2. Icemaiden

(2019-12-03)

2-1. 구성 환경

구성 환경

LAN segment range: 10.18.20.0/24 (10.18.20.0 through 10.18.20.255)

Domain: icemaiden.com

Domain controller: 10.18.20.08 - Icemaiden-DC

LAN segment gateway: 10.18.20.1

LAN segment broadcast address: 10.18.20.255

2-2. 문제 및 해답

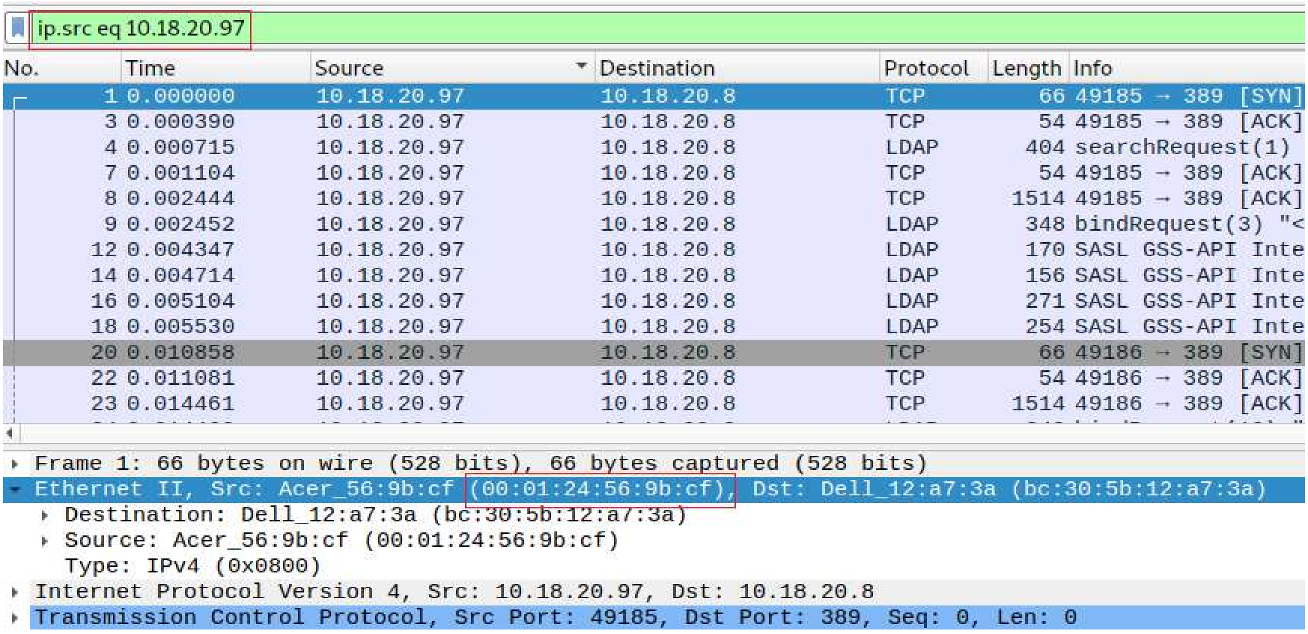
문제 및 해답

Q. What is the IP address, MAC address, and host name of the infected Windows host?

: 10.18.20.97, 00:01:24:56:9b:cf, JUANITA-WORK-PC

Q. What is the Windows user account name of the victim on this infected Windows host?

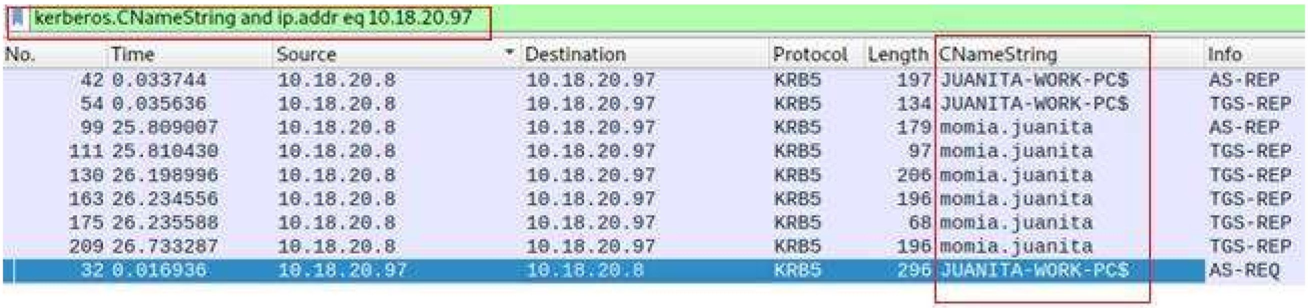
: momia.juanita



```
ip.src eq 10.18.20.97

No.   Time        Source         Destination    Protocol  Length Info
    1 0.000000    10.18.20.97    10.18.20.8     TCP           66 49185 → 389 [SYN]
    3 0.000390    10.18.20.97    10.18.20.8     TCP           54 49185 → 389 [ACK]
    4 0.000715    10.18.20.97    10.18.20.8     LDAP         404 searchRequest(1)
    7 0.001104    10.18.20.97    10.18.20.8     TCP           54 49185 → 389 [ACK]
    8 0.002444    10.18.20.97    10.18.20.8     TCP         1514 49185 → 389 [ACK]
    9 0.002452    10.18.20.97    10.18.20.8     LDAP         348 bindRequest(3) "<
   12 0.004347    10.18.20.97    10.18.20.8     LDAP         170 SASL GSS-API Inte
   14 0.004714    10.18.20.97    10.18.20.8     LDAP         156 SASL GSS-API Inte
   16 0.005104    10.18.20.97    10.18.20.8     LDAP         271 SASL GSS-API Inte
   18 0.005530    10.18.20.97    10.18.20.8     LDAP         254 SASL GSS-API Inte
   20 0.010858    10.18.20.97    10.18.20.8     TCP           66 49186 → 389 [SYN]
   22 0.011081    10.18.20.97    10.18.20.8     TCP           54 49186 → 389 [ACK]
   23 0.014461    10.18.20.97    10.18.20.8     TCP         1514 49186 → 389 [ACK]

▸ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▾ Ethernet II, Src: Acer_56:9b:cf (00:01:24:56:9b:cf), Dst: Dell_12:a7:3a (bc:30:5b:12:a7:3a)
  ▸ Destination: Dell_12:a7:3a (bc:30:5b:12:a7:3a)
  ▸ Source: Acer_56:9b:cf (00:01:24:56:9b:cf)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.18.20.97, Dst: 10.18.20.8
▸ Transmission Control Protocol, Src Port: 49185, Dst Port: 389, Seq: 0, Len: 0
```

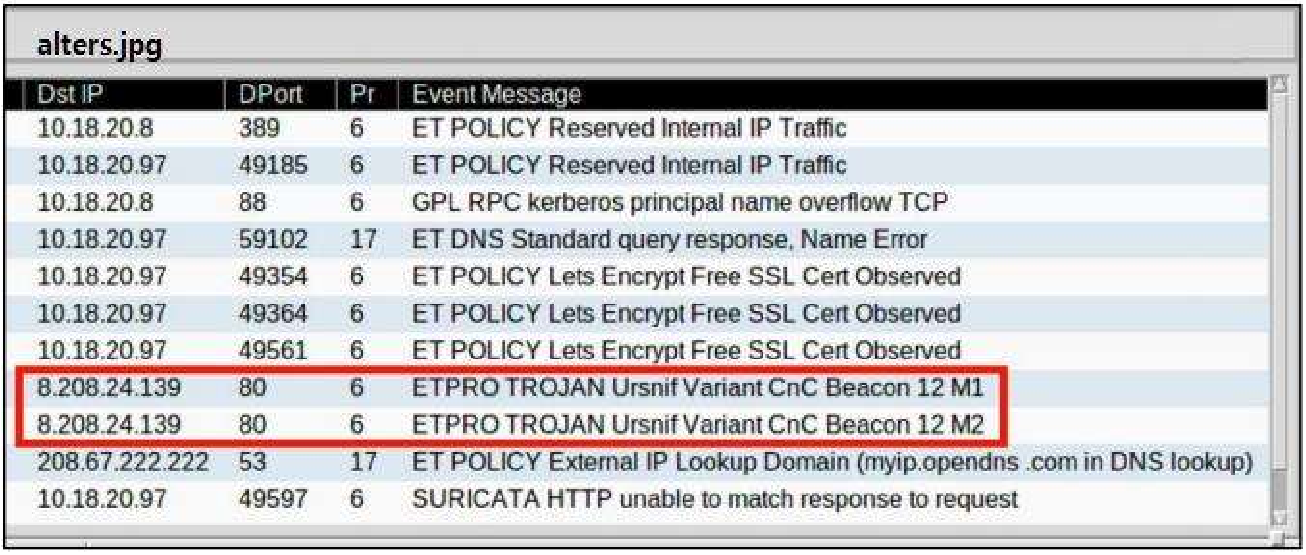


```
kerberos.CNameString and ip.addr eq 10.18.20.97

No.   Time        Source         Destination    Protocol  Length CNameString       Info
   42 0.033744    10.18.20.8     10.18.20.97    KRB5         197 JUANITA-WORK-PC$  AS-REP
   54 0.035636    10.18.20.8     10.18.20.97    KRB5         134 JUANITA-WORK-PC$  TGS-REP
   99 25.809007   10.18.20.8     10.18.20.97    KRB5         179 momia.juanita     AS-REP
  111 25.810430   10.18.20.8     10.18.20.97    KRB5          97 momia.juanita     TGS-REP
  130 26.198996   10.18.20.8     10.18.20.97    KRB5         206 momia.juanita     TGS-REP
  163 26.234556   10.18.20.8     10.18.20.97    KRB5         196 momia.juanita     TGS-REP
  175 26.235588   10.18.20.8     10.18.20.97    KRB5          68 momia.juanita     TGS-REP
  209 26.733287   10.18.20.8     10.18.20.97    KRB5         196 momia.juanita     TGS-REP
   32 0.016936    10.18.20.97    10.18.20.8     KRB5         296 JUANITA-WORK-PC$  AS-REQ
```

Q. What type of malware was the victim infected with?

: Ursnif

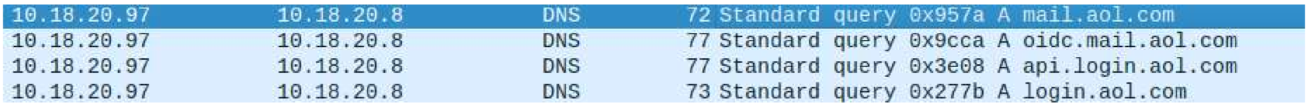


alters.jpg

Dst IP	DPort	Pr	Event Message
10.18.20.8	389	6	ET POLICY Reserved Internal IP Traffic
10.18.20.97	49185	6	ET POLICY Reserved Internal IP Traffic
10.18.20.8	88	6	GPL RPC kerberos principal name overflow TCP
10.18.20.97	59102	17	ET DNS Standard query response, Name Error
10.18.20.97	49354	6	ET POLICY Lets Encrypt Free SSL Cert Observed
10.18.20.97	49364	6	ET POLICY Lets Encrypt Free SSL Cert Observed
10.18.20.97	49561	6	ET POLICY Lets Encrypt Free SSL Cert Observed
8.208.24.139	80	6	ETPRO TROJAN Ursnif Variant CnC Beacon 12 M1
8.208.24.139	80	6	ETPRO TROJAN Ursnif Variant CnC Beacon 12 M2
208.67.222.222	53	17	ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)
10.18.20.97	49597	6	SURICATA HTTP unable to match response to request

Q. Based on traffic from the pcap, where did the malware likely come from?

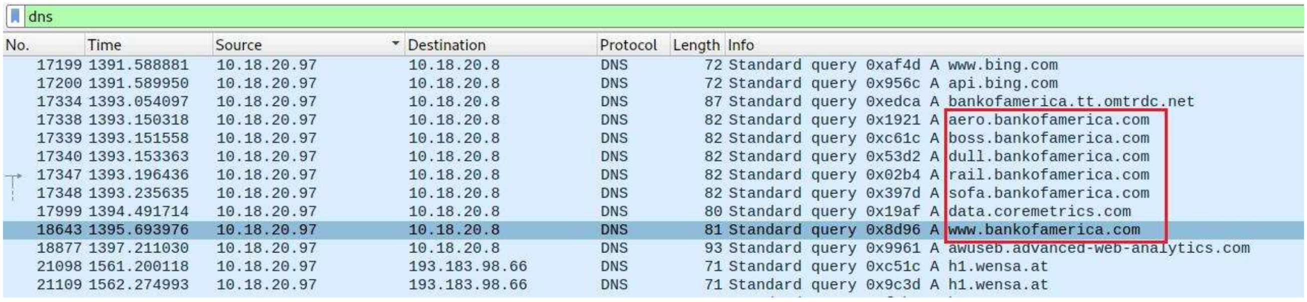
: Email을 통해서 온 가능성이 높음. 이유는 사용자가 감염되기전 mail.aoi.com에 방문한 짧은 기록이 있음.



```
10.18.20.97        10.18.20.8        DNS        72 Standard query 0x957a A mail.aol.com
10.18.20.97        10.18.20.8        DNS        77 Standard query 0x9cca A oidc.mail.aol.com
10.18.20.97        10.18.20.8        DNS        77 Standard query 0x3e08 A api.login.aol.com
10.18.20.97        10.18.20.8        DNS        73 Standard query 0x277b A login.aol.com
```

Q. After the initial infection, what type of web page/website did the victim appear to visit?

: 희생자가 뱅킹사이트에 접속한것으로 보인다. 이유는 몇 다수의 HTTPS 도메인 중 마지막 부분이 bankofamerica.com으로 확인



```
No.   Time          Source        Destination     Protocol Length Info
17199 1391.588881   10.18.20.97   10.18.20.8      DNS      72 Standard query 0xaf4d A www.bing.com
17200 1391.589950   10.18.20.97   10.18.20.8      DNS      72 Standard query 0x956c A api.bing.com
17334 1393.054097   10.18.20.97   10.18.20.8      DNS      87 Standard query 0xedca A bankofamerica.tt.omtrdc.net
17338 1393.150318   10.18.20.97   10.18.20.8      DNS      82 Standard query 0x1921 A aero.bankofamerica.com
17339 1393.151558   10.18.20.97   10.18.20.8      DNS      82 Standard query 0xc61c A boss.bankofamerica.com
17340 1393.153363   10.18.20.97   10.18.20.8      DNS      82 Standard query 0x53d2 A dull.bankofamerica.com
17347 1393.196436   10.18.20.97   10.18.20.8      DNS      82 Standard query 0x02b4 A rail.bankofamerica.com
17348 1393.235635   10.18.20.97   10.18.20.8      DNS      82 Standard query 0x397d A sofa.bankofamerica.com
17999 1394.491714   10.18.20.97   10.18.20.8      DNS      80 Standard query 0x19af A data.coremetrics.com
18643 1395.693976   10.18.20.97   10.18.20.8      DNS      81 Standard query 0x8d96 A www.bankofamerica.com
18877 1397.211030   10.18.20.97   10.18.20.8      DNS      93 Standard query 0x9961 A awuseb.advanced-web-analytics.com
21098 1561.200118   10.18.20.97   193.183.98.66   DNS      71 Standard query 0xc51c A h1.wensa.at
21109 1562.274993   10.18.20.97   193.183.98.66   DNS      71 Standard query 0x9c3d A h1.wensa.at
```