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 2023-12-07 23:22:47

> 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

Here are the requested domain controllers:

- _ldap._tcp.Default-First-Site-Name._sites.FASHIONKINGS-DC.fashionkings.com
- _ldap._tcp.Default-First-Site-Name._sites.FASHIONKINGS-DC.mshome.net
- _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.fashionkings.com
- _ldap._tcp.FASHIONKINGS-DC.fashionkings.com
- _ldap._tcp.FASHIONKINGS-DC.mshome.net
- _ldap._tcp.pdc._msdcs.fashionkings.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 files detected as malwares:

- file name: /
- magic: gzip compressed data, was "Scan.txt", from FAT filesystem (MS-DOS, OS/2, NT)
- size: 102400
- sha256: 8c9aa62f6459b553ca6a5023214f9fdd52c145e3a236c01d0a6e39b4ed25ca08

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: Google Chrome extension, version 3
- size: 1120
- sha256: 0cc666414cbffedca3dfa3eb55f0ec1e70b2920dbc224f98624c25b38902db3c

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638

- magic: data
- size: 28
- sha256: e72b687553c2521edac5ec7ffbdabd8e2ccb747f530f9f9b73852a8b75941ed9

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 10
- sha256: 583bb69ab8572b856a656969e3566920f236a88d8e64e4571ae5f14fe8d639bc

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 6
- sha256: e3cf17d7f3741b883e419b0dbd20573b9a6095e9457a5cfd423e6b8d5183c386

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: Non-ISO extended-ASCII text, with no line terminators
- size: 6
- sha256: b978f365c8eaa87dd4e885fc9d2c9ed47e9234f6109a04538000c1bbd3701749

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 7
- sha256: 4fc20f003b3a5298364235770343d452c8b68970cc1f659fd7ec303a9e77d93d

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 7
- sha256: 58b46f9d721dfe24fff2c157ccb6befbaad57021a8791dce9db4d537e2409376

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: ASCII text, with no line terminators
- size: 7
- sha256: 1513328494bb47f7d05cd47b2d21980bd2de474d2906cf10ae91cd1800beac77

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638

- magic: ISO-8859 text, with no line terminators
- size: 7
- sha256: 58e49dfcc1f962da4bd21bfbf1d284076a13e912fdb0488c490481d265c53196

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 7
- sha256: 59afacb27bad8fb672a0d10b3d92d3ef74f17f8cad0ebde8d4a26eeb591d88a6

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: ISO-8859 text, with no line terminators
- size: 7
- sha256: 65eb527d3adad13e3351e2e2a39a43b94ccc9b443bd16e935dbaabebe2a8b844

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: OpenPGP Public Key
- size: 7
- sha256: 9e500923a1ab7476808b715dfab4e91e1241f32c87d67a7a0dbe87b194d6820f

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: Non-ISO extended-ASCII text, with no line terminators
- size: 7
- sha256: 64baa2f4811ab8d969010c257672586a2230cd825133057bde9577f3f0f0498f

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 7
- sha256: 9c2f89e2738e938bf79424845acfbf704fbba98c60e784e6b703d08b15e30734

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: PGP symmetric key encrypted data -
- size: 7
- sha256: 4b5777812418b96f3e112470b7692d700dc83b4115d7a27601d4b4038d25fe2d

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638

- magic: data
- size: 7
- sha256: af99d30bc43569a99f6ef753333ff3d17d75ebb49f2f8043a4f949c2e5245d10

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: Non-ISO extended-ASCII text, with no line terminators
- size: 7
- sha256: 8e0ebf2becd176380dd98d2609dba755e2c03fbfa38f55a069e1a95087136c3e

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: OpenPGP Secret Key
- size: 7
- sha256: bb90238d82177e1573d23448c83ee302493012311ea0b2f50d9e50070b269da0

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: Non-ISO extended-ASCII text
- size: 7
- sha256: 9237f8a58189e34cf79c50e05181b244993029807b86645b5b1e516fb1b0810f

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 7
- sha256: 89662765e14222a7e87292aa5657023e41b4a5340b41ac4f81b600e510b461e8

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 7
- sha256: 6bc0aa83d14e20d2a88c68f0edd9eb4f9ee10c4b803d6b163546f364dea61783

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: Unicode text, UTF-8 text, with no line terminators
- size: 7
- sha256: 6673a4144b2f0759832bf6a3d3f652f4b6658ae581c69e063dff4acd8d287820

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638

- magic: Non-ISO extended-ASCII text, with no line terminators
- size: 7
- sha256: 8fea4cb6d6ef4b385e49a541f2cb6bd55352cd9327e9035cacda870db5e2624f

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: OpenPGP Public Key
- size: 7
- sha256: f902da3fc5750c895223114dc247c3906385c2fbd439872b320cc388a73d3250

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: Non-ISO extended-ASCII text, with no line terminators
- size: 7
- sha256: 77a7a06aefe8c4bc1fa097519f92f8e96141e61ddb706e131e84fa790501e710

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: ISO-8859 text, with no line terminators
- size: 7
- sha256: e38b56b0d2fbdd5b1cff0172734ba62fb74e6bf6b5d30da02645e0b085dbed04

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 7
- sha256: 3db6f7ee9af076e0212a50f25748f52f2d78b5e0688bd8b06d6ddb66e0c7e1ac

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: Non-ISO extended-ASCII text, with no line terminators
- size: 7
- sha256: db46ac47dcbdb7c2a656f9bc509198f5c4f2b37ee42f7e0106320d375c82b2b3

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 19746
- sha256: eb15cadeb97635bba603097f7d2a1f69ee03dd84f8c20316e8644089f48c50e9

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638

- magic: data
- size: 82402
- sha256: b1697c59e9864fa5c7b535281e904a1f528ce2bc0af8d383267b25c933db799f

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 102400
- sha256: 9f67411439abe996836ca9db5db0e27c6f10fbdc1f9faa064a26646cc27e0e65

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 102400
- sha256: de294852ba70fdba5292f094704b9d20bbf04a8c2a289b47656310d3c447718e

---

- file name: /filestreamingservice/files/c78f9967-7a8c-44b0-ad94-732b63c89638
- magic: data
- size: 102400
- sha256: 0504bd0a44e8be98dfbc601479e15b7dab61f4f6041455be2f74d761a0860fb8

- file name: /filestreamingservice/files/b22f5f18-f7ea-4290-929d-b13c03908334
- magic: Google Chrome extension, version 3
- size: 1120
- sha256: 52abfdd3d4da8915ebd6383520be29868de571e397e55ebafb76057d22ecbe5a

---

- file name: /filestreamingservice/files/b22f5f18-f7ea-4290-929d-b13c03908334
- magic: data
- size: 24
- sha256: 98e17b22805588c1a5d593428c34b5505635abc3615a9c7229b10be3f66336d6

- file name: /filestreamingservice/files/b22f5f18-f7ea-4290-929d-b13c03908334
- magic: data
- size: 41
- sha256: 38fe9f3b98e29dca85ef31be2c0375892e35369ebe7f3c8752336f38c08b2d61

- file name: /filestreamingservice/files/b22f5f18-f7ea-4290-929d-b13c03908334

- magic: data
- size: 170
- sha256: 9067f04ba42f76429bc24d41c2e6f61b59c9b4f63c83f6110868fb266ab97202

- file name: /filestreamingservice/files/b22f5f18-f7ea-4290-929d-b13c03908334
- magic: Google Chrome extension, version 3
- size: 1355
- sha256: 26123bef7d73536450862d2c4d44963d720aa80b6fc2d8496f559cb9c1fdeb00

- file name: /
- magic: Certificate, Version=3
- size: 1306
- sha256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd

---

- file name: fashionkings.comPolicies{31B2F340-016D-11D2-945F-00C04FB984F9}MachineMicrosoftWindows NTSecEditGptTmpl.inf
- magic: Unicode text, UTF-16, little-endian text, with CRLF line terminators
- size: 1098
- sha256: 01406b7bd612a8321213382482e44ea2c7b5467b57e17e9c135eab2a8221faea

---

- file name: fashionkings.comPolicies{31B2F340-016D-11D2-945F-00C04FB984F9}MachineRegistry.pol
- magic: data
- size: 2800
- sha256: d52beca5a2c54aa44d133221a9a470f58179e41caf8d5838bac98c898b52878d

---

- file name: fashionkings.comPolicies{31B2F340-016D-11D2-945F-00C04FB984F9}gpt.ini
- magic: ASCII text, with CRLF line terminators
- size: 22
- sha256: 4cac14573e271cd786fdfc02287143fd3de95cbbd84754d29bd3387ecd914669