Title: Group Network Challenge 1

Group/Name: Marty Schneider

Indicators and Technical Details

Include all relevant technical details and indicators regarding your investigation that pertains to your analysis, findings, and summary statements.

Datetime	Identifier (IP, Domain, URL, Hostname)	MITRE Technique ID	Analyst Comment
Feb 23, 2022 18:24:34.594654000 UTC	64.34.171.228		Host IP where first host was infected from
	172.16.0.131, 2c:27:d7:d2:06:f5, DESKTOP-VD151O7		First host infected (tricia.becker)
	172.16.0.170, 00:12:f0:64:d1:d9, DESKTOP-W5TFTQY		Second host infected (everett.french)
	172.16.0.149, 00:1b:fc:7b:d1:c0, DESKTOP-KPQ9FDB		Third host infected (nick.montgomery)
Feb 23, 2022 18:24:35.465005000 UTC	2mIaAtxprmXlTLZeFjkIqbexiFXkZkJ.dll		File downloaded from malicious domain
Feb 23, 2022 18:24:43.773918000 UTC	135.148.121.246		Malware C2
Feb 23, 2022 18:29:19.507652000 UTC	Ocklqc.jpg		File downloaded by 3rd infected host through HTTP GET

Executive Summary

Explain your analysis and findings to an executive member of the organizations. Focus on risk, compliance, and actions that a decision maker should weigh when reviewing your analysis and findings. Avoid technical details that do not improve the narrative that you wish to convey.

Technical Summary

Provide a technical summary to include relevant technical details that articulates your analysis and findings as if you were communicating with another analyst, colleague, or direct manager. Be concise yet descriptive in what you are doing and what was identified within the analysis.

Findings and Analysis

Question 1: What is the IP address, MAC address, and host name of the Windows host associated with user account tricia.becker? (answer in the format IP, MAC, HOSTNAME)

My answer is 172.16.0.131, 2c:27:d7:d2:06:f5, DESKTOP-VD151O7\

```
Source Address: DESKTOP-VD151O7.sunnystation.com (172.16.0.131)
Destination Address: sunnystation-dc.sunnystation.com (172.16.0.52)
[Stream index: 4]
ansmission Control Protocol, Src Port: 49187, Dst Port: 88, Seq: 1,
beros
Record Mark: 233 bytes
as-req
   pvno: 5
   msg-type: krb-as-req (10)
 > padata: 1 item
 v req-body
      Padding: 0
    > kdc-options: 40810010
    v cname
         name-type: kRB5-NT-PRINCIPAL (1)
       v cname-string: 1 item
            CNameString: tricia.becker
      realm: SUNNYSTATION
    > sname
      till: Sep 13, 2037 02:48:05.000000000 Coordinated Universal Ti
      rtime: Sep 13, 2037 02:48:05.000000000 Coordinated Universal T
      nonce: 1816792207
    > etype: 6 items
    v addresses: 1 item DESKTOP-VD151O7<20>
       > HostAddress DESKTOP-VD151O7<20>
```

Question 2: What is the IP address, MAC address, and host name of the Windows host associated with user account everett.french? (answer in the format IP, MAC, HOSTNAME)

Answer: 172.16.0.170, 00:12:f0:64:d1:d9, DESKTOP-W5TFTQY

```
Source Address: DESKTOP-W5TFTQY.sunnystation.com (172.16.0.170)
Destination Address: sunnystation-dc.sunnystation.com (172.16.0.52)
[Stream index: 11]
ansmission Control Protocol, Src Port: 54047, Dst Port: 88, Seq: 1,
beros
Record Mark: 234 bytes
as-req
   pvno: 5
   msg-type: krb-as-req (10)
 > padata: 1 item
 v req-body
      Padding: 0
    > kdc-options: 40810010
    v cname
         name-type: kRB5-NT-PRINCIPAL (1)
       v cname-string: 1 item
            CNameString: everett.french
      realm: SUNNYSTATION
    > sname
      till: Sep 13, 2037 02:48:05.000000000 Coordinated Universal T
      rtime: Sep 13, 2037 02:48:05.000000000 Coordinated Universal
      nonce: 1778030854
    > etype: 6 items
    v addresses: 1 item DESKTOP-W5TFTQY<20>
       > HostAddress DESKTOP-W5TFTQY<20>
```

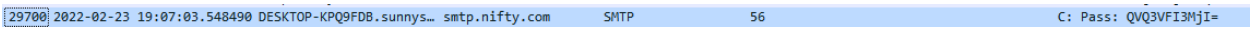
Question 3: What is the IP address, MAC address, and host name of the Windows host associated with user account nick.montgomery? (answer in the format IP, MAC, HOSTNAME)

Answer: 172.16.0.149, 00:1b:fc:7b:d1:c0, DESKTOP-KPQ9FDB

```
Source Address: DESKTOP-KPQ9FDB.sunnystation.com (172.16.0.149)
Destination Address: sunnystation-dc.sunnystation.com (172.16.0.52)
[Stream index: 25]
ansmission Control Protocol, Src Port: 49710, Dst Port: 88, Seq: 1, A
rberos
Record Mark: 235 bytes
as-req
   pvno: 5
   msg-type: krb-as-req (10)
 > padata: 1 item
 v req-body
      Padding: 0
    > kdc-options: 40810010
    v cname
         name-type: kRB5-NT-PRINCIPAL (1)
       v cname-string: 1 item
            CNameString: nick.montgomery
      realm: SUNNYSTATION
    > sname
      till: Sep 13, 2037 02:48:05.000000000 Coordinated Universal Ti
      rtime: Sep 13, 2037 02:48:05.000000000 Coordinated Universal T
      nonce: 2120916058
    > etype: 6 items
    v addresses: 1 item DESKTOP-KPQ9FDB<20>
       > HostAddress DESKTOP-KPQ9FDB<20>
```

Question 4: Over what protocol were compromised credentials sent in the clear from the host under suspicion?

Answer: smtp



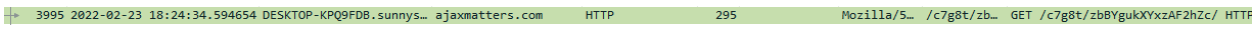
Question 5: What is the Subject of the email message sent from the host to conniebanner28[@]yahoo.com?

Answer: Subject: Farmers Union Oil Company of Kenmare

```
Date: Wed, 23 Feb 2022 19:07:05 +0000
From: "kenmarefarmersunion.com" <hrd5_hr@idn-ltd.com>
To: "" <conniebanner28@yahoo.com>
Subject: Farmers Union Oil Company of Kenmare
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_NextPart
```

Question 6: What malicious domain marks the earliest sign of compromise of the infected host?

Answer: ajaxmatters.com



Question 7: What is the file name of the DLL downloaded from that domain? (hint: there's a streamlined way to get this!)

Answer: 2mIaAtxprmXlTLZeFjkIqbexiFXkZkJ.dll

```
GET /c7g8t/zbBYgukXYxzAF2hZc/ HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: www.ajaxmatters.com
Connection: Keep-Alive


HTTP/1.1 200 OK
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Type: application/x-msdownload
Expires: Wed, 23 Feb 2022 18:24:34 GMT
Last-Modified: Wed, 23 Feb 2022 18:24:34 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/7.4.19
Set-Cookie: 62167be2a94a3=1645640674; expires=Wed, 23-Feb-2022 18:25:34 GMT; Max-Age=60; path=/
Content-Disposition: attachment; filename="2mIaAtxprmXlTLZeFjkIqbexiFXkZkJ.dll"
Content-Transfer-Encoding: binary
```

Question 8: What is the SHA-256 hash of that DLL?

Answer: 14B57211308AC8AD2A63C965783D9BA1C2D1930D0CAFD884374D143A481F9BF3

Question 9: Following the download, what IP does the infected host communicate with over an uncommon port?

Answer: 135.148.121.246, port 8080

```
    Destination Address: vps-d2049773.vps.ovh.us (135.148.121.246)
    [Stream index: 51]
Transmission Control Protocol, Src Port: 49748, Dst Port: 8080, Seq: 0, Len: 0
```

Question 10: What is the IP of the server the second infected host downloaded the payload from? (as you might've guessed, you won't find the payload itself)

Answer: 178.211.56.194

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets
172.16.0.170	54074	178.211.56.194	443	94	122 kB	199	1,469
172.16.0.149	49783	144.217.88.125	443	40	48 kB	254	781

Question 11: What is the JA3S hash of the server response during TLS negotiation? (hint: the server says "hello")

Answer: 9d9ce860f1b1cbef07b019450cb368d8

```
> Extension: extended_master_secret (len=0)
  [JA3S Fullstring: 771,49200,65281-11-35-23]
  [JA3S: ec74a5c51106f0419184d0dd08fb05bc]
```

Question 12: What malware family infected both of the hosts referenced above?

Answer: emotet

Question 13: What is the filename of the DLL downloaded with its bytes in reverse order?

Answer: Ocklqc.jpg

```
Internet Protocol Version 4, Src: DESKTOP-VD15107.sunnystation.com (172.16.0.131),
Transmission Control Protocol, Src Port: 49200, Dst Port: 80, Seq: 1, Ack: 1, Len:
Hypertext Transfer Protocol
> GET /Ocklqc.jpg HTTP/1.1\r\n
  Host: 156.96.154.210\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Response in frame: 10384]
  [Full request URI: http://156.96.154.210/Ocklqc.jpg]
```

Question 14: What is the URI path that consistently appears in the infection traffic following that download?

Answer: /uar3

Request URI	Info
	Standard query 0x06f6 A www.
	Standard query response 0x06
	Name query NB WWW.KRPANO.PRO
	Refresh NB DESKTOP-VD15107<2
	Name query NB WWW.KRPANO.PRO
	Name query NB WWW.KRPANO.PRO
	Name query NB WWW.KRPANO.PRO
	Name query NB WWW.KRPANO.PRO
	Name query NB WWW.KRPANO.PRO
	Standard query 0xe68d A www.
	Standard query response 0xe6
	49201 → 80 [SYN] Seq=0 Win=8
	80 → 49201 [SYN, ACK] Seq=0
	49201 → 80 [ACK] Seq=1 Ack=1
/uar3/?OX…	GET /uar3/?OXtd9L=cFNTMFX8k4
	80 → 49201 [ACK] Seq=1 Ack=1
	80 → 49201 [PSH, ACK] Seq=1
	80 → 49201 [PSH, ACK] Seq=13
	80 → 49201 [PSH, ACK] Seq=27
	80 → 49201 [ACK] Seq=4165 Ac
/uar3/?OX…	HTTP/1.1 403 Forbidden (tex
	49201 → 80 [RST, ACK] Seq=19
	Standard query 0x1d4c A www.
	Standard query response 0x1c
	49202 → 80 [SYN] Seq=0 Win=8
	80 → 49202 [SYN, ACK] Seq=0
	49202 → 80 [ACK] Seq=1 Ack=1
/uar3/?WN…	GET /uar3/?WN68=wVxHuY5BHg7y
	80 → 49202 [ACK] Seq=1 Ack=2
/uar3/?WN…	HTTP/1.1 302 Found
	49202 → 80 [ACK] Seq=202 Ack
	49202 → 80 [FIN, ACK] Seq=20
	80 → 49202 [ACK] Seq=218 Ack
	Refresh NB DESKTOP-W5TFTQY<2
	Refresh NB DESKTOP-W5TFTQY<2
	Who has 172.16.0.131? Tell 1
	172.16.0.131 is at 2c:27:d7:
	Standard query 0x384c A www.

Question 15: What is the SHA-256 hash of the reversed DLL file?

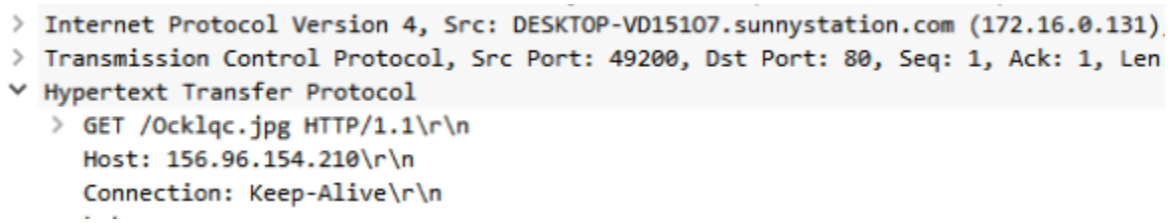
Answer: 2620bf96201e9f328aee98a74ce5b87f221e761a8b2662974b35f90991404337

Question 16: What is the malware family of that DLL?

Answer: xloader

Question 17: What is the IP address of the host it infected?

Answer: 172.16.0.131



Remediation and Recommendations