcode: Registration, Recursion desired, Broadcast
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
DESKTOP-LUOABV1<20>: type NB, class IN
Additional records
DESKTOP-LUOABV1<20>: type NB, class IN
Name: DESKTOP-LUOABV1<20> (Server service)
Type: NB (32)
Class: IN (1)
Time to live: 3 days, 11 hours, 20 minutes
Data length: 6
Name flags: 0x4000, ONT: Unknown (M-node, unique)
Addr: 10.12.3.66

- **Answer:** As from the screenshot in number 1 answer, the IP “10.12.3.66” comes from windows computer called **DESKTOP-LUOABV1**

WHAT WAS THE USER ACCOUNT NAMES FROM THE INFECTED WINDOWS COMPUTER? (SHOULD BE "NAME" NOT "NAMES")

kerberos.CNameString							
No.	Time	Source	Destination	Protocol	Length	CNameString	Info
224	18.627537	10.12.3.66	10.12.3.3	KRB5	292	darin.figueroa	AS-REQ
232	18.635989	10.12.3.66	10.12.3.3	KRB5	372	darin.figueroa	AS-REQ
234	18.637593	10.12.3.3	10.12.3.66	KRB5	387	darin.figueroa	AS-REP
246	18.640973	10.12.3.3	10.12.3.66	KRB5	285	darin.figueroa	TGS-REP
341	18.833789	10.12.3.3	10.12.3.66	KRB5	411	darin.figueroa	TGS-REP
395	18.899607	10.12.3.3	10.12.3.66	KRB5	357	darin.figueroa	TGS-REP
407	18.901126	10.12.3.3	10.12.3.66	KRB5	272	darin.figueroa	TGS-REP

[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (238 bytes)
[PDU Size: 238]
Kerberos
Record Mark: 234 bytes
as-req
pvno: 5
msg-type: krb-as-req (10)
padata: 1 item
req-body
Padding: 0
kdc-options: 40810010
cname
name-type: KRB5-NT-PRINCIPAL (1)
cname-string: 1 item
CNameString: darin.figueroa
realm: FARGREENTECH
sname
till: Sep 12, 2037 22:48:05.000000000 EDT
rtime: Sep 12, 2037 22:48:05.000000000 EDT
CNameString (kerberos.CNameString): 14 bytes

- **Answer:** The infected host name of the infected Windows Computer is **darin.figueroa**. We can see it from the **CNameString**.

WHAT WAS THE DATE AND TIME THE INFECTION ACTIVITY BEGAN?

2021-12-ISC-Forensic-Challenge.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Destination	Host	Destination Port	Info
2021-12-03 15:13:38.207622	185.151.28.85		587	Client Hello
2021-12-03 15:13:39.695835	199.168.117.91		587	Client Hello
2021-12-03 15:13:41.475177	59.157.128.3		587	Client Hello
2021-12-03 15:13:41.917368	186.64.117.195		587	Client Hello
2021-12-03 15:13:57.110924	212.227.17.168		587	Client Hello
2021-12-03 15:14:21.006571	108.177.122.108		587	Client Hello
2021-12-03 15:14:22.216551	213.46.255.64		587	Client Hello
2021-12-03 15:14:31.585556	108.177.122.108		587	Client Hello
2021-12-03 15:14:35.106469	200.63.98.23		587	Client Hello
2021-12-03 15:14:37.360446	207.8.183.5		587	Client Hello
2021-12-03 15:14:52.648184	213.46.255.64		587	Client Hello
2021-12-03 15:14:53.349890	2.207.150.234		587	Client Hello
2021-12-03 15:15:26.548700	106.187.245.203		587	Client Hello
2021-12-03 15:15:27.838221	89.216.47.170		587	Client Hello
2021-12-03 15:15:35.508803	213.165.67.124		587	Client Hello
2021-12-03 15:15:35.882012	195.4.92.213		587	Client Hello
2021-12-03 15:15:40.461696	194.177.200.158		587	Client Hello
2021-12-03 15:15:43.586983	192.185.121.134		587	Client Hello
2021-12-03 15:15:45.828395	118.23.155.30		587	Client Hello
2021-12-03 14:42:47.664570	104.21.29.80	gamaes.shop	80	GET /wp-content/plugins/sSTToaEwCG5VASw/ HTTP/1.1
2021-12-03 14:42:48.410086	139.59.6.175	newsaarctech.com	80	GET /wp-content/Sx9tvV5/ HTTP/1.1

- **Answer:** From the filtered traffic above, there are two unusual HTTP GET from unassociated domain. That means, the infection was began in **2021-12-03 at 14:42:47.**

WHAT WAS THE FAMILY OF MALWARE THAT CAUSED THIS INFECTION?

smtp.data.fragment

Time	Destination	Host	Destination Port	Info
2021-12-03 15:12:19.379697	58.80.137.169		587	from: "Iqra.Malik" <tenpo-kaihatsu3@acoop-ks.c
2021-12-03 15:12:20.237019	58.80.137.169		587	from: "Iqra.Malik" <tenpo-kaihatsu3@acoop-ks.c
2021-12-03 15:12:15.934244	58.80.137.169		587	from: "Kunj Sharma" <tenpo-kaihatsu3@acoop-ks.
2021-12-03 15:12:16.813761	58.80.137.169		587	from: "Kunj Sharma" <tenpo-kaihatsu3@acoop-ks.
2021-12-03 15:12:17.683906	58.80.137.169		587	from: "Kunj Sharma" <tenpo-kaihatsu3@acoop-ks.
2021-12-03 15:12:18.526407	58.80.137.169		587	from: "Kunj Sharma" <tenpo-kaihatsu3@acoop-ks.
2021-12-03 15:13:22.245161	219.99.220.143		587	from: "PHARMACY USA" <nobuyasu-takahashi@tachi
2021-12-03 15:13:23.469801	219.99.220.143		587	from: "PHARMACY USA" <nobuyasu-takahashi@tachi
2021-12-03 15:13:24.713160	219.99.220.143		587	from: "PHARMACY USA" <nobuyasu-takahashi@tachi
2021-12-03 15:13:25.637276	219.99.220.143		587	from: "PHARMACY USA" <nobuyasu-takahashi@tachi
2021-12-03 15:13:26.599015	219.99.220.143		587	from: "PHARMACY USA" <nobuyasu-takahashi@tachi
2021-12-03 15:13:27.525261	219.99.220.143		587	from: "PHARMACY USA" <nobuyasu-takahashi@tachi
2021-12-03 15:13:19.980659	219.99.220.143		587	from: "PHARMACY_Rx____" <nobuyasu-takahashi@tac
2021-12-03 15:12:21.082544	58.80.137.169		587	from: "R GOPAKUMAR" <tenpo-kaihatsu3@acoop-ks.
2021-12-03 15:12:21.975427	58.80.137.169		587	from: "Rashmi" <tenpo-kaihatsu3@acoop-ks.co.jp
2021-12-03 15:13:21.230161	219.99.220.143		587	from: "Rosangela Matoso" <nobuyasu-takahashi@t
2021-12-03 15:15:46.249581	190.81.124.11		25	from: "Viagra_Rx____" <elena.chavez@xertekcorp



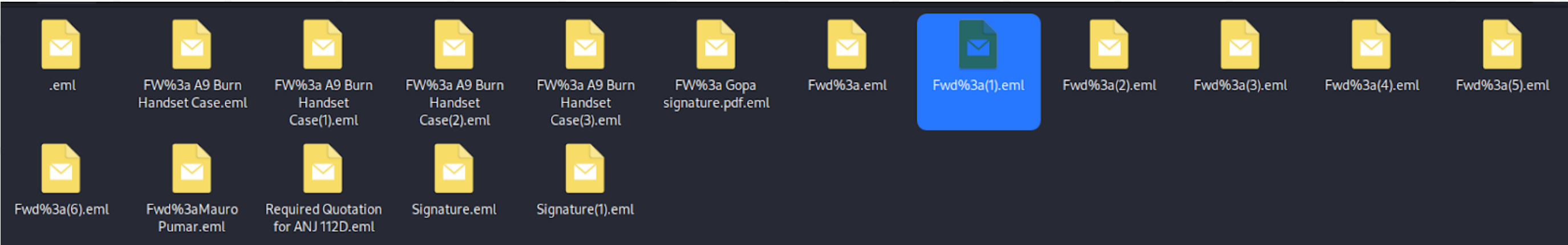
WHAT WAS THE FAMILY OF MALWARE THAT CAUSED THIS INFECTION?

Wireshark · Export · IMF object list

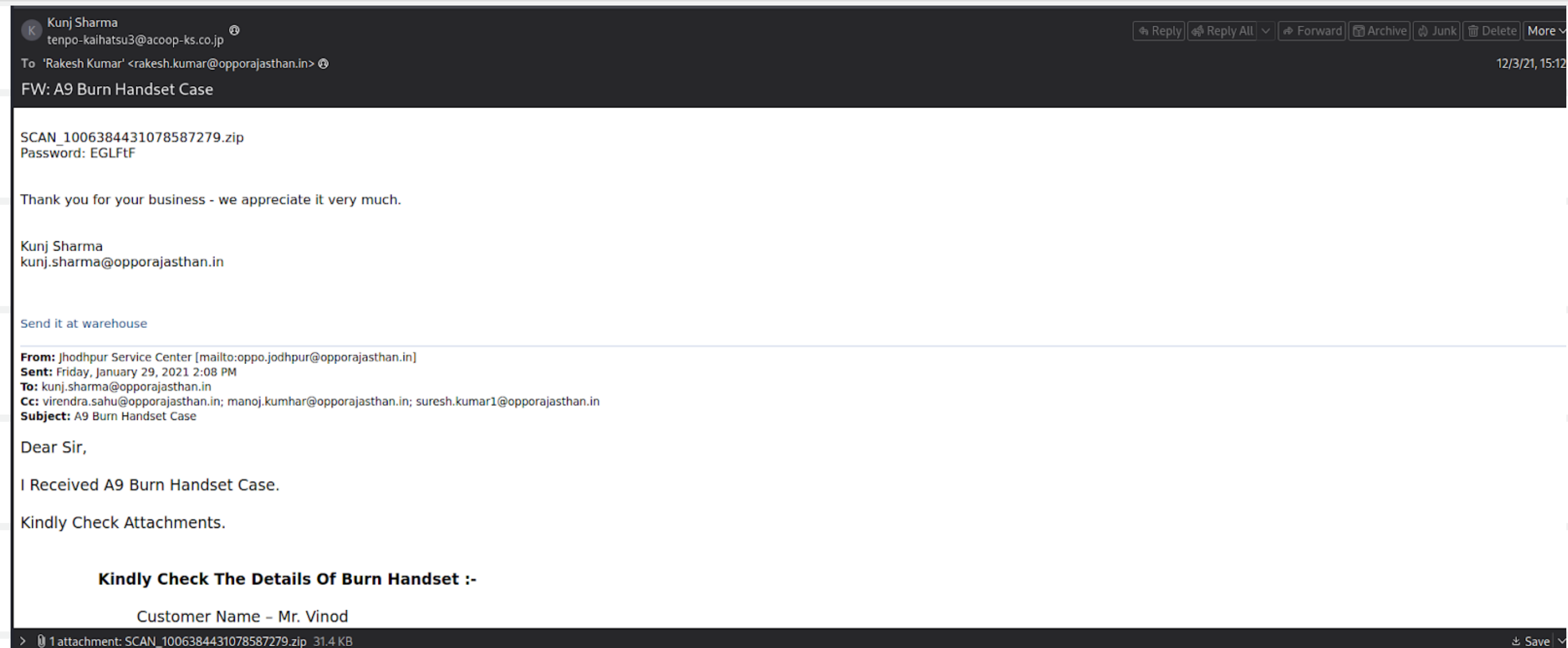
Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
24879	tenpo-kaihatsu3@acoop-ks.co.jp	EML file	59 kB	FW: A9 Burn Handset Cas
25106	tenpo-kaihatsu3@acoop-ks.co.jp	EML file	59 kB	FW: A9 Burn Handset Cas
25267	tenpo-kaihatsu3@acoop-ks.co.jp	EML file	59 kB	FW: A9 Burn Handset Cas
25398	tenpo-kaihatsu3@acoop-ks.co.jp	EML file	59 kB	FW: A9 Burn Handset Cas
25540	tenpo-kaihatsu3@acoop-ks.co.jp	EML file	62 kB	Signature.eml
25707	tenpo-kaihatsu3@acoop-ks.co.jp	EML file	62 kB	Signature.eml
25897	tenpo-kaihatsu3@acoop-ks.co.jp	EML file	48 kB	FW: Gopa signature.pdf.e
26336	tenpo-kaihatsu3@acoop-ks.co.jp	EML file	55 kB	Required Quotation for Al
39380	nobuyasu-takahashi@tachikawahouse.co.jp	EML file	53 kB	Fwd:.eml
40384	nobuyasu-takahashi@tachikawahouse.co.jp	EML file	53 kB	Fwd:Mauro Pumar.eml
41229	nobuyasu-takahashi@tachikawahouse.co.jp	EML file	53 kB	Fwd:.eml
42099	nobuyasu-takahashi@tachikawahouse.co.jp	EML file	53 kB	Fwd:.eml
43097	nobuyasu-takahashi@tachikawahouse.co.jp	EML file	53 kB	Fwd:.eml
43472	nobuyasu-takahashi@tachikawahouse.co.jp	EML file	53 kB	Fwd:.eml
43711	nobuyasu-takahashi@tachikawahouse.co.jp	EML file	53 kB	Fwd:.eml
43871	nobuyasu-takahashi@tachikawahouse.co.jp	EML file	53 kB	Fwd:.eml
55380	elena.chavez@xertekcorp.com	EML file	53 kB	.eml

Save Save All Preview Close Help



WHAT WAS THE FAMILY OF MALWARE THAT CAUSED THIS INFECTION?



Answer: If we look at the contents of the email sent, we can see that Windows Computer sent spam emails to many people with various contents. This PC is infected with spam robots which can be seen from the PC's unusual behavior (sending spam emails to many people). And from the traffic we saw from the previous question, the malware family that caused this infection was **Emotet**.



THANK YOU