For file test.json

First timestamp : Wednesday, 01 November 2023 00:46:34 UTC+01:00

Last timestamp : Tuesday, 05 December 2023 09:37:42 UTC+01:00

Private IPs :

10.10.31.255

10.10.31.1

10.10.31.101

Networks :

10.0.0.0/8

Windows domains :

fd.api.iris.microsoft.com

ctldl.windowsupdate.com

msedge.api.cdp.microsoft.com

licensing.mp.microsoft.com

fe3cr.delivery.mp.microsoft.com

maps.windows.com

v20.events.data.microsoft.com

storecatalogrevocation.storequality.microsoft.com

time.windows.com

v10.events.data.microsoft.com

disc801.prod.do.dsp.mp.microsoft.com

settings-win.data.microsoft.com

Domain controllers :

Users :

OS :

Services TCP/IP :

http port : 80

tls port : 443

THREAT DETECTION

Signatures detected :

ET MALWARE Win32/IcedID Requesting Encoded Binary M4

ET MALWARE DNS Query to IcedID Domain (manjuskploman .com)

ET MALWARE DNS Query to IcedID Domain (grafielucho .com)

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

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

ET MALWARE DNS Query to IcedID Domain (asleytomafa .com)

ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)

ET MALWARE DNS Query to IcedID Domain (qousahaff .com)

ET MALWARE DNS Query to IcedID Domain (brojizuza .com)

ET MALWARE Observed IcedID Domain (manjuskploman .com in TLS SNI)

ET MALWARE Observed IcedID Domain (qousahaff .com in TLS SNI)

ET MALWARE Win32/IcedID Request Cookie

Malwares detected :

IcedID

Private adresses impacted :

10.10.31.1

10.10.31.101

IOCS concerned (hostname,ip) :

104.21.32.6 grafielucho.com

45.61.139.232 qousahaff.com

45.61.136.22 brojizuza.com

45.61.137.225 manjuskploman.com

162.33.179.136 asleytomafa.com

Hashes detected :

54b0f02570144ac9d958041c4981123e8ad925b3f86fa03d8079bb35b2e9ff1e