Dynamic Analysis of Unknown Binaries

Goalsascii,42,.rdata,-,-,-,-,@http://serv1.ec2-102-95-13-2-ubuntu.local

[Request URI: http://serv1.ec2-102-95-13-2-ubuntu.local/msdcorelib.exe]

msdcorelib.exe

41 0.094770125 10.0.0.3 10.0.0.4 HTTP 256 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e2591b5962274d3d HTTP/1.1

C:\Users\vishal\SystemResources\RAT.Unknown.exe.mun

C:\Windows\Prefetch\RAT.UNKNOWN.EXE-7C7A80CB.pf

4:15:02.1988368 PM RAT.Unknown.exe 7572 CreateFile C:\Users\vishal\Desktop\IPHLPAPI.DLL NAME NOT FOUND Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a

4:15:02.2630710 PM RAT.Unknown.exe 7572 CreateFile C:\Users\vishal\AppData\Local\Microsoft\Windows\INetCache\IE\87WXFCZP SUCCESS Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened

C:\Users\vishal\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\

RAT.Unknown.exe,9208,TCP,Listen,0.0.0.0,5555,0.0.0.0,0,6/7/2023 4:42:49 PM,RAT.Unknown.exe,,,,