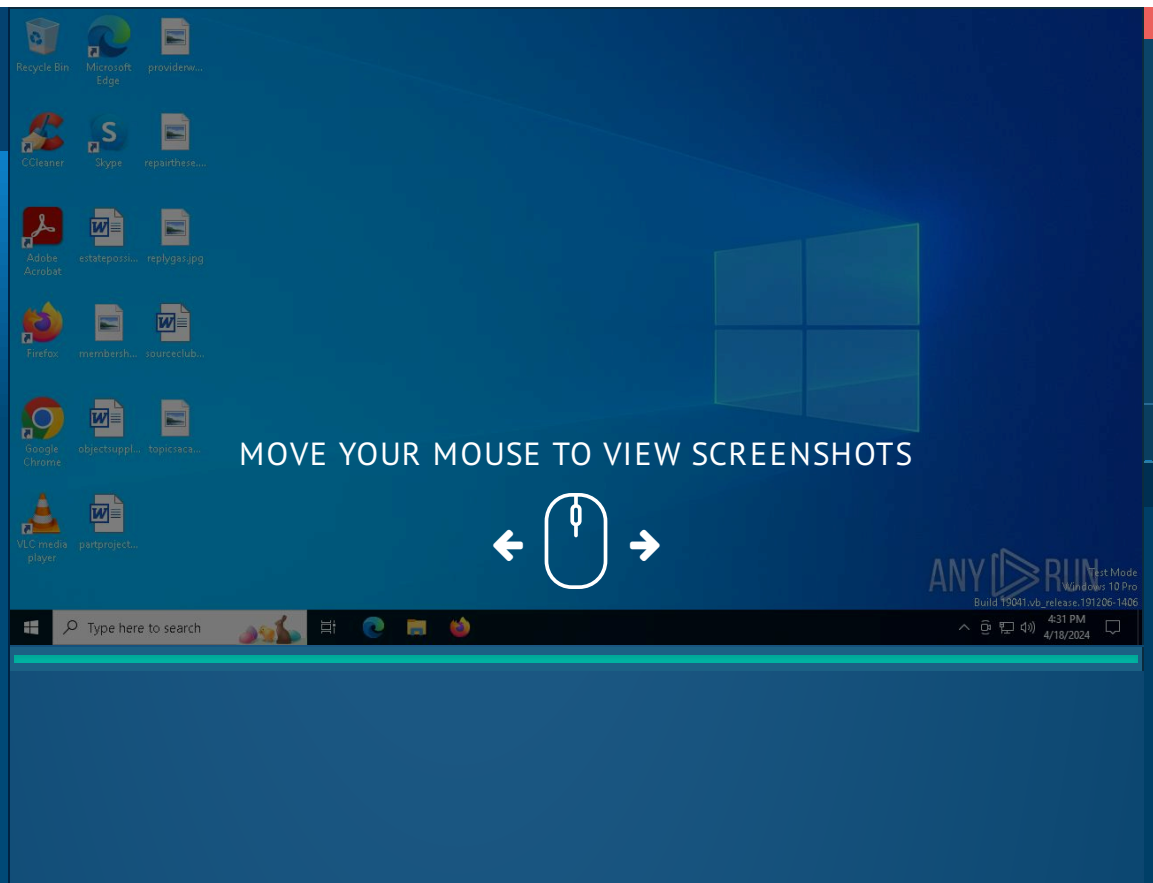

Malicious activity

2dcedda2d433140e29c0e0efa141df17c...

MD5: A6A52958BEC5F9BCA6D3DD49072B481B

Start: 18.04.2024, 18:31 Total time: 120 s

Win10 64 bit Complete

smtp stealer agenttesla

Indicators: Tracker: Agent Tesla, Stealer

Get sample | IOC | MalConf | Restart

Text report | Graph | ATT&CK | AI Summary beta | Export

CPU RAM

Processes Filter by PID or name Only important

6088 2dcedda2d433140e29c0e0efa141df17c0398b820922c7e39f4ab50... 137 35 21

1604 conhost.exe 0xffffffff -ForceV1 202 132 36

932 RegAsm.exe 1 0 3

6548 RegAsm.exe 0 0 3

6628 RegAsm.exe CFG DMP agenttesla 1k 1k 110

2284 COM SppExtComObj.Exe -Embedding 69 52 34

4876 slui.exe RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;Actio... 959 569 65

3744 COM slui.exe -Embedding 365 179 43

HTTP Requests 13 | Connections 40 | DNS Requests 20 | Threats 4 | Filter by PID, name or url | PCAP

NETWORK FILES DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
5861 ms	GET | 200: OK	?	4172	svchost.exe		http://www.microsoft.com/pkiops/crl/...	9
17142 ms	GET | 200: OK	?	5264	svchost.exe		http://ocsp.digicert.com/MFEwTzBNM...	4
25233 ms	GET | 200: OK	?	6312	SIHClient.exe		http://www.microsoft.com/pkiops/crl/...	4
25235 ms	GET | 200: OK	?	6312	SIHClient.exe		http://www.microsoft.com/pkiops/crl/...	4
67284 ms	GET | 200: OK	?	2980	svchost.exe		http://www.microsoft.com/pkiops/crl/...	8
68279 ms	GET | No Response	?	2980	svchost.exe		http://www.microsoft.com/pkiops/crl/...	
99016 ms	GET | 200: OK	?	2980	svchost.exe		http://www.microsoft.com/pkiops/crl/...	8
99017 ms	GET | 200: OK	?	2980	svchost.exe		http://www.microsoft.com/pkiops/crl/...	4

Info [4876] slui.exe Reads the software policy settings

Try community version for free! Register now