Report on the network traffic data contained in eve.json

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

It was generated by guigui on 2023-12-02 12:28:02

> 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 2023-11-21 13:26:50 and 2023-11-21 15:05:38

The total time of the analysis was 1:38:48

2 Characteristics of IP addresses

We can notice that some private IP addresses are used:

Address	Network	Probable operating systems
172.16.0.153	172.16.0.0/12 (255.240.0.0)	Windows 7 or Windows Server 2008 R2
172.16.0.12	172.16.0.0/12 (255.240.0.0)	Windows 10 or Windows Server 2016
172.16.0.255	172.16.0.0/12 (255.240.0.0)	

3 Domain names

The following domain names were requested:

edge.microsoft.com	fe3cr.delivery.mp.microsoft.com
licensing.mp.microsoft.com	msedge.b.tlu.dl.delivery.mp.microsoft.com
self.events.data.microsoft.com	settings-win.data.microsoft.com
slscr.update.microsoft.com	storecatalogrevocation.storequality.microsoft.com
v10.events.data.microsoft.com	v20.events.data.microsoft.com

4 Users

Here are the extracted users from kerberos requests through smb protocol:

- cifs (Common Internet File System)

5 TCP/IP services

The following services have been used:

- dns
- tls
- dcerpc
- smb
- http
- ntp
- krb5

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 POLICY OpenSSL Demo CA - Internet Widgits Pty (O)
- SURICATA Applayer Detect protocol only one direction
- ET MALWARE Windows arp -a Microsoft Windows DOS prompt command exit OUTBOUND
- ET MALWARE Windows Microsoft Windows DOS prompt command Error not recognized

7 Detected malwares

- signature: ET MALWARE Win32/IcedID Requesting Encoded Binary M4

        - family: IcedID
        - severity: Major
        - (IOC) ip source: 172.16.0.153 ip destination: 67.205.184.237 hostname: vgiragdoffy.com

- signature: ET MALWARE Win32/IcedID Request Cookie

        - family: IcedID
        - severity: Critical
        - (IOC) ip source: 172.16.0.153 ip destination: 67.205.184.237 hostname: vgiragdoffy.com

    - (IOC) ip source: 172.16.0.153 ip destination: 137.74.104.108

    - severity: Critical
    - (IOC) ip source: 172.16.0.153 ip destination: 137.74.104.108

Internal IP addresses impacted by malware: ['172.16.0.153']

Hashes of detected malwares:
No hashes found.