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 2023-12-07 23:23:07

> 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	

No domain controllers found.

4 Users

No SMB 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 files detected as malwares:

- file name: /
- magic: gzip compressed data, was "Husband.txt", from FAT filesystem (MS-DOS, OS/2, NT)
- size: 102400
- sha256: 54b0f02570144ac9d958041c4981123e8ad925b3f86fa03d8079bb35b2e9ff1e

---

TzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh/sBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxx

- magic: data

- size: 471
- sha256: 75d4b28b575a3139ad66eddb67f2e5d1a0099e2fb90002904d4fe9542c5ffb3d

---

EwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx/h0Ztl+z8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g/6+rkS7QYXjzkCEAqvpsXKY8RRQeo7

- magic: data
- size: 471
- sha256: 4e271516af10f631ef68c225af1f49600e5203b338a88813243942fe88c6590d