2018-02-13 TRAFFIC ANALYSIS EXERCISE: ANSWERS

"OFFICE WORK"

https://www.malware-traffic-analysis.net/2018/02/13/2018-02-13-traffic-analysis-exercise.pcap.zip

The zip file is password-protected with the standard password. See the "about" page of my site if you don't know it.

YOUR TASK:

Review the pcap, and document the following:

- Date and time of the malicious activity in UTC (GMT).
- IP address of the affected Windows host.
- Mac address of the affected Windows host.
- Host name of the affected Windows host.
- User account name on the affected Windows host.
- What malware might be involved.

ANSWERS:

- Date/Time: 2018-02-13 at approximately 05:06 UTC
- IP address: 10.23.1.205
- Mac address: 00:16:17:f9:42:e5 (Msi_f9:42:e5)
- Host name: REGINALD-PC
- User account name: reginald.farnsworth
- What malware might be involved: DarkComet RAT

DETAILS

As always, I recommend you set up Wireshark according to the tutorials I've documented at:

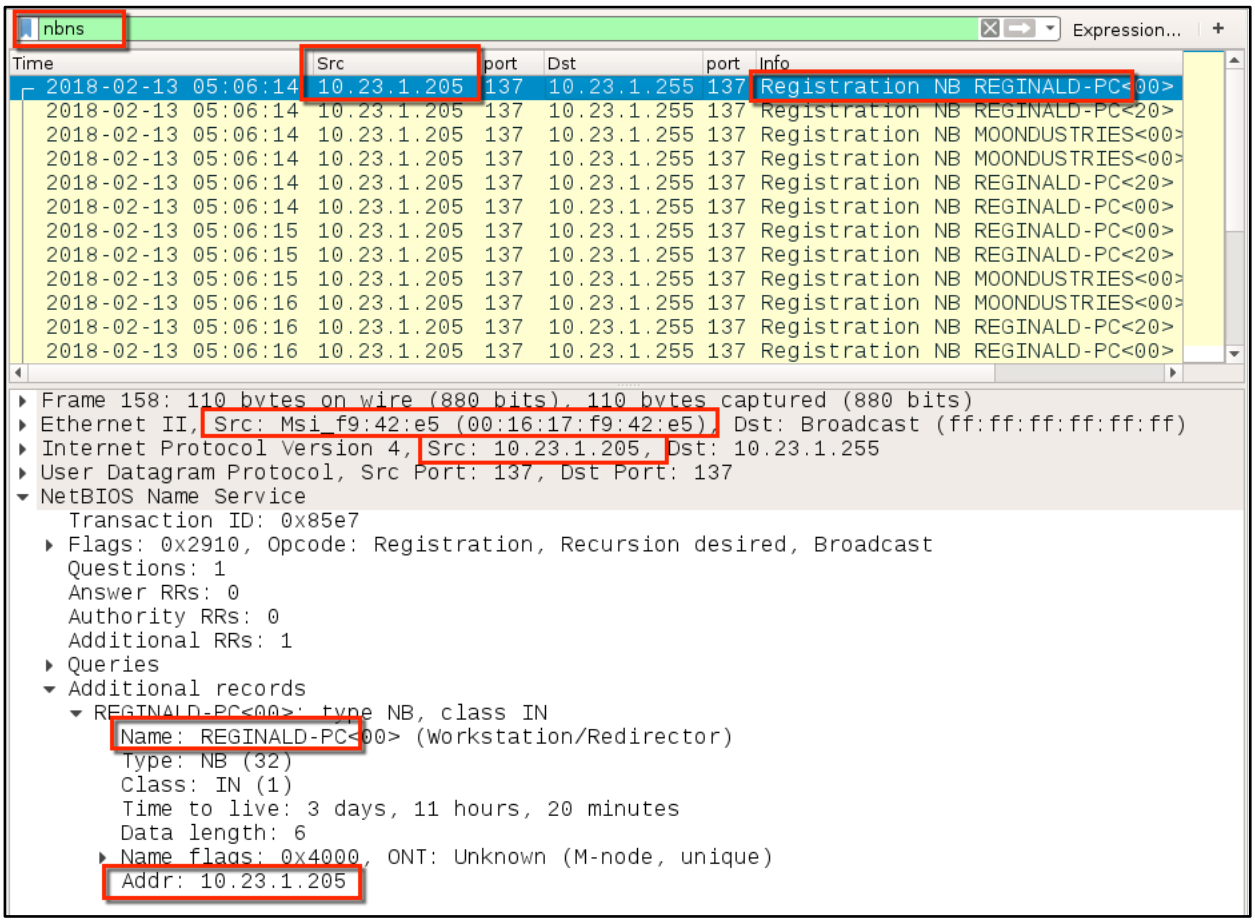
- http://malware-traffic-analysis.net/tutorials/index.html

User account ***reginald.farnsworth*** logged into his Windows client ***REGINALD-PC*** through a domain controller for ***moondustries.com***. The associated IP addresses are:

- Windows client (REGINALD-PC): 10.23.1.205
- Domain controller for moondustries.com: 10.23.1.7
- Broadcast address for this LAN segment: 10.23.1.255
- Gateway for this LAN segment: 10.23.1.1

2018-02-13 TRAFFIC ANALYSIS EXERCISE: ANSWERS

For Reginald's IP address, Mac address, and host name, filter on ***nbns*** and find your answers as shown in the image below:



The user account name can be found through Kerberos traffic generated when Reginald logged into his Windows client. To find the user account name, use the following Wireshark filter:

> ***kerberos.cname_element and kerberos.KerberosString and !(kerberos.KerberosString contains $)***

or use:

> ***kerberos.CNameString and !(kerberos.CNameString contains $)***

The first one works in Wireshark version 1.12, and the second one works in Wireshark 2.2 and later.

In the results, work your way down to the ***cname*** field and find the user account name as shown below:

```
kerberos.CNameString and !(kerberos.CNameString contains $)        Expression...  +

Time                  Src          port  Dst          port  Info
2018-02-13 05:06:50   10.23.1.205  49181 10.23.1.7    88    AS-REQ
2018-02-13 05:06:50   10.23.1.205  49182 10.23.1.7    88    AS-REQ
2018-02-13 05:06:50   10.23.1.7    88    10.23.1.205  49182 AS-REP
2018-02-13 05:06:50   10.23.1.7    88    10.23.1.205  49183 TGS-REP
2018-02-13 05:06:50   10.23.1.7    88    10.23.1.205  49185 TGS-REP
2018-02-13 05:06:51   10.23.1.7    88    10.23.1.205  49187 TGS-REP
2018-02-13 05:06:51   10.23.1.7    88    10.23.1.205  49190 TGS-REP
2018-02-13 05:06:51   10.23.1.7    88    10.23.1.205  49191 TGS-REP

▸ Frame 367: 297 bytes on wire (2376 bits), 297 bytes captured (2376 bits
▸ Ethernet II, Src: Msi_f9:42:e5 (00:16:17:f9:42:e5), Dst: Dell_53:d4:4b
▸ Internet Protocol Version 4, Src: 10.23.1.205, Dst: 10.23.1.7
▸ Transmission Control Protocol, Src Port: 49181, Dst Port: 88, Seq: 1, A
▾ Kerberos
  ▸ Record Mark: 239 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▸ padata: 1 item
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010 (forwardable, renewable, canonicalize, rene
      ▾ cname
          name-type: kRB5-NT-PRINCIPAL (1)
        ▾ cname-string: 1 item
            CNameString: reginald.farnsworth
        realm: MOONDUSTRIES
      ▸ sname
```

How can we find out the alerts? We can check the pcap on VirusTotal and PacketTotal. Both show alerts for the DarkComet RAT.

In the VirusTotal analysis of the pcap, you'll find alerts for DarkComet RAT under both the Snort and the Suricata alerts in the "File detail" section.

- https://www.virustotal.com/en/file/88413b71e5e2836f8686b3390c2d802d1a0c3de33b510bcfd1adc2b18ff07eb3/analysis/

PacketTotal analysis of the pcap also shows several alerts for DarkComet on traffic to 185.86.151.37 over TCP port 2200:

- https://packettotal.com/app/analysis?id=6f4a5f6d7b3c4af88577fa79f8aa105d

And I always check these pcaps in my lab environment using Security Onion and the Emerging Threats Pro (ETPRO) ruleset.

2018-02-13 TRAFFIC ANALYSIS EXERCISE: ANSWERS

The following alerts from the ETPRO ruleset triggered on my Security Onion setup from the post-infection traffic:

- ***ETPRO TROJAN DarkComent-RAT init connection 2***
- ***ETPRO TROJAN DarkComent-RAT server join acknowledgement 2***
- ***ETPRO TROJAN DarkComent-RAT activity***
- ***ET TROJAN Backdoor.Win32.DarkComent Screenshot Upload Successful***
- ***ETPRO TROJAN Backdoor.Win32.DarkKomet Keep-Alive***

See the next two images for details.

RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	3	2018-02-13...	185.86.151.37	2200	10.23.1.205	49212	6	ETPRO TROJAN DarkComet-RAT init connection 2
RT	1	2018-02-13...	10.23.1.205	49212	185.86.151.37	2200	6	ETPRO TROJAN DarkComet-RAT server join acknowledgement 2
RT	12	2018-02-13...	10.23.1.205	49212	185.86.151.37	2200	6	ETPRO TROJAN DarkComet-RAT activity
RT	23	2018-02-13...	10.23.1.205	49213	185.86.151.37	2200	6	ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful
RT	2	2018-02-13...	10.23.1.205	49212	185.86.151.37	2200	6	ETPRO TROJAN Backdoor.Win32.DarkKomet Keep-Alive

Shown above: Alerts seen using the ETPRO ruleset in Security Onion on Sguil using Suricata.

tcp.flags eq 0x0002 and ip.addr eq 185.86.151.37 Expression... +

Time	Src	port	Dst	port	Info
2018-02-13 05:07:43	10.23.1.205	49212	185.86.151.37	2200	49212 → 2200
2018-02-13 05:08:14	10.23.1.205	49213	185.86.151.37	2200	49213 → 2200
2018-02-13 05:08:16	10.23.1.205	49214	185.86.151.37	2200	49214 → 2200

Shown above: You'll find three TCP streams using the Wireshark filter ***tcp.flags eq 0x0002 and ip.addr eq 185.86.151.37***

Follow any one of the TCP streams shown in the above image, and you'll see what DarkComet traffic looks like. (See next page for an image).

tcp.stream eq 54 Expression... +

Time	Src	port	Dst	port	Info
2018-02-13 05:07:43	10.23.1.205	49212	185.86.151.37	2200	49212 →
2018-02-13 05:07:43	185.86.151…	2200	10.23.1.205	49212	2200 →
2018-02-13 05:07:43	10.23.1.205	49212	185.86.151.37	2200	49212 →
2018-02-13 05:07:43	185.86.151…	2200	10.23.1.205	49212	2200 →
2018-02-13 05:07:43	10.23.1.205	49212	185.86.151.37	2200	49212 →

Wireshark · Follow TCP Stream (tcp.stream eq 54) · 2018-02-13-traffic-analysis-exercise

```
BF7CAB464EFBA57DAD495BECB15D8B4C57F0BE8A00F8192DECDD3505C7F43A8CFAF9201
A3C4EDD496A9F5699707BCDCEDF47A24E6FBB926E4DD8FD3E94B4FD270D394FC74B6DF5
FBED4F702D5AAAF4BFF85FFC4C6D5919BBB60BDD7ECFE6CCA9478CD6DED839D5018C675
B5012DAE8D7C31473DED4ACB5D8C96816B4189E5EB3CF663BE5B622541F57C23234E390
2DDC5BFDE23613CB9715CF9CF1EA0D7905F228A31137D0A3AE4D1A07173161D00B968D0
3226C56F5D0BE9355212061305F16687561B374BB3DD5E4CE5AE3088A7FBAA651D1925E
A870FF31D806E76CF8E2E18DF430887A9161FE2080F35A47749B32648589E802FB91850
A9D9BF54DEF863764CCE747F99D2ABC8501A5E5796A4C409EAB4C6C642ED9B785175710
C0A426AD53661E8AE03DC92DD4D9C20EC5F394178970E7C0FF71E105EEC7C7CEA7A642F
E1DD1370E8991F531F77E425FFCC826BF6AE1EEB9E06C97350B4183D573BA5A4EFFC3FB
629308B17DAB5251F0C6E67B8478A47DAC5251F0CBF772977E518BD34E7EA78C5EF5D4E
D3C674628B9361C9AF2CF65654A2ADC93CFEE20B73B311C54EFA17AD47EC3F7CEBB5794
F6D0B322D8069E7B533C1BA8E1F5E9B27DAC544AF1DFF175867F488DB6370495F43A8AF
AFD6813734B954A218792913F675D3AE4E8BDFA53BB77B14C57E4CA824CE6532DA7C3D5
73BA5A4EFFC3FB629308D573BA5A4EFFC3FB629308A56CB04F5AFBDCF960997B2FECC73
7D573BA5A4EFFC3FB629308D573BA5A4EFFC3FB629308D573BA5A4EFFC3FB629308D573
BA5A4EFFC3FB629308D573BA5A4EFFC3FB629308D573BA5A4EFFC3FB629308D573BA5A4
EFFC3FB629308D573BA5A4EFFC3FB629308D573BA5A4EFFC3FB629308
```

Shown above: A TCP stream of DarkComent RAT traffic from this infection.