Report on the network traffic data contained in eve_2023-10-31-IcedID-infection-traffic.json

The following report is based on the alerts generated by Suricata.

It was generated by guigui on 2023-12-02 12:27:00

> Disclaimer
>
> This report is a tool for analyzing traffic activity; it does not guarantee exhaustive detection.

Contents

1 Time

The analyzed alerts were generated between 2023-11-01 00:46:35 and 2023-11-27 09:03:08

The total time of the analysis was 26 days, 8:16:33

2 Characteristics of IP addresses

We can notice that some private IP addresses are used:

Address	Network	Probable operating systems
10.10.31.101	10.0.0.0/8 (255.0.0.0)	

10.10.31.255	10.0.0.0/8 (255.0.0.0)	
10.10.31.1	10.0.0.0/8 (255.0.0.0)	

3 Domain names

The following domain names were requested:

ctldl.windowsupdate.com	disc801.prod.do.dsp.mp.microsoft.com
dns.msftncsi.com	fd.api.iris.microsoft.com
fe3cr.delivery.mp.microsoft.com	licensing.mp.microsoft.com
maps.windows.com	msedge.api.cdp.microsoft.com
settings-win.data.microsoft.com	storecatalogrevocation.storequality.microsoft.com
time.windows.com	v10.events.data.microsoft.com
v20.events.data.microsoft.com	

4 Users

No users found.

5 TCP/IP services

The following services have been used:

- tls
- http
- dns
- ntp

6 Alerted signatures

Here are the various signatures that have been alerted:

- ET MALWARE Win32/IcedID Requesting Encoded Binary M4
- ET MALWARE Win32/IcedID Request Cookie
- ET MALWARE DNS Query to IcedID Domain (grafielucho .com)
- ET MALWARE DNS Query to IcedID Domain (manjuskploman .com)
- ET MALWARE Observed IcedID Domain (manjuskploman .com in TLS SNI)
- ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)
- ET MALWARE DNS Query to IcedID Domain (qousahaff .com)
- ET MALWARE Observed IcedID Domain (qousahaff .com in TLS SNI)
- ET MALWARE DNS Query to IcedID Domain (brojizuza .com)
- ET MALWARE DNS Query to IcedID Domain (asleytomafa .com)

- ET MALWARE Observed IcedID Domain (asleytomafa .com in TLS SNI)
- ET MALWARE Observed IcedID Domain (brojizuza .com in TLS SNI)

7 Detected malwares

- signature: ET MALWARE Win32/IcedID Requesting Encoded Binary M4
  - family: IcedID
  - severity: Major
  - (IOC) ip source: 10.10.31.101 ip destination: 104.21.32.6 hostname: grafielucho.com
- signature: ET MALWARE Win32/IcedID Request Cookie
  - family: IcedID
  - severity: Critical
  - (IOC) ip source: 10.10.31.101 ip destination: 104.21.32.6 hostname: grafielucho.com
- signature: ET MALWARE DNS Query to IcedID Domain (grafielucho .com)
  - family: IcedID
  - severity: Major
  - (IOC) ip source: 10.10.31.101 ip destination: 10.10.31.1
- signature: ET MALWARE DNS Query to IcedID Domain (manjuskploman .com)
  - family: IcedID
  - severity: Major
  - (IOC) ip source: 10.10.31.101 ip destination: 10.10.31.1
- signature: ET MALWARE Observed IcedID Domain (manjuskploman .com in TLS SNI)
  - family: IcedID
  - severity: Major
  - (IOC) ip source: 10.10.31.101 ip destination: 45.61.137.225
- signature: ET MALWARE DNS Query to IcedID Domain (qousahaff .com)
  - family: IcedID
  - severity: Major
  - (IOC) ip source: 10.10.31.101 ip destination: 10.10.31.1
- signature: ET MALWARE Observed IcedID Domain (qousahaff .com in TLS SNI)
  - family: IcedID

- severity: Major
- (IOC) ip source: 10.10.31.101 ip destination: 45.61.139.232

- signature: ET MALWARE DNS Query to IcedID Domain (brojizuza .com)
    - family: IcedID
    - severity: Major
    - (IOC) ip source: 10.10.31.101 ip destination: 10.10.31.1
- signature: ET MALWARE DNS Query to IcedID Domain (asleytomafa .com)
    - family: IcedID
    - severity: Major
    - (IOC) ip source: 10.10.31.101 ip destination: 10.10.31.1
- signature: ET MALWARE Observed IcedID Domain (asleytomafa .com in TLS SNI)
    - family: IcedID
    - severity: Major
    - (IOC) ip source: 10.10.31.101 ip destination: 162.33.179.136
- signature: ET MALWARE Observed IcedID Domain (brojizuza .com in TLS SNI)
    - family: IcedID
    - severity: Major
    - (IOC) ip source: 10.10.31.101 ip destination: 45.61.136.22

Internal IP addresses impacted by malware: ['10.10.31.101']

Hashes of detected malwares:

- **ET MALWARE Observed IcedID Domain (manjuskploman .com in TLS SNI)**
    - ja3: 648432770b162235911a5150d4b08679
    - ja3s: 567bb420d39046dbfd1f68b558d86382
- **ET MALWARE Observed IcedID Domain (qousahaff .com in TLS SNI)**
    - ja3: 3248817f54a6ae4a9114c97a29f8ab9b
    - ja3s: 567bb420d39046dbfd1f68b558d86382