For file out.json

First timestamp : Monday, 21 March 2022 21:58:11 UTC+01:00

Last timestamp : Thursday, 07 December 2023 09:48:31 UTC+01:00

Private IPs :

10.0.19.9

10.0.19.255

10.0.19.1

10.0.19.14

Networks :

10.0.0.0/8

Windows domains :

login.microsoftonline.com

v10.events.data.microsoft.com

client.wns.windows.com

storecatalogrevocation.storequality.microsoft.com

settings-win.data.microsoft.com

checkappexec.microsoft.com

licensing.mp.microsoft.com

msedge.api.cdp.microsoft.com

ctldl.windowsupdate.com

Domain controllers :

_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.burnincandle.com

_ldap._tcp.Default-First-Site-Name._sites.burnincandle.com

_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.mshome.net

_ldap._tcp.dc._msdcs.mshome.net

Users :

DESKTOP-5QS3D5D$

desktop-5qs3d5d$

patrick.zimmerman

OS :

Windows Server 2019 Standard 17763

Windows 10 Pro 19044

Services TCP/IP :

tls port : 757

dcerpc port : 49667

http port : 80

dcerpc port : 49676

tls port : 443

krb5 port : 88

smb port : 445

dcerpc port : 135

smb port : 139

THREAT DETECTION

Signatures detected :

ET INFO HTTP Request to a *.top domain

ET MALWARE Win32/IcedID Request Cookie

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

ET MALWARE Win32/IcedID Requesting Encoded Binary M4

ET DNS Query to a *.top domain - Likely Hostile

Malwares detected :

IcedID

Private adresses impacted :

10.0.19.9

10.0.19.14

IOCS concerned (hostname,ip) :

91.193.16.181 seaskysafe.com

91.193.16.181 dilimoretast.com

157.245.142.66 otectagain.top

188.166.154.118 oceriesfornot.top

157.245.142.66 antnosience.com

Hashes detected :

f2662ee8432db821154d9279aab1a62b037fe11b976898b1b33dedc77099078b