Windows Analysis Report revil.exe

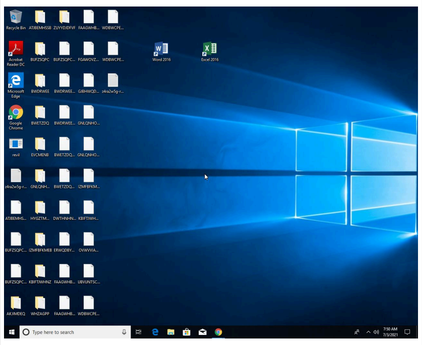
Create Interactive Tour

Overview

General Information

Sample Name:	revil.exe
Analysis ID:	443736
MD5:	561cffbaba71a6e8cc…
SHA1:	5162f14d75e96edb91…
SHA256:	d55f983c994caa160e…
Tags:	exe revil Sodinokibi
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

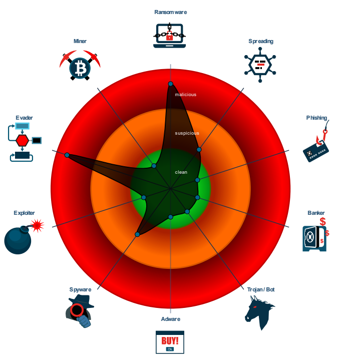
Sodinokibi

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

Signatures

- Found malware configuration
- Found ransom note / readme
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Sodinokibi Ransomware
- Contains functionality to detect sleep reductio…
- Contains functionalty to change the wallpaper
- Drops executables to the windows directory (…
- Found Tor onion address
- Modifies existing user documents (likely ranso…
- Modifies the windows firewall
- Queries sensitive service information (via WMI,…
- Sigma detected: Executable Used by PlugX in…
- Uses netsh to modify the Windows network a…
- AV process strings found (often used to termin…

Classification



Process Tree

- **System is w10x64**
- revil.exe (PID: 6960 cmdline: 'C:\Users\user\Desktop\revil.exe' MD5: 561CFFBABA71A6E8CC1CDCEDA990EAD4)
  - MsMpEng.exe (PID: 6972 cmdline: C:\Windows\MsMpEng.exe MD5: 8CC83221870DD07144E63DF594C391D9)
    - netsh.exe (PID: 5964 cmdline: netsh advfirewall firewall set rule group='Network Discovery' new enable=Yes MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 1424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- unsecapp.exe (PID: 5948 cmdline: C:\Windows\system32\wbem\unsecapp.exe -Embedding MD5: 9CBD3EC8D9E4F8CE54258B0573C66BEB)
- **cleanup**

Malware Configuration

Threatname: Sodinokibi

```
{
  "prc": [
    "encsvc",
    "powerpnt",
    "ocssd",
    "steam",
    "isqlplussvc",
    "outlook",
    "sql",
    "ocomm",
    "agntsvc",
    "mspub",
    "onenote",
    "winword",
    "thebat",
    "excel",
    "mydesktopqos",
    "ocautoupds",
    "thunderbird",
    "synctime",
    "infopath",
    "mydesktopservice",
    "firefox",
    "oracle",
    "sqbcoreservice",
    "dbeng50",
    "tbirdconfig",
    "msaccess",
    "visio",
    "dbsnmp",
    "wordpad",
    "xfssvccon"
  ],
  "sub": "8254",
  "svc": [
    "veeam",
    "memtas",
    "sql",
    "backup",
    "vss",
    "sophos",
    "svc$",
    "mepocs"
  ],
  "wht": {
    "ext": [
      "ps1",
      "ldf",
      "lock",
      "theme",
      "msi",
      "sys",
      "wpx",
      "cpl",
      "adv",
      "msc",
      "scr",
    "dll",
    "hta",
    "deskthemepack",
    "nomedia",
    "msu",
    "rtp",
    "msp",
    "idx",
    "ani",
    "386",
    "diagcfg",
    "bin",
    "mod",
    "ics",
    "com",
    "hlp",
    "spl",
    "nls",
    "cab",
    "exe",
    "diagpkg",
    "icl",
    "ocx",
    "rom",
    "prf",
    "themepack",
    "msstyles",
    "lnk",
    "icns",
    "mpa",
    "drv",
    "cur",
    "diagcab",
    "cmd",
    "shs"
  ],
  "fls": [
    "ntldr",
    "thumbs.db",
    "bootsect.bak",
    "autorun.inf",
    "ntuser.dat.log",
    "boot.ini",
    "iconcache.db",
    "bootfont.bin",
    "ntuser.dat",
    "ntuser.ini",
    "desktop.ini"
  ],
  "fld": [
    "program files",
    "appdata",
    "mozilla",
    "$windows.~ws",
    "application data",
    "$windows.~bt",
    "google",
    "$recycle.bin",
    "windows.old",
    "programdata",
    "system volume information",
    "program files (x86)",
    "boot",
    "tor browser",
    "windows",
    "intel",
    "perflogs",
    "msocache"
  ]
 },
 "img":
"QQBsAGwAIABvAGYAIAB5AG8AdQByACAAZgBpAGwAZQBzACAAYQByAGUAIABlAG4AYwByAHkAcAB0AGUAZAAhAA0ACgANAAoARgBpAG4AZAAgAHsARQBYAFQAfQAtAHIAZQBhAGQAbQBlAC4AdAB4AHQAIABhAG4AZAAgAGYAbwBsAGwAbwB3ACAAaQBuA
HMAdAB1AGMAdAB1AG8AbgBzAAAA",
 "dmn": "boisehosting.net;fotoideaymedia.es;dubnew.com;stallbyggen.se;koken-voor-baby.nl;juneauopioidworkgroup.org;vancouver-print.ca;zewatchers.com;bouquet-de-roses.com;seevilla-dr-
sturm.at;olejack.ru;i-trust.dk;wasmachtmeinfonds.at;appsformacpc.com;friendsandbrgrs.com;thenewrejuveme.com;xn--singlebrsen-vergleich-nec.com;sabel-
bf.com;seminoc.com;ceres.org.au;cursoporcelanatoliquido.online;marietteaernoudts.nl;tastewilliamsburg.com;charlottepoudroux-
photographie.fr;aselbermachen.com;klimt2012.info;accountancywijchen.nl;creamery201.com;rerekatu.com;makeurvoiceheard.com;vannesteconstruct.be;wellplast.se;andersongilmour.co.uk;bradynursery.
com;aarvorg.com;facettenreich27.de;balticdermatology.lt;artige.com;highlinesouthasc.com;crowd-
patch.co.uk;sofavietxinh.com;jorgobe.at;danskretursystem.dk;higadograsoweb.com;supportsumba.nl;ruralarcoiris.com;projetlyonturin.fr;kidbucketlist.com.au;harpershologram.wordpress.com;ohidesi
gn.com;international-sound-awards.com;krlosdavid.com;durganews.com;leather-factory.co.jp;coding-machine.com;i-arslan.de;caribbeansunpoker.com;mir-na-iznanku.com;ki-
lowroermond.nl;promesapuertorico.com;kissit.ca;dezatec.es;cite4me.org;grelot-home.com;musictreehouse.net;hkr-reise.de;id-vet.com;gasolspecialisten.se;vyhino-zhulebino-
24.ru;karacaoglu.nl;bayoga.co.uk;solhaug.tk;jadwalbolanet.info;ncid.bc.ca;bricotienda.com;boldcitydowntown.com;homecomingstudio.com;sojamindbody.com;castillobalduz.es;asgestion.com;dushka.ua
;hiddencitysecrets.com.au;danubecloud.com;roadwarrior.app;newstap.com.ng;no-plans.com;schoolofpassivewealth.com;senson.fi;denifl-
consulting.at;lmtprovisions.com;talentwunder.com;acomprarseguidores.com;myzk.site;theapifactory.com;midmohandyman.com;argos.wityu.fund;dinslips.se;kalkulator-
oszczednosci.pl;wurmpower.at;drugdevice.org;foretprivee.ca;nurturingwisdom.com;funjose.org.gt;blgr.be;readberserk.com;lescomtesdemean.be;firstpaymentservices.com;malychanieruchomoscipremium.
com;travelffeine.com;latribuessentielle.com;lusak.at;better.town;smessier.com;kafu.ch;ikads.org;id-et-d.fr;sanaia.com;prochain-
voyage.net;edrcreditservices.nl;yassir.pro;gantungankunciakrilikbandung.com;moveonnews.com;bhwlawfirm.com;bigbaguettes.eu;edv-
live.de;littlebird.salon;iyengaryogacharlotte.com;toponlinecasinosuk.co.uk;zonamovie21.net;caribdoctor.org;body-
guards.it;calabasasdigest.com;elimchan.com;herbstfeststaefa.ch;thewellnessmimi.com;corola.es;pomodori-
pizzeria.de;controldekk.com;lichencafe.com;lefumetdesdombes.com;seagatesthreecharters.com;copystar.co.uk;systemate.dk;alsace-first.com;webmaster-peloton.com;koko-
nora.dk;jakekozmor.com;mousepad-direkt.de;iwelt.de;dirittosanitario.biz;precisionbevel.com;boulderwelt-muenchen-west.de;chatizel-paysage.fr;praxis-
foerderdiagnostik.de;globedivers.wordpress.com;nosuchthingasgovernment.com;neuschelectrical.co.za;schmalhorst.de;mediaclan.info;ihr-
news.jp;bunburyfreightservices.com.au;edelman.jp;backstreetpub.com;spsshomeworkhelp.com;lillegrandpalais.com;smithmediastrategies.com;enovos.de;loprus.pl;bsaship.com;importardechina.info;shh
ealthlaw.com;freie-
baugutachterpraxis.de;maxadams.london;deprobatehelp.com;baylegacy.com;deltacleta.cat;financescorecard.com;maureenbreezedancetheater.org;plv.media;winrace.no;leoben.at;pawsuppetlovers.com;tuu
liautio.fi;paradicepacks.com;1team.es;testcoreprohealthuk.com;broseller.com;iyahayki.nl;lorenacarnero.com;satyayoga.de;notmissingout.com;chavesdoareeiro.com;mezhdu-
delom.ru;hugoversichert.de;jusibe.com;imaginado.de;craftleathermnl.com;sauschneider.info;atalent.fi;conexa4papers.trade;global-kids.info;serce.info.pl;agence-referencement-naturel-
geneve.net;zimmerei-fl.de;augenta.com;fannmedias.com;villa-marrakesch.de;ulyssemarketing.com;x-
ray.ca;schraven.de;bowengroup.com.au;sairaku.net;southeasternacademyofprosthodontics.org;modamilyon.com;pubweb.carnet.hr;alysonhoward.com;sahalstore.com;triactis.com;panelsandwichmadrid.es;x
n--vrftet-pua.biz;adoptioperheet.fi;miriamgrimm.de;filmstreamingvfcomplet.be;kostenlose-webcams.com;deoudedorpskernnoordwijk.nl;live-your-life.jp;mardenherefordshire-
pc.gov.uk;instatron.net;mirjamholleman.nl;euro-trend.pl;kojima-
shihou.com;nuzech.com;basisschooldezonnewijzer.nl;quemargrasa.net;actecfoundation.org;gamesboard.info;podsosnami.ru;extensionmaison.info;retroearthstudio.com;polzine.net;hmsdanmark.dk;linnan
kellari.fi;schoellhammer.com;elpa.se;mooreslawngarden.com;rozemondcoaching.nl;lenreactiv-shop.ru;uranus.nl;advokathuset.dk;ora-it.de;love30-
chanko.com;smartypractice.com;rebeccarisher.com;cafemattmeera.com;bargningavesta.se;www1.proresult.no;rhinosfootballacademy.com;polychromelabs.com;notsilentmd.org;makeflowers.ru;zimmerei-
deboer.de;ccpbroadband.com;iwr.nl;wychowanieprzedszkolne.pl;greenpark.ch;bimnapratica.com;lachofikschiet.nl;memaag.com;parking.netgateway.eu;tanzschule-
kieber.de;antiaginghealthbenefits.com;simulatebrain.com;digi-
talents.com;hairnetty.wordpress.com;samnewbyjax.com;helikoptervluchtnewyork.nl;devlaur.com;cimanchesterescorts.co.uk;houseofplus.com;rushhourappliances.com;pelorus.group;kedak.de;lapmangfpt.
info.vn;pivoineetc.fr;marchand-
sloboda.com;anybookreader.de;markelbroch.com;celularity.com;rafaut.com;unim.su;latestmodsapks.com;thedresserie.com;bigasgrup.com;slimidealherbal.com;phantastyk.com;thailandholic.com;tophuman
servicescourses.com;aakritpatel.com;navyfederalautooverseas.com;wien-
mitte.co.at;forestlakeuca.org.au;sporthamper.com;psnacademy.in;michaelsmeriglioracing.com;jbbjw.com;colorofhorses.com;iqbalscientific.com;cleliaekiko.online;stemplusacademy.com;effortlesspro
mo.com;microcirc.net;mbfagency.com;theduke.de;drinkseed.com;troegs.com;peterstrobos.com;consultaractadenacimiento.com;huissier-
creteil.com;geoffreymeuli.com;skanah.com;despedidascostablanca.es;alten-
mebel63.ru;theadventureedge.com;profectis.de;mepavex.nl;rimborsobancario.net;pasvenska.se;tampaallen.com;symphonyenvironmental.com;videomarketing.pro;pickanose.com;licor43.de;aniblinova.word
press.com;ventti.com.ar;hhcourier.com;buymedical.biz;oncarrot.com;nachhilfe-unterricht.com;mapawood.com;vox-
surveys.com;milsing.hr;sotsioloogia.ee;nativeformulas.com;kirkepartner.dk;partnertaxi.sk;visiativ-
industry.fr;transliminaltribe.wordpress.com;chefdays.de;cursosgratuitosnainternet.com;faronics.com;d2marketing.co.uk;lapinlviasennus.fi;miraclediet.fun;bristolaeroclub.co.uk;jameskibbie.com;
songunceliptv.com;baronloan.org;idemblogs.com;eglectonk.online;christinarebuffetcourses.com;bastutunnan.se;blogdecachorros.com;finde-deine-
marke.de;platformier.com;antenanavi.com;vanswigchemdesign.com;gporf.fr;pmc-services.de;atmos-
```

```
turtles.com;coffreo.biz;tandartspraktijkheesch.nl;vietlawconsultancy.com;deko4you.at;tennisclubetten.nl;extraordinaryoutdoors.com;crowcanyon.com;classycurtainsltd.co.uk;apolomarcas.com;veryt
ycs.com;manijaipur.com;veybachcenter.de;falcou.fr;associationanalytics.com;beautychance.se;pocket-opera.de;christ-michael.net;vdberg-
autoimport.nl;4net.guru;finediningweek.pl;stampagrafica.es;naturalrapids.com;ussmontanacommittee.us;beaconhealthsystem.org;upplandsspar.se;tradiematepro.com.au;oneplusresource.org;maasreusel
.nl;aodaichandung.com;campus2day.de;burkert-ideenreich.de;you-bysia.com.au;mediaacademy-
iraq.org;xtptrack.com;eaglemeetstiger.de;mountaintoptinyhomes.com;stemenstilte.nl;noskierrenteria.com;ivfminiua.com;biapi-
coaching.fr;art2gointerieurprojecten.nl;corendonhotels.com;ditog.fr;kadesignandbuild.co.uk;abogadosaccidentetraficosevilla.es;camsadviser.com;limassoldriving.com;worldhealthbasicinfo.com;koj
insaisei.info;schmalhorst.de;bigler-hrconsulting.ch;girlillamarketing.com;xn--rumung-bua.online;naturstein-hotte.de;agence-chocolat-
noir.com;stormwall.se;collaborativeclassroom.org;baptisttabernacle.com;streamerzradio1.site;mooglee.com;smart-light.co.uk;fitovitaforum.com;c2e-
poitiers.com;igrealestate.com;wari.com.pe;takeflat.com;logopaedie-blomberg.de;mrsplans.net;mooshine.com;humanityplus.org;otsu-
bon.com;onlyresultsmarketing.com;interactcenter.org;ungsvenskarna.se;35-40konkatsu.net;zzyjtsgls.com;spectrmash.ru;tenacitytenfold.com;torgbodenbollnas.se;drnice.de;lightair.com;huesges-
gruppe.de;promalaga.es;paulisdogshop.de;hotelsolbh.com.br;julis-lsa.de;myteamgenius.com;darnallwellbeing.org.uk;refluxreducer.com;educar.org;kuntokeskusrok.fi;truenyc.co;comparatif-lave-
linge.fr;frontierweldingllc.com;autodemontagenijmegen.nl;spylista.com;allfortheloveofyou.com;ilso.net;corona-
handles.com;micahkoleoso.de;fairfriends18.de;haremnick.com;ecoledansemulhouse.fr;blewback.com;macabaneaupaysflechois.com;osterberg.fi;surespark.org.uk;stupbratt.no;hokagestore.com;mirkoreiss
er.de;tomoiyuma.com;tigsltd.com;manifestinglab.com;glennroberts.co.nz;hardinggroup.com;zso-
mannheim.de;yousay.site;dublikator.com;oneheartwarriors.at;pointos.com;kenhnoithatgo.com;ausbeverage.com.au;testzandbakmetmening.online;grupocarvalhoerodrigues.com.br;werkkring.nl;hotelzentr
al.at;vibethink.net;123vrachi.ru;allure-cosmetics.at;mrxermon.de;bloggyboulga.net;bouldercafe-
wuppertal.de;sobreholanda.com;smogathon.com;beyondmarcomdotcom.wordpress.com;wraithco.com;bookspeopleplaces.com;montrium.com;webcodingstudio.com;lucidinvestbank.com;ncs-graphic-
studio.com;stingraybeach.com;aglend.com.au;lecantou-coworking.com;tongdaifpthaiphong.net;solerluethi-allart.ch;coursio.com;otto-
bollmann.de;madinblack.com;vibehouse.rw;bridgeloanslenders.com;erstatningsadvokaterne.dk;resortmtn.com;socstrp.org;pier40forall.org;ostheimer.at;quickyfunds.com;aminaboutique247.com;jobcente
rkenya.com;jenniferandersonwriter.com;marcuswhitten.site;mediaplayertest.net;irinaverwer.com;stoeberstuuv.de;lebellevue.fr;the-virtualizer.com;outcomeisincome.com;gonzalezfornes.es;kunze-
immobilien.de;myhealth.net.au;helenekowalsky.com;xn--fn-
kka.no;withahmed.com;simplyblessedbykeepingitreal.com;havecamerawilltravel2017.wordpress.com;muamuadolls.com;balticdentists.com;mank.de;croftprecision.co.uk;jandaonline.com;datacenters-in-
europe.com;gw2guilds.org;raschlosser.de;geekwork.pl;pv-design.de;opatrovanie-ako.sk;ausair.com.au;commonground-stories.com;parebrise-tla.fr;vloeren-
nu.nl;conasmanagement.de;dlc.berlin;liveottelut.com;4youbeautysalon.com;lykkeliv.net;adultgamezone.com;hexcreatives.co;citymax-
cr.com;portoesdofarrobo.com;patrickfoundation.net;tonelektro.nl;atozdistribution.co.uk;urclan.net;evergreen-fishing.com;body-armour.online;nsec.se;autopfand24.de;syndikat-
asphaltfieber.de;yourobgyn.net;vihannesporssi.fi;new.devon.gov.uk;teczowadolina.bytom.pl;antonmack.de;dpo-as-a-service.com;pogypneu.sk;creative-waves.co.uk;htchorst.nl;xn--
fnsterputssollentuna-39b.se;norpol-
yachting.com;parkstreetauto.net;sloverse.com;candyhouseusa.com;tsklogistik.eu;smejump.co.th;diversiapsicologia.es;unetica.fr;drfoyle.com;cranleighscoutgroup.org;dekkinngay.com;n1-
headache.com;amerikansktgodis.se;evangelische-pfarrgemeinde-tuniberg.de;fransespiegels.nl;coastalbridgeadvisors.com;qualitaetstag.de;kath-kirche-gera.de;alhashem.net;schutting-
info.nl;2ekeus.nl;berlin-bamboo-bikes.org;minipara.com;blood-sports.net;milestoneshows.com;physiofischer.de;ontrailsandboulevards.com;babcockchurch.org;healthyyworkout.com;plantag.de;krcove-
zily.eu;mylolis.com;fax-payday-loans.com;praxis-management-plus.de;smokeysstoves.com;longislandelderlaw.com;calxplus.eu;mountsoul.de;dubscollective.com;luckypatcher-
apkz.com;epwritescom.wordpress.com;fundaciongregal.org;klusbeter.nl;jobmap.at;oldschoolfun.net;abl1.net;labobit.it;romeguidedvisit.com;carrybrands.nl;people-
biz.com;blossombeyond50.com;theclubms.com;whittier5k.com;jolly-
events.com;kisplanning.com.au;rostoncastings.co.uk;ravensnesthomegoods.com;nhadatcanho247.com;vetapharma.fr;hihaho.com;tulsawaterheaterinstallation.com;purposeadvisorsolutions.com;faizanulla
h.com;directwindowco.com;herbayupro.com;pay4essays.net;work2live.de;stoneys.ch;webhostingsrbija.rs;lange.host;baustb.de;psa-sec.de;hushavefritid.dk;lloydconstruction.com;ra-
staudte.de;mbxvii.com;tecnojobsnet.com;starsarecircular.org;twohourswithlena.wordpress.com;stoeferlehalle.de;merzi.info;garage-lecompte-rouen.fr;hypozentrum.com;nestor-
swiss.ch;thomasvicino.com;kmbshipping.co.uk;denovofoodsgroup.com;planchaavapor.net;dr-pipi.de;qlog.de;lynsayshepherd.co.uk;aco-
media.nl;abogadoengijon.es;bestbet.com;liliesandbeauties.org;norovirus-
ratgeber.de;thee.network;stacyloeb.com;bundabergeyeclinic.com.au;sandd.nl;americafirstcommittee.org;milanonotai.it;kevinjodea.com;easytrans.com.au;westdeptfordbuyrite.com;carriagehousesalonv
t.com;operaslovakia.sk;corelifenutrition.com;hashkasolutindo.com;compliancesolutionsstrategies.com;edgewoodestates.org;mastertechengineering.com;pinkexcel.com;cnoia.org;aprepol.com;rieed.de;
katketytaanet.fi;lascuola.nl;assurancesalextrespaille.fr;paymybill.guru;xoabigail.com;ligiercenter-sachsen.de;answerstest.ru;airconditioning-waalwijk.nl;pixelarttees.com;freie-
gewerkschaften.de;dnepr-beskid.com.ua;eco-
southafrica.com;dutchcoder.nl;iphoneszervizbudapest.hu;allentownpapershow.com;bingonearme.org;summitmarketingstrategies.com;completeweddingkansas.com;wolf-glas-und-
kunst.de;employeesurveys.com;scenepublique.net;monark.com;seitzdruck.com;alvinschwartz.wordpress.com;knowledgemuseumbd.com;spd-
ehningen.de;boosthybrid.com.au;launchhubl.com;revezlimage.com;dontpassthepepper.com;petnest.ir;associacioesportivapolitg.cat;12starhd.online;jerling.de;kaotikkustomz.com;sarbatkhalsafoundati
on.org;solinegraphic.com;skiltogprint.no;craigmccabe.fun;puertamatic.es;mylovelybluesky.com;run4study.com;pierrehale.com;cactusthebrand.com;101gowrie.com;nicoleaeschbachorg.wordpress.com;arc
hitekturbuero-
wagner.net;mindpackstudios.com;vitavia.lt;bouncingbonanza.com;lukeshepley.wordpress.com;igfap.com;bockamp.com;levihotelspa.fi;exenberger.at;tinyagency.com;familypark40.com;alfa-
stroy72.com;boompinoy.com;mdacares.com;architecturalfiberglass.org;slupetzky.at;sinal.org;qualitus.com;deepsouthclothingcompany.com;groupe-frayssinet.fr;synlab.lt;kamienny-
dywan24.pl;ilcdover.com;humancondition.com;insigniapmg.com;arteservicefabbro.com;team-
montage.dk;iviaggisonciliegie.it;austinlchurch.com;rehabilitationcentersinhouston.net;zervicethai.co.th;vickiegrayimages.com;ziegler-
praezisionsteile.de;crediacces.com;comarenterprises.com;courteney-
cox.net;trapiantofue.it;space.ua;odiclinic.org;noesis.tech;urmasiimariiuniri.ro;8449nohate.org;xltyu.com;kikedeoliveira.com;remcakram.com;degroenetunnel.com;strandcampingdoonbeg.com;haar-
spange.com;pmcimpact.com;ceid.info.tr;gemeentehetkompas.nl;stopilhan.com;dareckleyministries.com;sportverein-tambach.de;ivivo.es;braffinjurylawfirm.com;pcprofessor.com;bordercollie-
nim.nl;hrabritelefon.hr;ctrler.cn;makeitcount.at;foryourhealth.live;seproc.hn;ianaswanson.com;nijaplay.com;brandl-blumen.de;lubetkinmediacompanies.com;ouryoungminds.wordpress.com;micro-
automation.de;apprendrelaudit.com;securityfmm.com;geisterradler.de;morawe-krueger.de;nmiec.com;sla-
paris.com;figura.team;vitalyscenter.es;jvanvlietdichter.nl;crosspointefellowship.church;handi-jack-llc.com;femxarxa.cat;wsoil.com.sg;xlarge.at;groupe-cets.com;admos-
gleitlager.de;liikelataamo.fi;sevenadvertising.com;nancy-informatique.fr;ateliergamila.com;stefanpasch.me;wacochamber.com;aurum-juweliere.de;hatech.io;centuryrs.com;ilive.lt;fensterbau-
ziegler.de;zflas.com;thefixhut.com;goodgirlrecovery.com;botanicinnovations.com;saxtec.com;tips.technology;smalltownideamill.wordpress.com;pt-
arnold.de;tarotdeseidel.com;bildungsunderlebnis.haus;brevitempore.net;imadarchid.com;sportiomsportfondsen.nl;digivod.de;darrenkeslerministries.com;smhydro.com.pl;echtveilig.nl;schlafsack-
test.net;galserwis.pl;eraorastudio.com;faroairporttransfers.net;connectedace.com;pcp-
nc.com;jyzdesign.com;suncrestcabinets.ca;offroadbeasts.com;teresianmedia.org;greenfieldoptimaldentalcare.com;thomas-
hospital.de;embracinghiscall.com;ralister.co.uk;rosavalamedahr.com;quizzingbee.com;richard-
felix.co.uk;sipstroysochi.ru;todocaracoles.com;shiftinspiration.com;campusoutreach.org;bodyforwife.com;katiekerr.co.uk;sportsmassoren.com;trystana.com;ino-
professional.ru;slashdb.com;selfoutlet.com;personalenhancementcenter.com;proudground.org;walkingdeadnj.com;d1franchise.com;anthonystreetrimming.com;forskolorna.org;brawnmediany.com;uimaan.fi
;journeybacktolife.com;pferdebiester.de;kao.at;asteriag.com;hvccfloorcare.com;parks-nuernberg.de;div-
vertriebsforschung.de;centromarysalud.com;asiluxury.com;chrissieperry.com;verbisonline.com;onlybacklink.com;radaradvies.nl;daklesa.de;sagadc.com;waveneyrivercentre.co.uk;mytechnoway.com;fitn
essbazaar.com;fibrofolliculoma.info;fayrecreations.com;maryloutaylor.com;whyinterestingly.ru;maratonaclubedeportugal.com;maineemploymentlawyerblog.com;kosterra.com;blumenhof-
wegleitner.at;punchbaby.com;wmiadmin.com;bxdf.info;harveybp.com;vermoote.de;johnsonfamilyfarmblog.wordpress.com;plastidip.com.ar;autofolierung-
lu.de;highimpactoutdoors.net;cwsitservices.co.uk;hairstylesnow.site;mymoneyforex.com;victoriousfestival.co.uk;farhaani.com;web.ion.ag;simoneblum.de;carolinepenn.com;blacksirius.de;trackyourc
onstruction.com;naturavetal.hr;heliomotion.com;rollingrockcolumbia.com;judithjansen.com;poultrypartners.nl;mirjamholleman.nl;baumkuchenexpo.jp;insidegarage.pl;irishmachineryauctions.com;inte
cwi.com;porno-gringo.com;penco.ie;jacquin-maquettes.com;anteniti.com;hebkft.hu;ftlc.es;dutchbrewingcoffee.com;behavioralmedicinespecialists.com;socialonemedia.com;cirugiauretra.es;c-
a.co.in;nokesvilledentistry.com;chandlerpd.com;aunexis.ch;gmto.fr;berliner-versicherungsvergleich.de;jsfg.com;vesinhnha.com.vn;joyeriaorindia.com;greenko.pl;cerebralforce.net;rota-
installations.co.uk;presseclub-magdeburg.de;yamalevents.com;renergysolution.com;roygolden.com;verifort-
capital.de;delawarecorporatelaw.com;jiloc.com;icpcnj.org;1kbk.com.ua;noixdecocom.fr;entopic.com;hellohope.com;flexicloud.hk;danielblum.info;thaysa.com;mdk-
mediadesign.de;nataschawessels.com;smale-opticiens.nl;charlesreger.com;kaliber.co.jp;almosthomedogrescue.dog;reddysbakery.com;waynela.com;ahouseforlease.com;binder-
buerotechnik.at;happyeasterimages.org;dr-tremel-rednitzhembach.de;mikeramirezcpa.com;zweerscreatives.nl;dramagickcom.wordpress.com;commercialboatbuilding.com;argenblogs.com.ar;heurigen-
bauer.at;ogdenvision.com;gadgetedges.com;izzi360.com;turkcaparbariatrics.com;spargel-
kochen.de;pridoxmaterieel.nl;heidelbergartstudio.gallery;ftf.or.at;kaminscy.com;filmvideoweb.com;meusharklinithome.wordpress.com;xn--thucmctc-
13a1357egba.com;tstaffing.nl;abogadosadomicilio.es;igorbarbosa.com;homesdollar.com;ncuccr.org;caffeinternet.it;abogados-en-alicante.es;evologic-technologies.com;oslomf.no;desert-
trails.com;gastsicht.de;nvwoodwerks.com;slwgs.org;vorotauu.ru;lionware.de;bodyfulls.com;myhostcloud.com;amylendscrestview.com;bptdmaluku.com;bogdanpeptine.ro;perbudget.com;strategicstatement
s.com;simpliza.com;innote.fi;365questions.org;sanyue119.com;walter-
lemm.de;cuppacap.com;teknoz.net;layrshift.eu;blog.solutionsarchitect.guru;parkcf.nl;themadbotter.com;upmrkt.co;modelmaking.nl;nandistribution.nl;ledmes.ru;coding-
marking.com;sachnendoc.com;thedad.com;mercantedifiori.com;artotelamsterdam.com;plotlinecreative.com;bauertree.com;woodleyacademy.org;dw-css.de;leda-
ukraine.com.ua;destinationclients.fr;jasonbaileystudio.com;cheminpsy.fr;devstyle.org;kindersitze-vergleich.de;live-con-arte.de;bee4win.com;fiscalsort.com;jeanlouissibomana.com;huehnerauge-
entfernen.de;eadsmurraypugh.com;fotoscondron.com;DupontSellsHomes.com;brigitte-erler.com;imperfectstore.com;shonacox.com;nacktfalter.de;devok.info;esope-
formation.fr;mariposapropaneaz.com;sw1m.ru;mrtour.site;hannah-fink.de;bafuncs.org;kampotpepper.gives;ampisolabergeggi.it;cuspdental.com;philippedebroca.com;abitur-
undwieweiter.de;hoteledenpadova.it;tanciu.com;delchacay.com.ar;cortec-neuro.com;theshungiteexperience.com.au;deschl.net;biortaggivaldelsa.com;fitnessingbyjessica.com;dsl-
ip.de;officehymy.com;shadebarandgrillorlando.com;bargningharnosand.se;mmgdouai.fr;daniel-akermann-architektur-und-planung.ch;xn--logopdie-leverkusen-kwb.de;buroludo.nl;ymca-
cw.org.uk;executiveairllc.com;allamatberedare.se;servicegsm.net;kingfamily.construction;nakupunafoundation.org;henricekupper.com;shsthepapercut.com;lbcframingelectrical.com;ladelirante.fr;cl
os-galant.com;dr-seleznev.com;siliconbeach-
realestate.com;tanzprojekt.com;fatfreezingmachines.com;kamahouse.net;gratispresent.se;softsproductkey.com;marathonerpaolo.com;gopackapp.com;manutouchmassage.com;marketingsulweb.com;craigvale
ntineacademy.com;catholicmusicfest.com;gaiam.nl;woodworkersolution.com;pasivect.co.uk;cyntox.com;advizewealth.com;y-archive.com;saarland-thermen-
resort.com;fizzl.ru;oemands.dk;mrsfieldskc.com;levdittliv.se;rksbusiness.com;sexandfessenjoon.wordpress.com;first-2-aid-u.com;simpkinsedwards.co.uk;the-domain-
trader.com;rocketccw.com;celeclub.org;urist-bogatyr.ru;lapinvihreat.fi;ecpmedia.vn;zieglerbrothers.de;piajeppesen.dk;joseconstela.com;carlosja.com;real-estate-
experts.com;toreria.es;analiticapublica.es;kariokids.com;leeuwardenstudentcity.nl;psc.de;tetinfo.in;ai-spt.jp;homng.net;em-
gmbh.ch;trulynolen.co.uk;oceanastudios.com;csgospeltips.se;luxurytv.jp;abuelos.com;birnam-
wood.com;theletter.company;bbsmobler.se;restaurantesszimmer.de;insp.bi;besttechie.com;autodujos.lt;chaotrang.com;galleryartfair.com;321play.com.hk;saka.gr;tandartspraktijkhartjegroningen.nl;
steampluscarpetandfloors.com;waermetauscher-
berechnen.de;sterlingessay.com;justinvieira.com;waywithwords.net;shiresresidential.com;naswrrg.org;spinheal.ru;slimani.net;modestmanagement.com;triggi.de;cityorchardhtx.com;narcert.com",
  "dbg": false,
  "pid": "$2a$12$prOX/4eKl8zrpGSC5lnHPecevs5NOckOUW5r3s4JJYDnZZSghvBkq",
  "nbody":
"LQAtAC0APQA9AD0AIABXAGUAbABjAG8AbQBlAC4AIABBAGcAYQBpAG4ALgAgAD0APQA9AC0ALQAtAA0ACgANAAoAWwAtAF0AIABXAGgAYQB0AHMAIABIAGEAcABQAGUAbgA/ACAAWwAtAF0ADQAKAA0ACgBZAG8AdQByACAAZgBpAGwAZQBzACAAYQByA
GUAIABlAG4AYwByAHkAcAB0AGUAZAAsACAAYQBuAGQAIABjAHUAcgByAGUAbgB0AGwAeQAgAHUAbgBhAHYAYQBpAGwAYQBiAGwAZQAuACAAWQBvAHUAIABjAGEAbgAgAGMAaABlAGMAawAgAGkAdAA6ACAAYQBsAGwAIABmAGkAbABlAHMAIABvAG4AIAB
5AG8AdQByACAAcwB5AHMAdABlAG0AIABoAGEAcwAgAGUAeAB0AGUAbgBzAGkAbwBuACAAewBFAFgAVAB9AC4ADQAKAEIAeQAgAHQAaABlACAAdwBhAHkALAAgAGUAdgBlAHIAeQB0AGgAaQBuAGcAIABpAHMAIABwAG8AcwBzAGkAYgBsAGUAIAB0AG8AI
AByAGUAYwBvAHYAZQByACAAKAByAGUAcwB0AG8AcgBlACkALAAgAGIAdQB0ACAAeQBvAHUAIABuAGUAZQBkACAAdABvACAAZgBvAGwAbABvAHcAIABvAHUAcgAgAGkAbgBzAHQAcgB1AGMAdABpAG8AbgBzAC4AIABPAHQAaABlAHIAdwBpAHMAZQAsACA
AeQBvAHUAIABjAGEAbgB0ACAAcgBlAHQAdQByAG4AIAB5AG8AdQByACAAZABhAHQAYQAgACgATgBFAFYARQBSACkALgANAAoADQAKAFsAKwBdACAAVwBoAGEAdAAgAGcAdQBhAHIAYQBuAHQAZQBlAHMAPwAgAFsAKwBdAA0ACgANAAoASQB0AHMAIABqA
HUAcwB0ACAAYQAgAGIAdQBzAGkAbgBlAHMAcwAuACAAVwBlACAAYQBiAHMAbwBsAHUAdABlAGwAeQAgAGQAbwAgAG4AbwB0ACAAYwBhAHIAZQAgAGEAYgBvAHUAdAAgAHkAbwB1ACAAYQBuAGQAIAB5AG8AdQByACAAZABlAGEAbABzACwAIABlAHgAYwB
lAHAAdAAgAGcAZQB0AHQAaQBuAGcAIABiAGUAbgBlAGYAaQB0AHMALgAgAEkAZgAgAHcAZQAgAGQAbwAgAG4AbwB0ACAAZABvACAAbwB1AHIAIAB3AG8AcgBrACAAYQBuAGQAIABsAGkAYQBiAGkAbABpAHQAaQBlAHMAIAAtACAAbgBvAGIAbwBkAHkAI
AB3AGkAbABsACAAbgBvAHQAIABjAG8AbwBwAGUAcgBhAHQAZQAgAHcAaQB0AGgAIAB1AHMALgAgAEkAdABzACAAbgBvAHQAIABpAG4AIABvAHUAcgAgAGkAbgB0AGUAcgBlAHMAdABzAC4ADQAKAFQAbwAgAGMAaABlAGMAawAgAHQAaABlACAAYQBiAGk
AbABpAHQAeQAgAG8AZgAgAHIAZQB0AHUAcgBuAGkAbgBnACAAZgBpAGwAZQBzACwAIABZAG8AdQAgAHMAaABvAHUAbABkACAAZwBvACAAdABvACAAbwB1AHIAIAB3AGUAYgBzAGkAdABlAC4AIABUAGgAZQByAGUAIAB5AG8AdQAgAGMAYQBuACAAZABlA
GMAcgB5AHAAdAAgAG8AbgBlACAAZgBpAGwAZQAgAGYAbwByACAAZgByAGUAZQAuACAAVABoAGEAdAAgAGkAcwAgAG8AdQByACAAZwB1AGEAcgBhAG4AdABlAGUALgANAAoASQBmACAAeQBvAHUAIAB3AGkAbABsACAAbgBvAHQAIABjAG8AbwBwAGUAcgB
hAHQAZQAgAHcAaQB0AGgAIABvAHUAcgAgAHMAZQByAHYAaQBjAGUAIAAtACAAZgBvAHIAIAB1AHMALAAgAGkAdABzACAAZABvAGUAcwAgAG4AbwB0ACAAbQBhAHQAdABlAHIALgAgAEIAdQB0ACAAeQBvAHUAIAB3AGkAbABsACAAbABvAHMAZQAgAHkAb
wB1AHIAIAB0AGkAbQBlACAAYQBuAGQAIABkAGEAdABhACwAIABjAGEAdQBzAGUAIABqAHUAcwB0ACAAdwBlACAAaABhAHYAZQAgAHQAaABlACAAcAByAGkAdgBhAHQAZQAgAGsAZQB5AC4AIABJAG4AIABwAHIAYQBjAHQAaQBjAGUAIAAtACAAdABpAG0
AZQAgAGkAcwAgAG0AdQBjAGgAIABtAG8AcgBlACAAdgBhAGwAdQBhAGIAbABlACAAdABoAGEAbgAgAG0AbwBuAGUAeQAuAA0ACgANAAoAWwArAF0AIABIAG8AdwAgAHQAbwAgAGcAZQB0ACAAYQBjAGMAZQBzAHMAIABvAG4AIAB3AGUAYgBzAGkAdABlA
D8AIABbACsAXQANAAoADQAKAFkAbwB1ACAAaABhAHYAZQAgAHQAdwBvACAAdwBhAHkAcwA6AA0ACgANAAoAMQApACAAWwBSAGUAYwBvAG0AbQBlAG4AZABlAGQAXQAgAFUAcwBpAG4AZwAgAGEAIABUAE8AUgAgAGIAcgBvAHcAcwBlAHIAIQANAAoAIAA
gAGEAKQAgAEQAbwB3AG4AbABvAGEAZAAgAGEAbgBkACAAaQBuAHMAdABhAGwAbAAgAFQATwBSACAAYgByAG8AdwBzAGUAcgAgAGYAcgBvAG0AIAB0AGgAaQBzACAAcwBpAHQAZQA6ACAAaAB0AHQAcABzADoALwAvAHQAbwByAHAAcgBvAGoAZQBjAHQAL
gBvAHIAZwAvAA0ACgAgACAAYgApACAATwBwAGUAbgBgAgAG8AdQByACAAdwBlAGIAcwBpAHQAZQA6ACAAaAB0AHQAcAA6AC8ALwBhAHAAbABlAGIAegB1ADQANwB3AGcAYQB6AGEAcABkAHEAawBzADYAdgByAGMAdgA2AHoAYwBuAGoAcABwAGsAYgB4AGI
```

```
gAgAHMAZQBjAG8AbgBkAGEAcgB5ACAAdwBlAGIAcwBpAHQAZQA6ACAAaAB0AHQAcAA6AC8ALwBkAGUAYwBvAGQAZQByAC4AcgBlAC8AewBVAEkARAB9AA0ACgANAAoAVwBhAHIAbgBpAG4AZwA6ACAAcwBlAGMAbwBuAGQAYQByAHkAIAB3AGUAYgBzAGk
AdABlACAAYwBhAG4AIABiAGUAIABiAGwAbwBjAGsAZQBkACwAIAB0AGgAYQB0AHMAIAB3AGgAeQAgAGYAaQByAHMAdAAgAHYAYQByAGkAYQBuAHQAIABtAHUAYwBoACAAYgBlAHQAdABlAHIAIABhAG4AZAAgAG0AbwByAGUAIABhAHYAYQBpAGwAYQBiA
GwAZQAuAA0ACgANAAoAVwBoAGUAbgAgAHkAbwB1ACAAbwBwAGUAbgAgAG8AdQByACAAdwBlAGIAcwBpAHQAZQAsACAAcAB1AHQAIAB0AGgAZQAgAGYAbwBsAGwAbwB3AGkAbgBnACAAZABhAHQAYQAgAGkAbgAgAHQAaABlACAAaQBuAHAAdQB0ACAAZgB
vAHIAbQA6AA0ACgBLAGUAeQA6AA0ACgANAAoADQAKAHsASwBFAFkAfQANAAoADQAKAA0ACgAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0AL
QAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ADQAKAA0ACgAhACEAIQAgAEQAQQBOAEcARQBSACAAIQAhACEADQAKAEQATwBOACcAVAAgAHQ
AcgB5ACAAdABvACAAYwBoAGEAbgBnAGUAIABmAGkAbABlAHMAIABiAHkAIAB5AG8AdQByAHMAZQBsAGYALAAgAEQATwBOACcAVAAgAHUAcwBlACAAYQBuAHkAIAB0AGgAaQByAGQAIABwAGEAcgB0AHkAIABzAG8AZgB0AHcAYQByAGUAIABmAG8AcgAgA
HIAZQBzAHQAbwByAGkAbgBnACAAeQBvAHUAcgAgAGQAYQB0AGEAIABvAHIAIABhAG4AdABpAHYAaQByAHUAcwAgAHMAbwBsAHUAdABpAG8AbgBzACAALQAgAGkAdABzACAAbQBhAHkAIABlAG4AdABhAGkAbAAgAGQAYQBtAGEAZwBlACAAbwBmACAAdAB
oAGUAIABwAHIAaQB2AGEAdABlACAAawBlAHkAIABhAG4AZAAsACAAYQBzACAAcgBlAHMAdQBsAHQALAAgAFQAaABlACAATABvAHMAcwAgAGEAbABsACAAZABhAHQAYQAuAA0ACgAhACEAIQAgACEAIQAhACAAIQAhACEADQAKAE8ATgBFACAATQBPAFIAR
QAgAFQASQBNAEUAOgAgAEkAdABzACAAaQBuACAAeQBvAHUAcgAgAGkAbgB0AGUAcgBlAHMAdABzACAAdABvACAAZwBlAHQAIAB5AG8AdQByACAAZgBpAGwAZQBzACAAYgBhAGMAawAuACAARgByAG8AbQAgAG8AdQByACAAcwBpAGQAZQAsACAAdwBlACA
AKAB0AGgAZQAgAGIAZQBzAHQAIABzAHAAZQBjAGkAYQBsAGkAcwB0AHMAKQAgAG0AYQBrAGUAIABlAHYAZQByAHkAdABoAGkAbgBnACAAZgBvAHIAIAByAGUAcwB0AG8AcgBpAG4AZwAsACAAYgB1AHQAIABwAGwAZQBhAHMAZQAgAHMAaABvAHUAbABkA
CAAbgBvAHQAIABpAG4AdABlAHIAZgBlAHIAZQAuAA0ACgAhACEAIQAgACEAIQAhACAAIQAhACEAAAA=",
  "et": 0,
  "wipe": true,
  "wfld": [
    "backup"
  ],
  "rdmcnt": 0,
  "nname": "{EXT}-readme.txt",
  "pk": "9/AgyLvWEviWbvuayR2k0Q140e9LZJ5hwrmto/zCyFM=",
  "net": false,
  "exp": false,
  "arn": false
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
revil.exe	APT_MAL_REvil_Kaseya_Jul21_2	Detects malware used in the Kaseya supply chain attack	Florian Roth	0x176ba:$opa1: 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 0x176b7:$opa2: 89 45 F0 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 0x176bd:$opa3: 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 0F B6 14 01 0x17679:$opa4: 89 45 F4 8B 0D 10 20 07 10 89 4D F8 8B 15 48 21 07 10 89 55 FC FF 75 FC FF 75 F8 FF 55 F4 0x17f0d:$opb1: 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC CC 0x17f15:$opb2: 18 00 10 0E 19 00 10 CC CC CC CC 8B 44 24 04 0x17f0b:$opb3: 10 C4 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC

Dropped Files

Source	Rule	Description	Author	Strings
C:\Windows\mpsvc.dll	APT_MAL_REvil_Kaseya_Jul21_2	Detects malware used in the Kaseya supply chain attack	Florian Roth	0x52a:$opa1: 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 0x527:$opa2: 89 45 F0 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 0x52d:$opa3: 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 0F B6 14 01 0x4e9:$opa4: 89 45 F4 8B 0D 10 20 07 10 89 4D F8 8B 15 48 21 07 10 89 55 FC FF 75 FC FF 75 F8 FF 55 F4 0xd7d:$opb1: 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC CC 0xd85:$opb2: 18 00 10 0E 19 00 10 CC CC CC CC 8B 44 24 04 0xd7b:$opb3: 10 C4 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.917270010.0000000000F60000.00000040.00000001.sdmp	MAL_RANSOM_REvil_Oct20_1	Detects REvil ransomware	Florian Roth	0x5cab:$op1: 0F 8C 74 FF FF FF 33 C0 5F 5E 5B 8B E5 5D C3 8B 0xad3f:$op2: 8D 85 68 FF FF FF 50 E8 2A FE FF FF 8D 85 68 FF 0xb32b:$op3: 89 4D F4 8B 4E 0C 33 4E 34 33 4E 5C 33 8E 84 0xa564:$op4: 8D 85 68 FF FF FF 50 E8 05 06 00 00 8D 85 68 FF 0xad2e:$op5: 8D 85 68 FF FF FF 56 57 FF 75 0C 50 E8 2F
00000001.00000002.917636237.000000000029A0000.00000040.00000001.sdmp	MAL_RANSOM_REvil_Oct20_1	Detects REvil ransomware	Florian Roth	0x61af:$op1: 0F 8C 74 FF FF FF 33 C0 5F 5E 5B 8B E5 5D C3 8B 0xb243:$op2: 8D 85 68 FF FF FF 50 E8 2A FE FF FF 8D 85 68 FF 0xb82f:$op3: 89 4D F4 8B 4E 0C 33 4E 34 33 4E 5C 33 8E 84 0xaa68:$op4: 8D 85 68 FF FF FF 50 E8 05 06 00 00 8D 85 68 FF 0xb232:$op5: 8D 85 68 FF FF FF 56 57 FF 75 0C 50 E8 2F
00000001.00000003.649759193.00000000033F8000.00000004.00000040.sdmp	JoeSecurity_Sodinokibi	Yara detected Sodinokibi Ransomware	Joe Security	
00000001.00000003.650121407.00000000033F8000.00000004.00000040.sdmp	JoeSecurity_Sodinokibi	Yara detected Sodinokibi Ransomware	Joe Security	
00000001.00000003.649936181.00000000033F8000.00000004.00000040.sdmp	JoeSecurity_Sodinokibi	Yara detected Sodinokibi Ransomware	Joe Security	

Click to see the 7 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.revil.exe.17a790.1.raw.unpack	APT_MAL_REvil_Kaseya_Jul21_2	Detects malware used in the Kaseya supply chain attack	Florian Roth	0x52a:$opa1: 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 0x527:$opa2: 89 45 F0 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 0x52d:$opa3: 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 0F B6 14 01 0x4e9:$opa4: 89 45 F4 8B 0D 10 20 07 10 89 4D F8 8B 15 48 21 07 10 89 55 FC FF 75 FC FF 75 F8 FF 55 F4 0xd7d:$opb1: 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC CC 0xd85:$opb2: 18 00 10 0E 19 00 10 CC CC CC CC 8B 44 24 04 0xd7b:$opb3: 10 C4 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC
1.2.MsMpEng.exe.6d4c0000.3.unpack	APT_MAL_REvil_Kaseya_Jul21_2	Detects malware used in the Kaseya supply chain attack	Florian Roth	0x52a:$opa1: 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 0x527:$opa2: 89 45 F0 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 0x52d:$opa3: 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 0F B6 14 01
0.2.revil.exe.1750c0.2.raw.unpack	APT_MAL_REvil_Kaseya_Jul21_2	Detects malware used in the Kaseya supply	Florian Roth	0x5bfa:$opa1: 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08

				1 00 00 00 6B C2 00 8B 4D 08 0F B6 14 01 • 0x5bb9:$opa4: 89 45 F4 8B 0D 10 20 07 10 89 4D F8 8B 15 48 21 07 10 89 55 FC FF 75 FC FF 75 F8 FF 55 F4 • 0x644d:$opb1: 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC CC • 0x6455:$opb2: 18 00 10 0E 19 00 10 CC CC CC CC 8B 44 24 04 • 0x644b:$opb3: 10 C4 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC
0.0.revil.exe.1750c0.2.raw.unpack	APT_MAL_REvil_Kaseya_Jul21_2	Detects malware used in the Kaseya supply chain attack	Florian Roth	• 0x5bfa:$opa1: 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 • 0x5bf7:$opa2: 89 45 F0 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 • 0x5bfd:$opa3: 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 0F B6 14 01 • 0x5bb9:$opa4: 89 45 F4 8B 0D 10 20 07 10 89 4D F8 8B 15 48 21 07 10 89 55 FC FF 75 FC FF 75 F8 FF 55 F4 • 0x644d:$opb1: 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC CC • 0x6455:$opb2: 18 00 10 0E 19 00 10 CC CC CC CC 8B 44 24 04 • 0x644b:$opb3: 10 C4 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC
0.0.revil.exe.17a790.1.raw.unpack	APT_MAL_REvil_Kaseya_Jul21_2	Detects malware used in the Kaseya supply chain attack	Florian Roth	• 0x52a:$opa1: 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 • 0x527:$opa2: 89 45 F0 8B 4D FC 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 • 0x52d:$opa3: 83 C1 01 89 4D FC 81 7D F0 FF 00 00 00 77 1F BA 01 00 00 00 6B C2 00 8B 4D 08 0F B6 14 01 • 0x4e9:$opa4: 89 45 F4 8B 0D 10 20 07 10 89 4D F8 8B 15 48 21 07 10 89 55 FC FF 75 FC FF 75 F8 FF 55 F4 • 0xd7d:$opb1: 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC CC • 0xd85:$opb2: 18 00 10 0E 19 00 10 CC CC CC CC 8B 44 24 04 • 0xd7b:$opb3: 10 C4 18 00 10 BD 18 00 10 BD 18 00 10 0E 19 00 10 CC CC

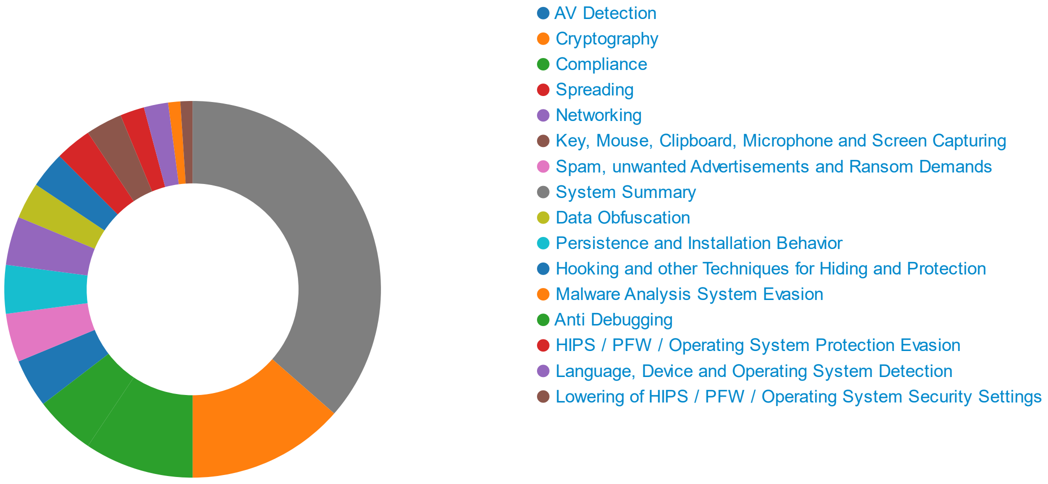
Click to see the 2 entries

Sigma Overview

System Summary:

Sigma detected: Executable Used by PlugX in Uncommon Location Show sources

Signature Overview



Click to jump to signature section

Show All Signature Results

AV Detection:

Found malware configuration Show sources

Multi AV Scanner detection for dropped file Show sources

Multi AV Scanner detection for submitted file Show sources

Networking:

Found Tor onion address Show sources

Spam, unwanted Advertisements and Ransom Demands:

Found ransom note / readme Show sources

Yara detected Sodinokibi Ransomware Show sources

Contains functionalty to change the wallpaper Show sources

Modifies existing user documents (likely ransomware behavior) Show sources

System Summary:

Persistence and Installation Behavior:

Drops executables to the windows directory (C:\Windows) and starts them Show sources

Contains functionality to detect sleep reduction / modifications Show sources

Queries sensitive service information (via WMI, WIN32_SERVICE, often done to detect sandboxes) Show sources

Lowering of HIPS / PFW / Operating System Security Settings:

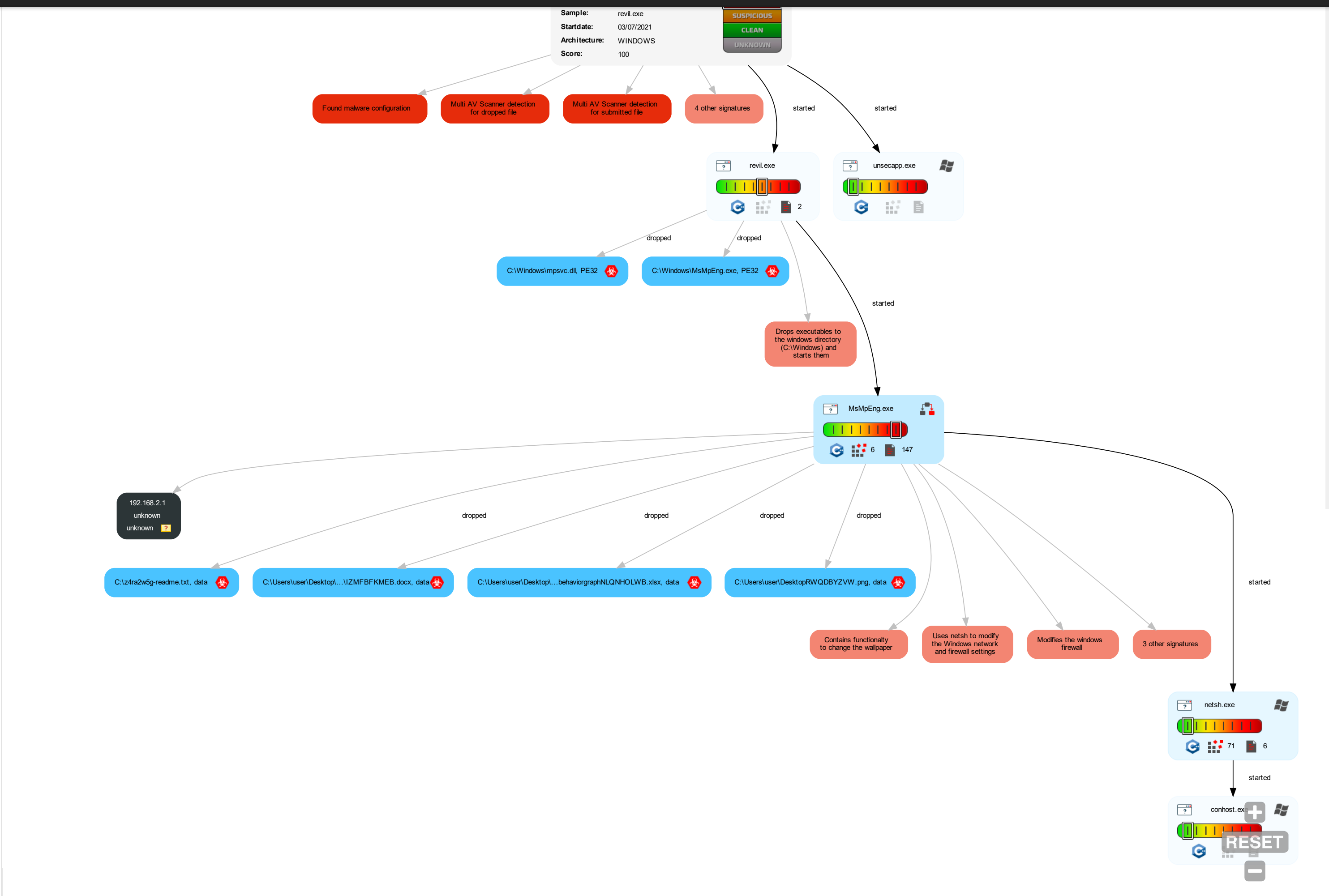
Modifies the windows firewall Show sources

Uses netsh to modify the Windows network and firewall settings Show sources

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
Replication Through Removable Media 1	Windows Management Instrumentation 1 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 2	Input Capture 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Data Encrypted for Impact 1
Default Accounts	Native API 1	Windows Service 1	Windows Service 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Proxy 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	System Shutdown/Reboot 1
Domain Accounts	Command and Scripting Interpreter 3	Logon Script (Windows)	Process Injection 1 2	Obfuscated Files or Information 2	Security Account Manager	Account Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Defacement 1
Local Accounts	Service Execution 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	System Service Discovery 1	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	Masquerading 1 2 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1	Cached Domain Credentials	System Information Discovery 2 6	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Query Registry 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Security Software Discovery 3 6 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Virtualization/Sandbox Evasion 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Process Discovery 3	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Application Window Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	System Owner/User Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

Behavior Graph

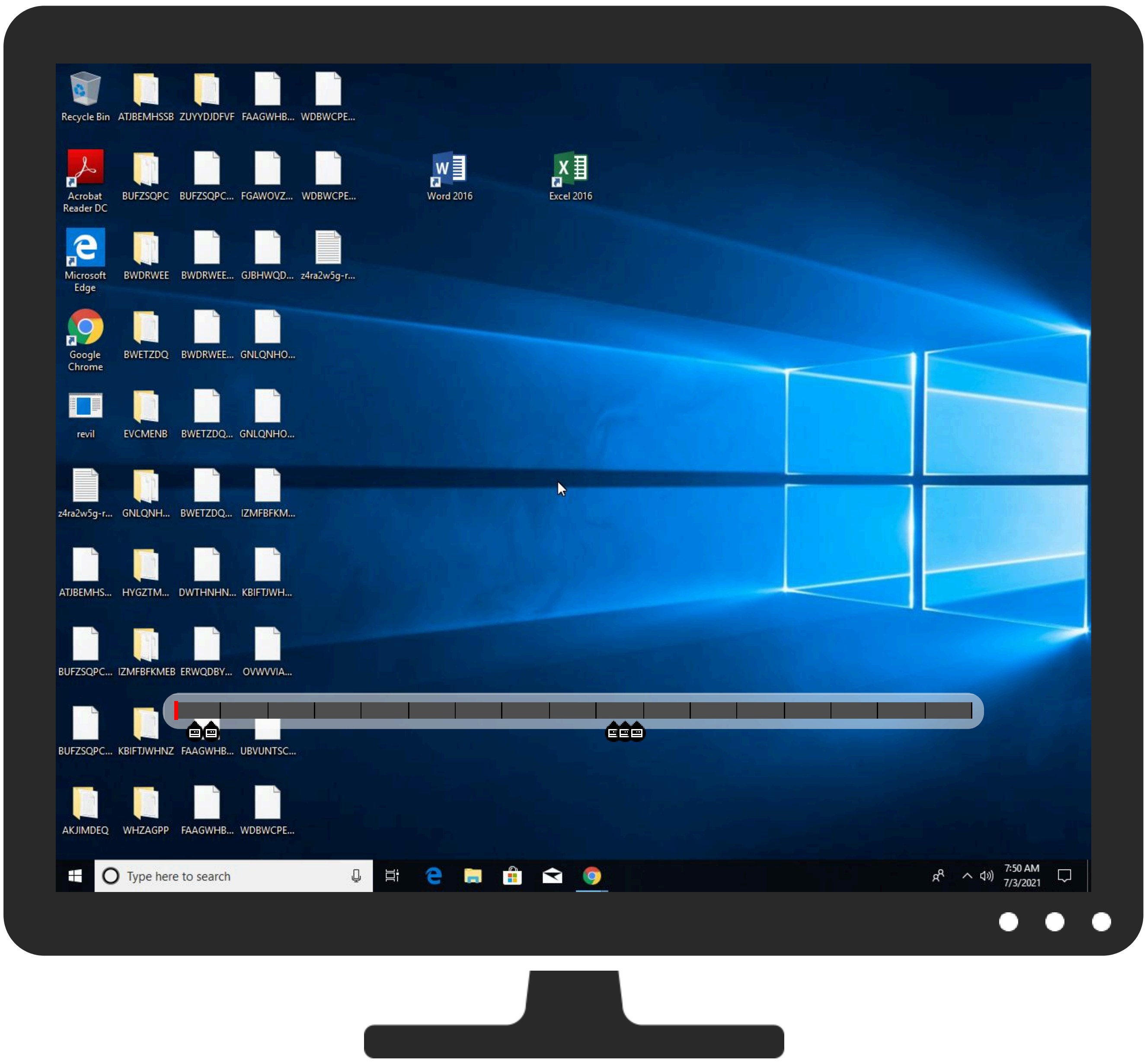

Sample: revil.exe
Startdate: 03/07/2021
Architecture: WINDOWS
Score: 100
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Multi AV Scanner detection for dropped file
Multi AV Scanner detection for submitted file
4 other signatures
started
started
revil.exe
2
unsecapp.exe
dropped
dropped
C:\Windows\mpsvc.dll, PE32
C:\Windows\MsMpEng.exe, PE32
Drops executables to the windows directory (C:\Windows) and starts them
started
MsMpEng.exe
6
147
192.168.2.1
unknown
unknown
dropped
dropped
dropped
dropped
C:\z4ra2w5g-readme.txt, data
C:\Users\user\Desktop\...\IZMFBFKMEB.docx, data
C:\Users\user\Desktop\...behaviorgraphNLQNHOLWB.xlsx, data
C:\Users\user\DesktopRWQDBYZVW.png, data
Contains functionalty to change the wallpaper
Uses netsh to modify the Windows network and firewall settings
Modifies the windows firewall
3 other signatures
started
netsh.exe
71
6
started
conhost.ex
RESET

- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Screenshots

Thumbnails

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



Initial Sample

Source	Detection	Scanner	Label	Link
revil.exe	48%	Virustotal		Browse
revil.exe	14%	Metadefender		Browse
revil.exe	15%	ReversingLabs	Win32.Trojan.Graftor	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\MsMpEng.exe	0%	Virustotal		Browse
C:\Windows\MsMpEng.exe	0%	Metadefender		Browse
C:\Windows\MsMpEng.exe	0%	ReversingLabs		
C:\Windows\mpsvc.dll	17%	Metadefender		Browse
C:\Windows\mpsvc.dll	30%	ReversingLabs	Win32.Ransomware.Bulz	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.revil.exe.160000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen5		Download File
0.2.revil.exe.160000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen5		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
https://sectigo.com/CPS0	0%	URL Reputation	safe	
https://sectigo.com/CPS0	0%	URL Reputation	safe	
https://sectigo.com/CPS0	0%	URL Reputation	safe	
https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/	0%	URL Reputation	safe	
http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/	0%	URL Reputation	safe	
http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/	0%	URL Reputation	safe	
http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/3C6DAF927BB6748F	0%	Avira URL Cloud	safe	
http://decoder.re/	3%	Virustotal		Browse
http://decoder.re/	0%	Avira URL Cloud	safe	
http://decoder.re/3C6DAF927BB6748F	0%	Avira URL Cloud	safe	

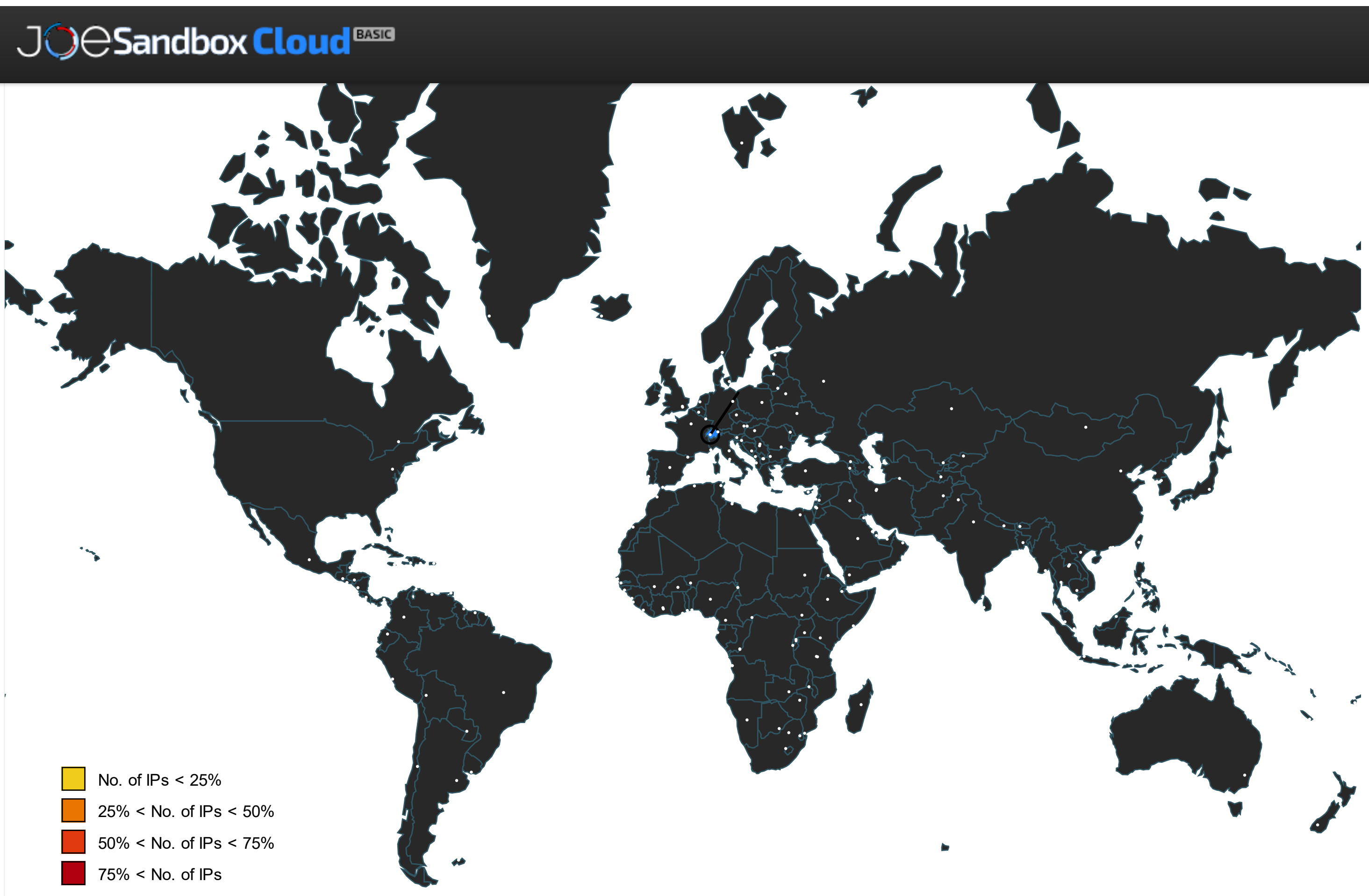
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	443736
Start date:	03.07.2021
Start time:	07:47:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 7s
Hypervisor based Inspection enabled:	false
Report type:	full
Sample file name:	revil.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.evad.winEXE@7/216@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.8% (good quality ratio 20.2%) • Quality average: 78.8% • Quality standard deviation: 29.7%
HCA Information:	• Successful, ratio: 84% • Number of executed functions: 77 • Number of non-executed functions: 67
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Windows\MsMpEng.exe	Broker.exe	Get hash	malicious	Browse	
	835f242d_by_Libranalysis.exe	Get hash	malicious	Browse	
	seu.exe	Get hash	malicious	Browse	
	srnmp.exe	Get hash	malicious	Browse	
	BORANG MAKLUMBALAS - SESI WORKSHOP DIREKTORAT.doc	Get hash	malicious	Browse	
	BRIEF WRITE ON EVENT IDE 18 JAN.docx	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\Microsoft SQL Server\110\Shared\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Reputation:	low
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Program Files (x86)\Microsoft SQL Server\110\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Reputation:	low
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Program Files (x86)\Microsoft SQL Server\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Reputation:	low

	.f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Program Files (x86)\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Reputation:	low
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Program Files\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Reputation:	low
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Recovery\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Reputation:	low
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Default\Desktop\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Reputation:	low
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Default\Documents\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false

SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Reputation:	low
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Default\Downloads\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLwJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Reputation:	low
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Default\Favorites\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLwJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Reputation:	low
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Default\Links\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLwJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Default\Music\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLwJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Default\Pictures\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe

Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Default\Saved Games\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Default\Videos\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Default\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Public\AccountPictures\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Public\Documents\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Public\Downloads\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Public\Libraries\RecordedTV.library-ms Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1231
Entropy (8bit):	7.84421496015369
Encrypted:	false
SSDEEP:	24:Zw9QADnsR3OZ8RqMc0yRLbcak5o01PBupDg9k7sEEZSDuutrOX+:ZyIRqMcfbBF0VBupDg9k70YNOX+
MD5:	3605E498D39CC19B0C788621211E2C02
SHA1:	C0AD795329F14602632EA440CDB28B94CAE35105
SHA-256:	0EC7C1749295F047979367EAF4B7FCBCC689421F513E8E5C6C04CA3B2517C389
SHA-512:	DD9C6C624CF0A8404BFC8F9CECB038EC730F6616AD94E59493D68DDF0AE4A8A45D3169A421365FE0BC6A62A211AD5717BD5AEB3F42BD9CAAD5340599E88CA0F3
Malicious:	false
Preview:	.Mv..p?.){.....Ri.......(....I.\.I2Y.6as........k.&.2.r.$..f.8Q....D..k..!X..22.^..b.*....AU....B......*!._..Um.......um.@DG....X.6U....O.>~.k8...?.$.j...{..T.gi+..OX..U?t.....7....]P8IK^.u..@}R>.\..}.q?(.......e..%.Y\.w..A1.!.......R.....L]!?NUl..t5.".2]Lx.[.i..H.A..].5.h@..T.*+.2.;<..?.<j.......ak...f.#ZGg%...6...-.6&..~...3 ..."\....+..........V.......\..S=.....g.:&.=...J.*8.G.U.<Q.+...f....u..".4.6G....k......R^.m.{...]5.D&|."eE.MP...&J6.2Ik.....5..v-;.....1._..O.z..".J.!...."...Z.|Yl.[.j.c.;.........up8.,.....m.M.7...R..A...r5.....ph...C..5......X.{5k......_...xVN.~^........m.7+.M......N..3n.y.g..K..zj..Hp.6.......:0RD...p.\....D.l...[..x.`.Net.%.....b...(......Q.N....j..~4M5g.*..$......y.+O..O...U...p.cP.b'=Z..........4.\|#.t..+.?@....*W..e..i....l..\.o*.a..9...j....z..;B...4...S...v.\|wFd..y$.[.r9<o..U..v?,..Q....$Fc$..K._.....:.e....2.J..?I...^..k@{..AT.I#.o.......|....)*.U...:.f=.}A]R;.i..>.x.....u4.....N.:..+.Rs..G`...2u.!(..

C:\Users\Public\Libraries\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o.

C:\Users\Public\Music\z4ra2w5g-readme.txt	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Public\Pictures\z4ra2w5g-readme.txt	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Public\Videos\z4ra2w5g-readme.txt	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\Public\z4ra2w5g-readme.txt	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\3D Objects\z4ra2w5g-readme.txt	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false

	.f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Contacts\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Desktop\AKJIMDEQMB\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Desktop\ATJBEMHSSB.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.858633400253478
Encrypted:	false
SSDEEP:	24:oQtt5u9ZJyRddIQpL3aLvQ2BKWt4NDP586rdS7q9uVwUuutrdo+iPn:3492UawvBKO4Im6ZSm9uV5E
MD5:	23120BE97892557DACF0C21259C7AA34
SHA1:	303134304838ADAD135918263AFBB2108D631179
SHA-256:	EADEE6430DA2DC7989EE585BF149E3FBE5758AF81A62B61D97CCF8B222B800CB
SHA-512:	AEE9AA0B2BF0EE0971AF7C0A2EAF23566F46AE7CB1071DD0C152C5348BCD8B582939ED5609A35EE42933A9F52767841C99D4BDE32D8387A08AF9D2AFEA3DD80A
Malicious:	false
Preview:	N..[_.....Sm..K...'>......m....D......>....%H....w....u...G..=........^.x).5(..n.^.q.......3.#%.Qq........O......o..%...!V..WCc.>...g.h.....=^....y.pX.[.OJ..l....dW.....c..6Xjo..w5.@.../..+......D...|.9... ...M>*`...v.],.0z.L~$.\|.{.4cs.F. <~b*...._L.X..z%..>..UJ.1...I6...tDj....T}.&j.2!j.B...."....'`3.._.>^v`.Q8*....~aT.= #.\..A...<so.z......M;.J..(....K..#G...BCJ...H...;9.sv<.6"_.j.;ZT.i...;i)..g...Tu:......n......+....{S.....S8.8t.....o>M])..2q.~...1.....T..}L......Y......$ ...b.y..x.:....'P...Jh&{../pGj`...EZP..^...s...... ...0..\z;=..Hn[...vS..H .5z....&.bO=.}O}.......L....t.x.4..A...K..G.d..S...C).....f=....."'#..b..QD..I?6...j...~....C#...5...'WP...g.X.JH.7A..........)M{Ne.c....F;......S.{.].TQ...5b.....W. .0D..GN.k..m..9.......m.%...{.]...Dl{......56#..Q.PO1...#.&...~}23[.X..}...MZ.V.y..-i.5.~:).EX....E..3CLj..O.f.4.G.2....u3....^.m...&...j..o.. [..`>.X`w......s...}.A0.*;9ah..%..$...s.p.E...g.......)....t.qs8sN...B'X..

C:\Users\user\Desktop\ATJBEMHSSB\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Desktop\BUFZSQPCOH.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.839763269040904
Encrypted:	false
SSDEEP:	24:xIrST0PI9GfbVzbowo8/1p4oIMHnMNWbN3elcurN47jVAOmrVAvGqCBMDBvtuutr:RA9YzRNCoAWwlcu54nVArAvGVBMhbL
MD5:	8DBA82BFABBC61E73BC48F5352C36D7B
SHA1:	2D1451BD734861B9F2E283A9C049508120534D45
SHA-256:	B3970E791BC62989D7342159E29596F19D3EE7F2EAB95F05807F8BE10729EBEE

Preview:	~..+.-.b..nU.Y..9.1..,.5gW.=..2"&...n.Z.....F^..W..~}!.I.!.=..V..)R.*D...Y...w...v.}R[..78.%...&e.S..}...V.YX.TWF.|..|.n.YQ...V...]..B..J...K@.7^.{.Z...t).X.,..u.X..4......)C/.0.z...+.p......W....S..n9wV.L.....a.\.8-..{I..8.a.m.+ g\.:......].H..G`.....u.nB.?...D..#{c...M!......D.......gZ.Z&..V"!.8.+...o.............<.....o.C......L.nz/.~...^.`H...d...E.&N.S@...Yb8..O.j...:K..).Z..Q.Z..P.q......7...5..c...-.(.x..4.R..po....\......bJ.'..Q.~......[3<8...-....'.:...... ..:A..x..Dj..<s.s.e..rJ......R..U..|.Q#...F....v-..V.C.x.fk.....~...%.;>.2.r./.B-3..n...Bh.....<.g.....HO)L$.......+.U..$......eA. .yR$.N...6......../.v\.^.....O.QiJ.....i.u.....M.<?G."x...}......,.U.d.Ck.]m....F...K.*..J....^W.x3 w5#3.S..U.>..,..%.S.2.L...-.Sv.f...;..0...j.@.}|.......*_.`i.P7.ls.9.......xj..../.J~.1...7U".U...LV...A{...[.....>.......&....D..i-Dl?'.H.......'@.../.}Dh'..*...i..v..m.BXD./...............U.r...'.....V..G..3..X..9f"?...o.......vM.qwL

C:\Users\user\Desktop\BUFZSQPCOH.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.852685188384449
Encrypted:	false
SSDEEP:	24:SA6smki4Kf5H/OlWrSuySiENb420UlcTjn7MhUEsnrBIL+4Ko9xuutrJW:D6smJ4afT9iENb420Ulo6iBOoNJW
MD5:	C6E39D16B07B564A5E519289C7698527
SHA1:	FCE41534B206A04F111518B4BECDF529A5E4C302
SHA-256:	C36132E75FB2B4D79D439951953C7888E377D9DBA1E47D764E21ED3CC7C11267
SHA-512:	B307D8EE964ABAF89BFDD2DF8DC32A5F37566A7C9130D4DFC4E622EFE13011A675AE67E5C413D298ABB008D38F5792BD95B53B8D65B4F10A5D4B5438CF24D78B
Malicious:	false
Preview:	.#.&m...m.|I.R..T..cNf..Y|H.........G\....D^.2..F.9..M..8MY..F..}E.9.D.....H......7...5U}.#A:...`."dy:o>-^F.A>o.....KA_.j.M....u..J.K.r.+=.*.V.........,.4.T.......|..iU1!....er.G.v....x2.@=7AV.......:._{.wN....`Gr..a.8...Q...'A.B. ....&#k.....n..n(..F..E6{p...\.Q.n.d.i.F..?.*.+...V7^:..B.."......v..[.\..xu.2.YR..:P..].h..oBD...;.....!.....h>._.N.X2.\..7r.......Zn......T..9k.@.!...3{..z|/g(._...|^.._.3<.pX.QJ.;..3.3...`.{.^SV....F..Dz\S......8..@6.4.....Y..6{.. ..~.)q8.m.....>3.B...G.<..9R:.-.......I8fv..14..w'..C;....=.)....?.s@......CFi..K......9B..`..2N...~k.(....h0.+...-t.E.IRr0h...'@O...\.gV=n$.s..Y{.....)..0.+=a..b.B.........E.{..4.........-I...w..J.\|K$.h..E..(...R..;..jXw..8<.F......X}..A. 8..z.F.I..."R./.. .UR.J....,..*!.jc....&B1.J./..h ~...2.. ......5#X.h,.....e....hHr...>..[er.X.%KbtB.WO..g!..B...u...B*.x\...:.......u...g...!V..o.=.>Hb[.Uv@a..^hXy.....#R.=.(....!....dDG{.....I...<F...N.....s!a...Qn+..5[.V...k..E'..

C:\Users\user\Desktop\BUFZSQPCOH.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.852864156723663
Encrypted:	false
SSDEEP:	24:DQVYV443DxbJPCXy8h1WkHK9X4P5AdHr/3b2kR7dFlipuutraP:DQVY4SxJC5hEkMBr/C2lcu
MD5:	61BDC8A7B0EFEC3BD2EDA66034B55344
SHA1:	34C0BE4F6CBF6CA2F1EE0F3A2C80D176E2BFE7FB
SHA-256:	559E3F400E4727571E3D0C67CEFD58FB3DCCA40FED18D747823975A57D24457D
SHA-512:	117590A7339430D4D915D0D5FCE7F48764AD9670BF1C08E66E55B2B271F63F80D7CAF79296E008E3F53E840E330CCF29B45345B4F9E970841899AE96962CFE2C
Malicious:	false
Preview:	.{j......yu.?.b.P....Y?#.I.TF...eP0..].Q.)YT.^.....................8...T.W...H6.]u;.. ....g/..j'..&6..p.P=..q.....Qu.e....~..}..C......N.........T..R> ?.w..Sm.}"..rs..A...o..5.....i..o...x .....j.}.b....P;.....=....#...b(...5MET..<... .f.@w....6nx|)....0'n.io%.....@}.........S.I......f..f~.4.WI[0.M...px..pA.....<'.z.A..R.N.r...dq!..8..!..s.....>...*...'.iP......p.N.....iB.N.Zk9..A.O+.wM..I...>...n..f .... .H........v,*.!..d.h.[."....9=b.C:..{kF.s....^..!...F...`Z@..E.... pz.m.(.kv}b&.m k.@..@.....M......p....dP.^>.g$.CA3.!.....[?..]...'.`..I.[........E.k'......%..9.)...a.....[yA..`....h....bj.(k..q_....b@...s.]..P.....[....Tlhi.5..w'.?%6...W.....7O...uh".~...L./HPG. ....o..3-3.P..YGi.e...1....~).. k..xXj.c.....?..dl..%..)...69c..~.T8.]RF![...M.c./.;'....t..V=..[`QQ..z....(...6.....:;@L.u..%.K..n.....J...w.^./F..7K...Ds.t..Q.%.\..'u,j.....~.zR....{+.`k.,.C...\Y.m.&P..~51H....*7-........6...;.t^........I;9+>x...#.Z.i.P..,....3.|..MS^

C:\Users\user\Desktop\BUFZSQPCOH\ATJBEMHSSB.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.846970649974634
Encrypted:	false
SSDEEP:	24:8QTFJewf5Gvc0kRZQXA33tmvxldbP79SpU61LIWsjtX47hmdfouutr0Q:lJLfic0CiAHov9Ri54sjq7hmBq0Q
MD5:	0247FDCF24909164CCCB15A539AE6D9A
SHA1:	8C0D1DDEA735AB0C11F17E7A64675E4E133681C4
SHA-256:	0C0D8AA0BA6005E09C5F557F78EC1513652E501B1BAE1DC04CD879F7F1F7975F
SHA-512:	3FBB5AD78645027A7750C34E730DDF5ED2614E65C60DFA585CAB3CDAEED0B3E1EDA5EE670EC157D3666C7E8280C0CA71BB31DDB6AC8717BE971C39114678F77E
Malicious:	false
Preview:	.CbZ.}I@.s..5m.$(@O..+..?/....F.H.t..>..J4...N..mK .A.....N.X...0%..;p...B.7z..EY\|./...0..y....%:.L..`...>`...........g.j...b'b.. ..Sz...@x.>........'.j...mg..h...%.n.....&=4.8$OupA.#.N:..I..[x....H.&!...a..w.. /.=......a...yy.(.D..z....q.jb..h.Rc$.?H....N.-tR..V5:...;...+%.@4........k.....C.9.........>......L.......w.h.....$-.....hr5...-"..A.?o....Z..N!.iR...../y..W.So..se..R..,/6...f?.(5.H.=...&hf ..p82..T.As7.{}|..S..3..vi...<..*<...RN%...B.....KG..O3 ....1+.D....../E.G.a...*../.#h....}.g..e...H...@...^y...^.0...,.x..q2/Z...u...A....O.,.}.w.......c.....].:..`..8b.'.*Bh.=....p>.}w..h...#...D....H.z.'.}g.e.Q..o...%....L......c.H.)G..@pL.$.....Wp).v../..........be...h$.D..S.#.46g?...0?.a... ...%....a.L.f.LN..A...H.B.R.f+b ..v....N6...rX.B..WM.+...Bd..*.u....5.c......A.P.*<1..MV.;h._.=<....F.:.....4...n...d.=5.P.,+<..3....:5f...&......H...y........r.R.......s`<..>..;t.&.UD........U.&j....R.\n.Jl..Q ...,.........F..............I .CR.b.

C:\Users\user\Desktop\BUFZSQPCOH\BUFZSQPCOH.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.865268017099501
Encrypted:	false
SSDEEP:	24:S+q+Sxal81TaMIDaFqvQhQUzSkVffOE/S0mORztRBC6lWuutr5Log:pq+SxoMI+FqvcQUzSof5/SZ+BDC6/V
MD5:	1354C6C87D42A64530637F5C79EA2336
SHA1:	E5B0481BDD4E630CB13C5BB24AC11221D29D86CD
SHA-256:	2E60852A5F449BB11D493B2F1071CDF29652BC2892798D1F1A51FC652C057BC4
SHA-512:	94770CCA0A1054935A7E56B1BE31F5B3F8552B27E25D3D1A6DA899A7A4184C779EF659ED1D5AF4AC5674DFDA7F0F1C016E8C40855E72F4E4BD1E7333F7EA5EE6
Malicious:	false
Preview:	o.8...`.4.u.&5...3i:O.......I./...t3....../.&..7\..ON.n..L..<..p .......u'.%.....p%...M.......@;t.W..".Ejrt..[C.(.}A...bk..IBX.3E..4..R..|-y....JA.o.7l...].....N.8..;r?.&..{.Y...W..'W.E.['....&n...>..V.o...#bZ...Dd('..|JB.g.a....\+b.. {.P+m.g..../.]..t..s..i.>._G...>.F).q.Y.` .\......"..f^..FA....<..K.R..M<.....2.T....1.....}D.N[.2<../...F.4l....R.H.....).s..Cp...........C.A.W.^.L.n8@F..........p.<.\..q.a.....?...^W... ...].%E.s.q+.622@.P....%,.(.l..m..eDe.L.n...g.w. ....Y.Hx.|...@:>...o.`4..iJ.aB....v..ka._...Y.H..C.b....D....._7E0....-ibWf.Y.^e..D,CD iR^..!o.........Z...6&N.6j..S.....U....%..)k!...h...S*8{..'....;u..,...n^.p.x..X.r..N^+5.v.......D..V.....0d=..i.......'2..D.,0....H.+.o.f.f..,.s^*..).k; ...Y.a...e..l.c"`.....Q.-7.d.:...:^..1...{9ke9.m>........\Ok..`.!..;..gH.B./x....m..n..l.7X.4UB..^..;]<.......pKJA*W.b.@..B......I/X.t..l.i.z9.........l..+.}..xB .e\....c.i.2.f..,Z..}ei.-..JY........z....j......."..#4i..R%...Ha....=.Q.-....c.

C:\Users\user\Desktop\BUFZSQPCOH\BWETZDQDIB.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8454966142244436
Encrypted:	false
SSDEEP:	24:TAAJPIXZoerKleHdF4tXDWM3ALmk4qzIqVBul6Muutrtri:DJwpoEKXHH4tXDR2mkNzIqLul6uc
MD5:	0A0A0639D3A14257AAC9AC4012A4B010

SHA-512:	F08F0931045 1CF3AEB1348DBE4BF431A4A72F39787058BAE77D632512D1CA4DB805D4889F247256965DB3630F26B24D77E283896FE4FCD20B51D1D0BDD1E25A7
Malicious:	false
Preview:	.`X............/cd..r).&..f..........T>....)....=...@...Q[.V..........Y.]7...E.....M..U...........&="7C......?o...Ba......z...qh....)p..~...<.N..S'...P...h].9.m.U}.M).k+.1.]7.....B..@.P.cvnm.e.!...B.. 5.(..{.{ HGo..).Q$..).N...-....."....$ O....4x...."c.{....C...}..K....rmK..\....J..k.f.....X......f...[...;....k....h...5..^..f...l..j.Q......^6...y..X..`.L..I.E...-.);v.Z..}?XpX.G........59.6ur".]..8u(:|E.x..q!..b>..<]a..,{...F.%..h..Kw.....N8..Au..........0.c.pQ..:..*Q.:'ae....u.[..a.... ..../M....^.P..T.@...1....,.!....@u...)!]eOv....vHo.[w........>.k....H...7#.^....w.:.6.j.xq...\...s..c....M.x..-|c7......Sq..s..@T..V....B..}..@...m.e...F.Oz.b...@J{F..@..A...x.m\..h!{-e}."N'..@.<.^{...qaE[....f.[.kj,*u.A...].y..!....(..T.. ....-v,A'N.8*8k.G.k.*....$v.M.nJ.~=.". _Z...Ai.$.Dk...7.X...l...8.LR....x...Z.......F.\c?.Q[.C\{8V.."5....F-y.AA..\.1.,...=...u...]X@.dWg..*f6.Tv....^N..xA$C.v....>`..9.t.c+<.z.E.RW q.)7....^l..t.o...6.;.T.V..V..".X..`.f.i..^..:.

C:\Users\user\Desktop\BUFZSQPCOH\DWTHNHNNJB.png

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8341692532083425
Encrypted:	false
SSDEEP:	24:2+PTLP3Jmd1lfgMoR6irBCxcltbd8pyejguutr3wB:2eBmBS6QBCUztgB
MD5:	62B638A546427A9BF6DF86004197AA63
SHA1:	977BAECB8EF2553CC76616E6A02B39FA6EDCBC9A
SHA-256:	FB7C024E1D2F8DBEB1FE435D282F1EFFF440F7716744FD3BC2F6A7D21A36BDB8
SHA-512:	ECC476CA6E1A58B268599D612AEC16723534A0A48487BE9EA474B44AB03D52E7EA49546479BE2F55BD4C2E3DD58792EDCE909D8B9EB1FAF3B20E1FEEFBD9B801
Malicious:	false
Preview:	y.x=............x2.qv....F.R);.4.....s..T..Nsf.@.u'.....D......k.....n...;....."..i...1.o..........H......G...%...X>.......f..6d.=...1....~.......(}...,.`c.{.N.9xH.o.|=9.a../.._.!....EnF....x...Y8.Ca.m.QL....3.H..L_.%J.(...x.%..UZ(:K...l.s .l....."i./]z."..%].q;.....Xl2\D.i..qx.....WzC......F...D.Q.aQ.*.^{.T..23....C?l.c*+....<..a.H.s.......,nzW..W{5..^.:Nt...'..9..t.A*Gm.......pX.....{..2$..=..}@BG%Y..j.M.-L.d.D...D...-.m'. $..`..-.....jRn...)`.z.["l..7P.Z$./..n.. Z..V.V/U..?PXKu.*%.*..@-..........i...<.9E: .U~.[...T.T....eB..p_..e..D.w.4q....K.7g.!.a..!..*...G.j`b....'.............&..6...~...p....i..m..O.#...;...L..m..;....*..n........!.*^...BKEa..Czt..C.?.$~t.1.L...l|..=#K...X..1.5..e..u.T.....Z.). .x.D.y.l..n....X....G8.}H.......H.n.aWb.W.....m...2....L.Y.OY...G.q..*.3a.....<..D_"...&.Vx..Xv^>.A..F....'..cG...u..7.....U....{.G%....n..[nM.>%....kk...\t...E....(%mT.f.!.d.b..n....SD...G.C.d.{(o..M...B.A...W.&].'Ea.../ .=..J..7;.{D.h?.....

C:\Users\user\Desktop\BUFZSQPCOH\KBIFTJWHNZ.mp3

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.836866160861808
Encrypted:	false
SSDEEP:	24:ik5DSuE+JKV1I+4w+b709qqvH5AqhVMCRjb4KF5BDuutrx5n:ik55JA1I+BDznicj84xLn
MD5:	46209687FBCF150E4D286F5DCB7C0E4C
SHA1:	DFCA987BAF7F81A187EE2453DED687A24982386D
SHA-256:	FCC6C8ED059062491BAE4FD3983441A97EC12D53B9E7CD7E97E978452219E81C
SHA-512:	B50CBDD8E1BE6E3BB914BECE342EF7C9532D013445E0D2D4A5A445EB295062538693AE8B755B5E7BA9C796F8AC7F6D85BAAD839E582B8211A2E17B657FF73A19
Malicious:	false
Preview:	......I.U.)..D...`..)D..%..e..xi.VE.c.V......5.r;g....bE.R.o..iF..0.8.iX.>n.G.....Y.|...o`.W..t;.7..%'|$2C......l6~#.".T....uN.)..nyVJ..o7....c..h.... (...;{I.._7.\$8d-...!.f*9%5.a.8kn..........+A.4~.D9*[."....o V.F..."..Ez...D%...j.n..I... 0.Z....^..>.T.._..n.......98)9.k,.[....d;.....rg...b~.bR.%S[...!.rf$%f..}J...[.E....*..W._......^./....DG........!...#.G~....v...>.._..?.2.c......>;..*.....=`w....v..z..8F.b.w[.!.#......]...v.......~....k..cj.....>...R.M....1la..'.uJa..K(.. @l,7.m.]?.Z..+_...:z...D..iuWDg......."..Z...OS.6(.p.8.....Y./..[v......s.....E;v...>....X0..8Y..s...?4.y..m...h.A.%.p....B.TH..E7.....#$s',...4s....1./.`.<h.....L...;.....B....6v.9.1'.9.J^xZ.......1.q=4XW.IY.../2.D....%5...n.yP.8 ...2.FwM.........2.1.....r...E.Y..F8....]....A....).2e.......7.bQ<.. y....?z+b..G"...*:B..@..q+B...v..\3..J.......0.Bxo......r).83.....0!u..Z7...R.*9F....ZV..C9.QA.....urf.o.............u..........l.k......Bt.....:w..7.>...0..}.O.%D

C:\Users\user\Desktop\BUFZSQPCOH\WDBWCPEFJW.pdf

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.852305750635348
Encrypted:	false
SSDEEP:	24:HHIBgd1YcXuZWsTUgsE+yft7T7ukcW7hacKcBM7YjX6uutrZCJ:n1XYzTfNftruCdacKcBMSQZ8
MD5:	A7B2EEDED3D238CBCC9E605C2BA65B1B
SHA1:	CCFAC007EFABD58BF327F64E51B2495D8CD9C56C
SHA-256:	4AC2821A7702A5794DBD7FEE69B2FB375816604A63D8AD0A23E53CC4857A8F6F
SHA-512:	DD0F52C9E9218B7911744B0274B1E36FC2F3B2F73F29D0D611CF9BDFAF7B4AE5728925381DC62423E6E969EA07B976A80BA062239EC3EA943565A4FE8CF9D6F7
Malicious:	false
Preview:	_..=y H..&...".x;...54.fk.G....*).....|Hj.e9b&\.......M.Y7?.+..hJ....>UK ..6.ve.....V...@...&..|ba...6.2 ... .UOAVP.L_7.%..e1.n......V..[.m..%.....:..>...3. .....;..G.g.x9z.:.#....K..c.4.E..up.....{....7.V....`....t'&.;...... :.f..^.V.,w....Z.(z^/*.2..R.J...w.a.?'u......T ....X.p.A .....]_./....k....x........M........}.....n'..l..).u{..M.K.iLC.ceo#V.Gr......L...d.3.1S..?...|..W..z[..+...*... .:.S.*.L.......S..2.*......LW.Z\#..__'..W......i./3h..<W~[.Om...$....kq b..G0N..{..e....8,g.2..<s.D.s)P.......%...}_.....P..~IWI..i<...@E.z.4....`#.r....meZ.1...(.0nx....\...r.A....\|....t..\.@.......d.S..*...d_.T.5..7....../P.{g......a.7....,\|.......&.".<..\|.L~.M%8.....$t...C....@V.R..].c..!l..@....,Cv.V...[.O\ .2.T.8rO..v.=...../-.).1..<)X.>)*..e)....h......(l..b..f..T.k.....g.......&34.8...]h..;.u.6..vg...-p....D.......-GlQ...4..g.s..Z....|.:...hxU.MFP......5..............W)9..e_.Bqn%...U.cYj.)W:?{...^dpU.w.....Y,.T..+.QV.....M...^R.5.1...

C:\Users\user\Desktop\BUFZSQPCOH\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Desktop\BWDRWEEARI.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.869192329356546
Encrypted:	false

SHA1:	9F1791114185B9AB5510401E93A824EA911B69ED
SHA-256:	3FC9559D889C6EBEAC6E6F8264023BF293F7D344EF589DC1F352CB61590DE5A2
SHA-512:	A13538E5C17E2FFE283DD5D5FF2045C44AFE93AD5EE414929B2D1896A008EE52E0AC991AD25BDDF027862C9EBCB4ABB499DA63F2226176376AAE4966D89EC495
Malicious:	false
Preview:	1.wf...\.........&4....;........`.i.........g..zF..j.$W...J..{}..;.DYj...".J..[..l2.jd......K_0.)'\..5l....]...C.....G[./.....y..E..?g{@...l.....B..fx..cg.k....t.....4......=G......J.D...qm.-..'.y..j.KST....).........7...f..l.=h..`.......w.A.m<.F>..W 4[....GU....Z... @.8._.s\..Q.....?...7Se&..........w.m.c.....H........$....Q^.poCl.E........n._..WN...).l7....hCN.......P...6l...sdD.4-s.s...-.d9..q..b...{.`....l.j1hf..........Z...l..egc..e...J.g.a.3G.t.c."..._.6)L.8.#.+...l.......37M...^U. *.........Y.{.j4.1..R/..0N...b.e...]w...2....<:.....t..u.v.M.NM.-.p.\q..{.KUW@........*...3..3:...\.U-..(.9.....gq..B.(....RJH.d.\....F...Y..O...QV#.3....ow.\....S...9.}.. .P>l...8N$...aJ0.......yAgc.~...z...l*.;.Pv..n.Y.xQ..B.... [U+X..>.G%.....4.Z../..1....U..1...U....s...c0.F.......7.b....<...F.....i.Y...........T...5X.(.S..'.AS..... ....&.*._j.!...U.9......n._...q .....z.?....C....|vQ.-....e..M.M..DV.52.;...z,..Z......X.y.mA..im(\.+:.J~.K

C:\Users\user\Desktop\BWDRWEEARI.pdf	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.821787033705641
Encrypted:	false
SSDEEP:	24:+v0nbJwYWiX8C1DQ2nNjLlnn1uLdS75KSn9qFPWuutrdbjA:+0nini02Nudl5KK9MP8dY
MD5:	E539D14ABA862510D66FFDE651540DD6
SHA1:	DA854C2692C4050F673EE84903EF03D6FF10783A
SHA-256:	D606ED4819D2493021E9BFF76BDA11DDB5F5903FF8186E886454D480DD4738CB
SHA-512:	8172766A148C88945E1D340E63EEA0AAE9DBA67EAA1EEC5B8BD11595D19B58B468B9238F72B3D0044BBDC4A5816BDC9760925485414A1FF64D2FEABE95188443
Malicious:	false
Preview:	....y....+..NL.W..^.......4..... .}p. *)|....l....j...!....K....x ..g.D._cQ.'..?.T.a!....J[:..0..n.1.B...............V..%..........l..+../bw..'..".jw.H9..~2..|4....0...[V.dM4..$....-]..U.'r.j..~<.m.gk..}.B<..t......."E.Su..[.N.;..F0......i.%^..y..U.g ..Q...9.p.:.'.B.!~F6..x..E..,;f.#.z..s..9. y.y.....U....9.p.{$.,C.%.P.&.cp....U.....X...\..G.........-cM5...U.N...GRH.5.jo...G..}....v.]...:........U.... W.......l....x.z.:.3yM...\...l....STd.h..(.A.F....(....g...yd=.,.DL.?.p$........]El.. ^^-.ux.4..9.NV..lrfHs_...ALMn.o..&c.4N....T..(........2.d./Q.fej........q-0#R..z....O....E..GZ....Rg..-..W0.B..3.V..LC>.bdR .%`~.......=w@*=..n...Zj....T...IW..oHv....j...,..:*.@g&0.=......Fg...(.3.O.g........@....n1^1T.|0..P..T... ;U.......n....SS....Y...1./.a.31..QZg......4&..l.Wkc.@.6........F.,.V..t!....6<H.w:w..3C.v.....R^..f.L..>s..:~v..t....g........S4=..PB..t......j.....q.v.".='....+...}T.....i...d[....>wZB..n. .07.dg....xwg..#.1...G........H.....4

C:\Users\user\Desktop\BWDRWEEARI\BWDRWEEARI.docx	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8289657125032015
Encrypted:	false
SSDEEP:	24:Dpaye6r8rwFYxDSaHTMZEBMzuRksAFeXv7xHcz5uutrdy:1ew+xejC2uRkPFeXR2/g
MD5:	DCD1154FA859DF393992333A33EABB6B
SHA1:	93C7AA3B51E10DA37609CA10307B60869BDA8FCB
SHA-256:	AF2A62760283C4F85977328B0AE71558A7C78FF2D2BE67DCFC5913D9FEA994AE
SHA-512:	F57C50AEA9A33070BE996E7BD4F39CB7AB7C36FF93011C24F61A344FAFCDFAC46484E463C22820BAC4959BCE9BE7638B437FDA101A815B15EF328F806766FB12
Malicious:	false
Preview:	.C1.M.C..:u...wm[..".{..zXH..$.+.y....e.O.HD}...z^u-}.p..L.f.h=O......`....v.N.<...3.r..u. ..n.%.Ay:.....8B.\...@G2....Q....l$..C$.%d.H.%..A..8,().g....,...Wz.....v[W.c.u.{C.e.x.t.....d.^.G..*.#o.m"gZ....-..0.....Q.).....5.9.....q Ly"K^.m."..1.....9a.a.1....."..L%.......y{....<.}Jqm..R...7?V.e......["..GiC..t...6.\z..t.^<...z.w!.f....S..y.5......;*...4...1(.lK....5.K....X.....]n.Xn.hP..x^K.#...0......q5i....rX.EqC.2Ui0...[U.....G.ho+_..............,'.w.1+...nF.....Ry. ..9E^....t...m4l...r....ZO!........9.LTt[..Y.OM.../....... ...:..e..<....Rj.x..5h..A..1<l.il."z...9.C.:.1.......).Q^.E.`[.5.V...9.v.....,........d.h.....rEE...EP.{...<z=."tR?...`....T.4.\.......9.L.i..b..=V...t ....w.n...........{l.\...*..?.n.".-d)......:..j.......z..H..W.+..;.H...r....F.;.A...X....!t....+.....A..C.R!....)..5..+.....U.|....6]...7Y.J..P...w..Xr+2!.^.....C..3.4.R.PH.....(..+_..7..#.............}..L.........T...]...E1...\...l.....O\..H1.............8.;

C:\Users\user\Desktop\BWDRWEEARI\ERWQDBYZVW.png	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.842852420550572
Encrypted:	false
SSDEEP:	24:aTSIFgzFdB0qwhU6Z/VTr9+L52NAEB+VtICi+Y4tj5SVyYXRX0NDZuutrYmRBdx:ESAgp7/YjZ50L52NFNb4t4ykgfVRBX
MD5:	19225B1D700747081FB46C230E8DF8AB
SHA1:	6B2C727B757380402E50C377BE273C36BBE275D1
SHA-256:	7A3BB21741511614F47A36DAF69A8C0379E3B7407A5676E45F9E96C5A38ABE83
SHA-512:	8A5547DDC944DE28C601BCEA1AFC3FB19965666D58763DDC02A783A639684B432B7AA9D3879BAF1C28D8209120285B437F69954B34F53680AB7B802B886DE66B
Malicious:	false
Preview:	9..{gE..P.._..b.;.Kv...<.TmLd...T....{....b..%S?.VW..)...`E.m.!m`..F...[...y.U..i.c.....d.4.d....!.M..q.x2.......0a..l=._y.-....0.h.W...5.$\|....Mi..q.Q....W....L..2^.Rp;....?.M.?;...V.1suQUE..}..V.#.[_.F.;5..d x.}.......a..4.M...R ..sH=}.76..>..d.Q.._.\...2.oK...dA~..k8.r..c.Y..@S_9....d.H.3.<..3[@~!$n5dcz/)b..P. l.............4....Rk.Sc..;...>2u]..i'7Bv...A..}....-.o......i.f......g.:...`...n~......Z.....>...,....y.n<%,...c.....|g..).d@.....7...tcFl..,Rt......e .*1 .z.D..G.;\p........8N..:)..VN'.9o.Y....zt.Ey...._.b.|...GE..!.Q..Z.h.&R..s.(..}..C...FL...(.]........"x~....8f..|..Y|..g......]......5..o..^..u~Q..A.%...4.}..@...%R.gD.4.9$V..a.#....~~...,........(<..2.....6'...Q!.&.S=g...h........ ...S.L~..Wj...Xa.Q.c...^.hnis.S#.P..T.ruX.2.d...)RrK^...^.....jwHz....di.....8..2.g.#.?.e....j=..B[...p...W.....zw...8..S..l!...x.........`...+.2....km...{....*j.wm.;.>...,...f......G(&..M..4..=....oj...`J..(..W.-..1.<.2.d.../../.[KJ5.[.... W..T.L.c#[m...-K...

C:\Users\user\Desktop\BWDRWEEARI\FAAGWHBVUU.xlsx	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.843156224322512
Encrypted:	false
SSDEEP:	24:5m4c9dTc+shD4VvZErMYZE2sIQzyLcxK2uxJuflNHpuutrF5J:5m42T4h6ZEr3E7GLQJQEflhFf
MD5:	371B3006141CB75ACD550EE2D3BA6079
SHA1:	66E3428872B6D9BCC06BBA4CD4CA65CDFFCA86DA
SHA-256:	A2658936B5453DFB439894E9CA7E71C7B391ADA9F2B774A6F92137BA5ECDEFD4
SHA-512:	BED25A93E0A7A961FC707653F21A9455AF5DB386140363201A3EF01489C4470F92EFF484A232637A4FA1BBFD504F8770552E453A2860D78EEE09C20ED090E298
Malicious:	false
Preview:	l...v...ySQ.....y..nj....,9......a.6x6...y..:..........3..o..J+D.+...c.H..X...../...}.......K1n..1.[..F.Ps.m...y..>.98z&.`nq.5..j..u...%^...y..T..\....|.'.$.x..m.u..J*.....5.K.=....7...T...:V.Dv....i.0.Q"T.l...m....y...p@c..:..9...t+..Z...E .....^...Z.P0.8..n.RsV.6.t...$)0.{}e..H...p.x..?\.....v..$v.].N'....t..@...Q3..Z..Y.7o.]...z.T@..(?\|....eB...P.RG_`...........h...K....`".(.H..:...)o.B..7". ....../..$.c.E.S....6.gw....g..M.K..Y..3..`...Zo%.N\.`.H..z.1h.<....*Y... D..#.&...M...+c`_..>.f..t..#..d......]0..l.S\......Q.....>.P\._.+..4U./.i...>.'..L.6-.A.O...QR]W..R\..`..2.j..S..%.7..g..lm..u4GV..E.p/~P.n.-.'mA.s..h.h.^##..:a...."L_........l"w #.....R2.Dc.. ...9..H....*..l.... ..k{....e..K1.ej: .....]T@>.C.V4%./6...:@5...z.h....jG.F.{{....Le..u.&N..m.t^...(K...\..o.......g@..y....y....|6._N-.3Wc..+.....y.|.t..S}...."........}..k+X_)..@,.....S.....@...=av.....H.[..rZ...F...!.jm}H..t...'..&..o*.P..1u.s../......<b6.....e...i. f.m2... ...we..V..(..O

C:\Users\user\Desktop\BWDRWEEARI\FGAWOVZUJP.mp3	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped

Encrypted:	false
SSDEEP:	24:hXGLQUzv7YVBVi4E4UuYv+qiz948wGsk3tN/CRsKnBv0Rv7Z6/Duutr8:hkJsTVi//Vpizi8wvk3OmKU7Z0N8
MD5:	3C402EC9AD223D4D361D47E5DC6CCEDB
SHA1:	7C38B6E3F2767AFC378E7AE606A0E8AE95512A2A
SHA-256:	56817D180760F3BDF81E0057A3EEE1FE9109024EF7CBB310584AE0C01D2A5AC8
SHA-512:	F18BF9E96C52E35CB8DC92152EA70D9CDD199B5205C1E7F5D5FC169952DEEB85D2E8773FAEA2BBF7970C1B50A3A56FD0DCA7B56EF7BB29667CF6D99C74CF711F
Malicious:	false
Preview:	^...H....I....KW..(.....m...]x..}f.\,..}=.X....2..r.C3G.a>.M........T&....q...GE.t....@^.d.$qe...AT...........$..ra..........y.v...m..g....YC.2S..NR..5l.h...7.w#.C}0..P.+.Te..................b$..3.._.N).Y.['F...,(S!P...Csg3{..^ID.-J..'...?. H......G.......6.l/;....ddN.>.S....P.,..!s.....4..tvq....^h~...{.S..E..E.y.H.!\|.?......._.....f.Vo.V&.=....0..6.:T9l.2.w.......r.m..[.s.wf.'d.....L..6.....P.[.....J...!XFDu9..lQZ.=RD..d.....c...-*.\l.K...W..U..m.....9.xk.PGB;...e....A.....l= .5."...p..e..=.. ..B...e:q"dRT_.._.<...2....-..P .../~.^c.)..Bm..&.4r........*Y..'.&.z........`.....0.B...~...01.j.n.ic]........VQHE...."...u...."2.wu....Hl .A....[.F ...........1"..!Hz...a..9K.>.0>h........6.Qc..r........-..C.O.....3.b.J.<. .N.x..'..lb.....o..%A....u...W..........@.L......L.HUP,........$...6.@..&............)..F..?.....?O.{.=...<../\..p...r...&|.v..{>n...W<H(P......_...`;.2O...r...T.}g/.+..."......_=N2....R...lk....x.....FS..7jT...h.+.KM.&.)2.c

C:\Users\user\Desktop\BWDRWEEARI\OVWVVIANZH.pdf

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.856277979705629
Encrypted:	false
SSDEEP:	24:tBz5z/w+Uxw/SbViYhKYoBYVim83eXIN3bd8W8euutrSI7:tzOESb4RzBSimceb3ayl7
MD5:	FDD8081BC6697D0AA10ECA4B46275C01
SHA1:	D57856F6D2991B20DE1D18784F82C06097348765
SHA-256:	BBC22FEFB2996CEAA7C27D31914BCF4DD258AA9CF1A2E9526E371B34823537E5
SHA-512:	91E6406A54E8AB52169A684BF8ED5AC18A38E79DE3103FAE7DE259A62020CFA53F9650E46093A5252A08114CEE4E8CFFB28518A159D5DA1F8D6AF1BA2B811D02
Malicious:	false
Preview:	u.e.<"..|1....."..z.....|+..m.c.LA..e&C-J..S...).2V..F.R...?....'...\..8.3..4....}f.v.rDF..7}.r.2.g_"..(...O..G./%F.yCm.j.nr_0.,..x{...(..#.N#."..h..F4.n..?...(.3.2"....{b..JW...OP"r.\~.x..?..!.X..np0.3..Cc.........CzU....*....yi[..R+.oX....tz,1=.......{.....E..|M^y.O#~. z.py...8.^&.8......."l.H.u....1..qX*.iu?...........q...{......#.....+o@...$.....36.V.S.[4.Y.....V&..S.n.......^K.r6..~...B.pg\:Lh......^h.G.............Xv.sI.U..R.....-.V/..BrH..;._/.... n....P..L.. ....H.sN[..m .N.Q....K..ix....O}6U...5.0.Zid...cq......'.g...m|x.\...y...+p......+..KU...\..*N.....I...@..Q..Le..%..i.....L.].].1.~....D.6.=..g...:.N!!.&J...o..!._..hE..q..A....Z....{..#.?h....v.qO.d>.'\....< ...l....v.}.........;..G..Z. ..}.....C...... ..Y.i..]kj..._...c9%....U..W. "...2.........u.du_.L.........`.].z..fg.5,.....@...7|Z..#....M......&w_X.e..ha.3....2..m..W...<4"..A.a.x...Sp&.c...1=b......Q.j....^.}{...k..N.jr.....-... u.8....]....8e-.. PN<g

C:\Users\user\Desktop\BWDRWEEARI\WDBWCPEFJW.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.85147010479057
Encrypted:	false
SSDEEP:	24:RXsUjZJDX3odwUU4nfkYy/9kIbgYVdAZpdma8rj3fcWjGpzVvuutrgyCfan:RFVJDldNf9DlbTdKbmPjE8GpZJgyXn
MD5:	C82BAF91277D9AD996752865DDFE5892
SHA1:	E9B6FAC61EB44367E91529BFE2470F8F38AB13B0
SHA-256:	FAC4FB227E62DCF83D4098E1DD35DCB5348B44346C550309871884C84F6625D1
SHA-512:	E51BDBE198EA530E30F412A0E668EF5F8F274D561E2EBA1CC1B1BCF48D99BC38D37200CDE743ABD4864274865271F34DDE4D8F4A56B6BAD93C031F954CABD62A
Malicious:	false
Preview:	.7.E.....F...4.7.... .Z....K.T..3...vI.K!P......xq.....[.../Qh(.z.Z..I(..Ur.2,,..Z....4........6.mx..w..m.....rU..Z.W.+.w..{x...}..i..9..[a..;5.@./o.ux....qKu..TN_.....a....ml2..S<..k.~>...x*w@..n.tY....\.A.n+a..|.l.:....OdJ..A.>. `x=...!9..T....Ml...^..5....u...Tt..lEd.e.;b...x,.Q..... ._..y-J.o.m.H.^.p..-+...%M+......<`V....4.A. .(F......k\...|.a...g..].7..4.......l..]P...9.rN.....0..`ph..p.."N..-...4@..f.a....JwW.....?...........^.{.....]..,..n...nS....F.N...W.J.O ..M.....r.q...H....{.....E.SO...d.H6...7.e..MZ........Tl.Nn...$.......C.7.~....n8.2D$.kp..$S.D]a.y...V..S.l..p..f.R`.t;n...M...L........b...1....Y+Hp...l]..o..1m.....Y5.pT.......Q......J..REb..67...UuS....m...}..V.W..6.6 .(...<... .SQ.L..d.....p.Vu.8L...N......_....D....[..m1.3...S)!....iq....5.......$.B.g.....q\.!...jd5...]b].....|/H.`+.B$y#.t..^...y$_H.^,....~.....F...j...u8[K..B.........mO....*@...h..:.c.(......0.iR....5..l....5LP..V..O.0.._v.P@.%X...Q.;>...

C:\Users\user\Desktop\BWDRWEEARI\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Desktop\BWETZDQDIB.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.850292754554404
Encrypted:	false
SSDEEP:	24:gjMtxdLXdYau1ulWMGT0g66NHlCfNoYwULf+IOMuutrk:gMtLzu1HQgJHlPYwULfok
MD5:	A7EDBBFDFC1D971AE41CBFF9B7A6B2AE
SHA1:	D9FC433D611603358501725CACF7835B7D2106FD
SHA-256:	654A559F31FDB6FC4523769335AFB250D5F189E2BF91542B82CEB6A02EAFECFA
SHA-512:	0E56A492C84C3122ECA147CFEB13FA25DD2D7464008B4DF61CE8EAE25E3D5EDE0A7205665D93D419429E8664A1FB176401CF7CF8FC8DDB2CE4B46C33839829D7
Malicious:	false
Preview:	....8!..5....s.C6.7'S..`..N.4.O.n.u.H..[{.p....D..L...L.H*d.....G...{Q....<....F.....'GuR.6....L9Q.......V.$%.?..9.#..Ej.v....U.X.;b.......a`."(R[..Fr....K4.e-.......9H...*.....a......E..$...:..B..uV.t...<.&..z7.E....\........].:......t&.~.. .....$d...x)f...k..J....lz.DYU...[.....s.@>7.q..G+(...\..n=Q?.(4.T....m......6..:K.A.....w.)4..!..=.V.T.]V}N/.W.}e16..<...pO....^...}Q.t.....:Eb..S...t.%K."..n...=..F...<...%...2.....Dd..&...>....o.....2.q.*.o.Q.f.\|..D.......)V.2.W.c... <......\7..a..6..../%@.6......&...#......2.2'd....2......a..\|..zj.6.KT.0..,z.:5..a...{.a......P$..G%y...;+..^......|...g...H...1.\u..[..:...i..{.fuPtO....)....=\..7..@$<...K;/.K..uq...:..#..Y.....}gQ.a..Q]...r.M.Q....3.3y0...M.0..3.L..Ll.4z).o[%......!2.P...mv... &...-|. ....D..;..X..*.uS.9...d+..7......dW...._..f.3.....3..4.R)9..m"I%..).A.1iY....V>..y....l.w...c.s.2l&....~p^}....:...l...g..z....X.0Vj..Vt.........[.t..R\U......K..9k~.=&gr>...O......gH.4...

C:\Users\user\Desktop\BWETZDQDIB.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe

Size (bytes):	1258
Entropy (8bit):	7.852295773127187
Encrypted:	false
SSDEEP:	24:4zDoMh5bkO994mpW7qPRUpNOv1Eys0gJLFbYFVv/GWbeGhKn1fHeeHuutrkFp:4zDombr94YIqJivyqsVv/GWbThavXBMp
MD5:	3E0C11076A7BC785317A82C941F3BB17
SHA1:	743BD36A019BE75A53E5E429E4379353478A0FAF
SHA-256:	42C44FABF5F42349AFB2844C122869162A54B69F3D9268CBA14EBDE90BEA1320
SHA-512:	0D36E87E454FAFF8A8E1594006400E0E4C4BD083DFBDA779C3632CD852A51DCD77468450C8146319224B19D1680895C32E77A34A649F3C40D9A775176592B676
Malicious:	false
Preview:	j...l.km.uOx..6K.b2Z......J..'.~..?...7...#....O.T!a.Y!S7....E..mO. .il...d......."s.W...4.2.B..If......\N<h.&...,...,..BK.u..i..HB.....q...........Q..!.Q...&91..=....}q..]...\.=.V.]3..=....P..b1.Y.).........r.....uT.........\e.z...lC4v..L ......Q..b@.j $.fAT.0...d#..O.o..{.C.v..[....G.....T.\..Z."...Q..~...~<%...qE..(....,.5.....F..a}.{.a....78L mK...a..D#..xn.D..iV.8.6...Fk.E.,.....*..Si..J=....Y.^.t.!i0h.....J".U.7".z..X[......8z..s#.kBql..r.!..7i0...MO...3D...N*..Z....?\ .6.2...._.>....i..z........SAs\|.b.......l.>.........\1u...:8.W.4.n. .AH....P.ef.B..DH.^...O.O3.h...Fi...Ff(zO..........X......z..TFMtD@5...^/.\|a..Yh.u..8..oY\|...C...@.AT.....^.P.....&...`0[....fk.&R...r.5.!A...6v...o..UX.A..o...c. .Dl..}.A.w.F$l.*.\@z..e.>3.....m..{....HZ5Y...J.av/fH.;....@....5....Ss..t/..1Ti.7..._..N...Y..k.x&1..F3......c!.X5....C#7;.<Q2...#...S4T..Qa.j.:0.S..`8...`..<0Y..f!3.8.V.z.+@.3j..3.f[.2..;..1;_...8.q#.QE.......A...#/=.W...P`CL... .*9......

C:\Users\user\Desktop\BWETZDQDIB\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Desktop\DWTHNHNNJB.png Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.854879488673598
Encrypted:	false
SSDEEP:	24:FGYN7nlpBipLl7CTcoifQ4hVO5BBU/eeRXqFfL/lJeu+wZWLXuutrt:tlpUBCTjf4hM5BwfkjsrPWdt
MD5:	8AF5E1669EC3A98997E359B4CFED98E4
SHA1:	60370F8F442BA01051C6E31DC29962BF4E05648A
SHA-256:	32072E68A38E4D13C64408C54376034D19F4766FF6C05650ECA9CE15D36FCBB1
SHA-512:	F25FD72789E3FB052CA7111F3EB51B62D35C36303C3655EED950D79FB12589F20B45E3ADA4CD06115EC334446BD798A3976EC8D70B51E97600149640DA0338A4
Malicious:	false
Preview:	.{,.P{[@....~q.)..2.-.*.......m....s....o1.vJo..'^.y..f.$..v.PB`...q.y&-.$k.TF...h.R}=........2.r...D..>..PH.4....._k...aV..Q.q.........=....g..\.U....{g.N...$:\|}..\.y.;.=K0....i.h.+%[8f....P.>p.$.......q....a..K...\.?.6..b.vT..}....D0J.g.. .....Wh.*....M.1.."/?h..g........j.87%J...."G.qM....M..b........}`..e.NY..(..D.;.....'oM..H.....Xd.z.ok.z.c.....-..@e.E.s69....X.6.^..(vY....o[L..)...>..,(.......K..h.>..9~vK.A......%..Z.@.\Y.qy....D.|.-r.E..F.n-....|.V...Y...2.,..P...|.u) .Wx[..N...........'...}V.R]...T.....|...Ova....?.Z#....SM.S..=."^...D....X..b0+..i...)n.<].U.x..9..W...l.`...7..@BC...`.Q...i#.,t.k`.'.2sA..$Z......t...j..........m....h......2.kH.c....t..K...C.?..B........0.......\|..7.\|......5o2i...}...Q.H......[.... ....Uk.#..d..DG?J.g.5.g-.....y....{..N$...w......9.r(.I....E.."2.....<..'..+.......F...5....]G.bE.0.Y.._...z......1g.|.....T.....>...KeO....Pyt..*O%.n...Y...h7.....?oZ...^...*((.N...zX.@.w2.Z.E...;_x1l...kT....5>

C:\Users\user\Desktop\ERWQDBYZVW.png Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.833893179882195
Encrypted:	false
SSDEEP:	24:GkTBEShlltxGJDqal9sgtC72Vrf+f3n/UCXqmXz+spd2+potq8vhFhuh/HuutrTz:GkTCSqlDUDjl99E2pU7qmXztD2+Ow8vs
MD5:	45F70562AC0EB04747FF1A593FA15DD6
SHA1:	B87E5D4499E6D234C315BACFDD101C8FB810E51E
SHA-256:	AFD4568A2511BD2186EBD9787F58D6F6904589C15E7D7A9F12305620A6CA09FE
SHA-512:	4B6FED25AF653B4206793E7DA4AF443C7722523860CD011AF911ABDF6FE961DE071428C47505E9C6B07DE07C849D9B0AF4329A9B1FC64F5FB24996524D9CFCE6
Malicious:	**true**
Preview:	#...J...Q\...jGk#..Is..M..:j..s..].>B.......X..!.l.l......E.t......b.I..n.{..xk3Z3...B$.U.......5.V.R.i.0...$"..n...Y.7yr...~.w..S.U.D..P.gl..:9Q.5`....C%.^S..|.H.mc*3...,....(.p.5....Rl.f........c.._..M`]<...e7..y..@.<+....R\/......Y`.|.. 95{.`.G7%....3{V.<.g.P....t..S.biV..+D|....{..M&.>eLe$..Om..a.\.IN..B.7H....C[.D..>.,..c..Ud....u@..[tuP...6hq.#N............"....2.-7..3.f..}...]..G6...*.>n..r'.,dj$.ib.j...0...>lc.....Nv.....).}ob...*."..._....;?..8pHj...q...... B2iv).L%G.w4.......0Vi.#..._H..6..T...#..x..(...tv......_....B.....|...m..1...*.$oKl.._..BDg..:..R7........_.G'.7a...j.._x.;.....v..,u..<........~.{......yV..X~.B...1Y.\|x.@../..l;...k.:..BA....L.xl..v.2.gG.....$...j.cN{..S...U..qr.1.^...j.a ..Qg....G....2.K..Au2Dx..Q.,...h.?P4.q...}....DO..H...,.#mSWqy..KQ~.t*....x..D.;.3.._@...R.....|+..]...$.D&hq..v....G.S.1..7gv._.n.+.ad.{*(..m..iUP5.H.}.....;.x.+Q...l.!..xP....@..[.k.q..8..&....=.2....-H.=.qz.../<.......b.W.. {..[..

C:\Users\user\Desktop\EVCMENBQHP\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.86256517715577
Encrypted:	false
SSDEEP:	24:g/+ceXxARZ/wFlec7zJvoQn2XKBzldnYSIDl9uutr6LS:O+ceXxAwF/1q+ldnHlD3
MD5:	BAF067BC5F06B22800AB3EA6F453BA12
SHA1:	7B4C37882CF7E4E3721394F88BE38D9900588C19
SHA-256:	6A776993160B4B57D9374D1B671EC6EE41C32370AD0CAF6276F6F749363E987B
SHA-512:	2F6511BC5D55D777E30268DEE004A3A12C24F21E377FDCB838CB314F53BEBC76331FBDA50D243366F09377F92EFA2BAD8E48ABC4107219E2728691B7649AFD5C
Malicious:	false
Preview:	..q..'U^.X.Rl....h..[..tM...|.e81j.6mq..dL.u7a......ya....Q..#.../.F.J+.P..7\...+*(.M..<.5.....j.k..[...`.|.L.H.H.$.........2.~`.F.Y ;U9.....^i.y.N.s.B\..o...G)c..3.....m!+....&.e\|..n...A..I...2b.'E..?..(..st..{g.Mv../Y"..f..........cy..F.. .h...jS...5..(...3....t8^...^...^...>....d.....~..V..M.}._..N.&\|....)..."7^^u4.k..u....~........+..u.......A....>....E2.+.>.rkc.8Ze.y.....xA.a.,-$...S!....k.+..&u..q.0..`..":OW.y...pHD.....^....T...L.~.....=i.v......C....3..e+[\...~.zn.@.. ....;8.~.)._f.S.{.:X.qT.....d.#..'........]....?....Lc..%....%D<.q...J......N%#0.......#A.h.7.9X.b.f....i....E7..j...W..t.2...=:^.~..r..:.t.....e.N..2.i.P.....g......=...{+..A|.Y.&\....*h....c#a....=.A.I*....X9.6.%..w../f..y/..5..y...E...fhlr.... ....'v....(..bM...1@e....O.j....8L...z...x.$..Ad........M.3..:Z.V>.Ll..?....a.Ul....A.v8..."w.!+b.e^..g.2n9...[.J.k.S..].J7...............G...X25_.R.K./.................qN.O.r.A....PW.>B........*..E.w/ZH......F.

C:\Users\user\Desktop\FAAGWHBVUU.pdf

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	SysEx File - Eventide
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8279073482959625
Encrypted:	false
SSDEEP:	24:6a09bFG04A8dZeeLw7AzrQwyYqG2wstcNClGVLjcD0x9pBAyLiuutrNYsf:A5FGJdEM+aKiogzpBBLINpf
MD5:	3384FDDC7F8F5A38587B185F8D135B04
SHA1:	BFF8ED1768B4B370B4D298E0C418427D934409DA
SHA-256:	63DADAA6CD101F0C03AB04B615F13F31713B51DBAB9D811DB5CFD273FF297718
SHA-512:	93A0E52A97348AD0AABC457104A26CD1A202E7CD719A3BF52A9AAA1FA00143E36D6095D1808CFE7F1334259DEA804BF31F299230311CB6CE3714866ACDB749C6
Malicious:	false
Preview:	......&...I.a..+.(.:r8..I.=`P.......*...(r....a...?...../.kp..>H.:nQx...M..]<. . ..~.<.....>....H...#e.{.-..<yu.cz.].Kt........1....PJ3...OV.+.Z...dR.{....S.4......J.H......*..p..Mx.D...9%P.{.....up...{.J.rv...G.y........Q........7....]H|.6 @....u1...HL.m.f.....}k.YP.].T.r...q.r.{..&.pF.Ze.)..?.F.>.R.>h.e...]>..p...T.U.s_.........;.&.,......w&/...(a..*....^a...J@3.s.H.._..t....5..T&Vo...L....@.e..2...B..I...z..V.8.o.5..R.H1......).+......D.,...@.$...7.......!|%.j.StA 4.3w.>R..t~..0Hjx.&./.o.H.D..?|=.=*E..r.......Y.~s.W."..P.k.~.F.2(...:.Oi...@........Rl....z.Wv.0..*eqw..J....+xf...Q...{.Cy..&."....9..Z.'c3.......|.Yv.....d.o.C=..=..L..p7C.....Y....g....Sm..x...?..Z=....x.hR.T!V ._1?.Qh:..,..{. .k..Y...........MRu......bB.r.f.[.{7.........[....3F/...i.z...q..........=.:.....R|r.(.a-.U...*3 .<.!....t..k..x...%...y...U.&.}lfX.j...D....u.....M.rg.}..N.....P.QsPzC....@!.....B....v....|..3.k.Z......]'.m.V.. .._B...7.O....e.8/SJ.q/....ni

C:\Users\user\Desktop\FAAGWHBVUU.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.839497848034277
Encrypted:	false
SSDEEP:	24:YaifdkxxsQawa+wGBWPsuEs4tyO3Uj5nKCHBNZ0lvtuutr4AL1/v.YDFWnawlU9EVbkgkBNfb4O
MD5:	A3E569E30A8DC2ECD028EC2323C61CFD
SHA1:	9533E00479D476344AB99A7211EBDB3A08083571
SHA-256:	258C9F74B66DE7050754CB43875ABB02FC96C2D20DBD4F4D024A01CCC74924B1
SHA-512:	95653EE2B1768F7FED0DCA1608E56579BA1CD32F7B6966F2CF58F49F7C9F82535E6AF73E4B0F02115BA30E7078BF33853C2463722487ED5D4CBAC3126D382A56
Malicious:	false
Preview:	.".-3...N_..%....!}.,.....3!AA..0].]?7..tY...F.(....!".....s....W..2.R(#..z]......g...I.'..|V...n.e..RZ..........w.....E.w...y...&.._..;..Z.Mw......`)...#.f.*]M...d.......=.F......^..1.V.L.2a....>B8.[..oQ...?D.......D{.Z.f....8\V."........i k..q5%.@1J..I..8E..!|&e..!.5O..4);....OMyc.k`..).........V.[$.j........ D.XK3..2".........ox,}O.P.....x.I%.6.....B..6.Xg.....k...A...A6.0..f...#1..D'.T...AG.]...5dj.u.D.a%{..\|...S....v.&...A.7..`.8..v._Z.Y.$_.:Gj}.6.........m..iy. .J...q.a..*{.).._.nM1&..../.k...I..x`.a... ..NE....H.eg...f>..I.SE..%.._..Z.!u.f.....^y..Es.80.\......P............H..z..:B..B.Vt....e|2.{D.;.......U.Qm.$9L.......Sw......K.....?.5...KHp...E...B....:b.Q..Q.....9.).O....2.A.Y..Y..FVI...J .prM..s.4..N..W.`wb&0`.M...A...A..F.H.tzE3v9..>...A...q.D!K..h.F...,.B=I..^.+..[.A&6..Y..Rx.Cg.XI.2.).c@P..W..I^.a..@........#...N4.Y.d+.t.K..).E......Jc.K.......r.....@.w.d.4y..\-...H....t-......0p...2QI..>P5..T...b< ..S.BIV..I.

C:\Users\user\Desktop\FGAWOVZUJP.mp3

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.825185332810085
Encrypted:	false
SSDEEP:	24:PLLsSZZLlLkOwGbemL5StJVAKZp/9alUo6uj7HAKuutrHi9:jdZhTXGqmLQBAKD/+UWgwC9
MD5:	C245057CCF796F7751CE399BC40FE75D
SHA1:	1B5C022FEA40AC9EC816335DA3B1D5786A0EC3A0
SHA-256:	6A00EFE8308EB393B168064EB0E5F4A9997361B0EE885BF2C8FD47B816552A40
SHA-512:	591E63D5E5B2491B43D7D586FDD0EC8BB65E02015B7476178B0A2647342BE029E703684503A88B97AD51958EBF4D7E8A2E9BE886B989FE6CE85CFC75096A6F78
Malicious:	false
Preview:	.....zm..G..06]...>.... ."+.*.2...)..,s.k.@....0.tex...|.~.......#W.....F6b...N.J...Wx5.u.Jf....S2.Z..a..B%2....H..'j.+..~.kMf..sK.r>+...{f...M.9....d.e.%...-..(\..=.1l....vn|7....s....U.6.N..?...6b..T...I...E...$.....>.t+VD&)?!T)v .yW=_..T.9c....W....Q...v>..3.qO........tz.Eh.;/....C{....6..........!..h.A,}......G...>...a}a.C.....!.j...(.n....p;|.d.l|..g.....*W.s..CiD..._X..6.-.T..=.....g....F...zXD..k..?.I+..P?....T*.[D.........;..e...fN....M.o.....s.][.B.....{...U ...Qm.?.X.x...mt.=r.~.'.......v.....Y...=.;....U1...F.dU...%.pDm..U..3E..-F]\.e.X.M.u..T.......W...5o.1r.)b.bb........".xd."...&...5..YX"..<f!`.eU..$3.y...?..\|..6....al.-..T....I..q..]..........v........q...A.{...E.0..6..&U3...ua./i...?.... ...x.......&.*m$..p/.. .....@..._...7G.f.....9...E.5((..&~9..we4.,.....k..*.Z....g....g.mS....).....b......Du t...-.N:.G.....K..6.EG#qS..I...%..G..*.....r..>..&z.o.._..Z.p.:n...n.... u.\.i-..q.[...8.M...I.!.Q....fE.Y..wDu.....8Q...H ..B2...Em{.$S....

C:\Users\user\Desktop\GJBHWQDROJ.png

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.828057862674834
Encrypted:	false
SSDEEP:	24:oPAm93eXsZcGwscmUiLLguFvtTOXtuVuPxgV3ttJydYBDqKVrJLauutrb:ocXstlNtLLguJtqA4gN7gaoKBgb
MD5:	14E85260E9D83FD1DFB790118CFBCFEE
SHA1:	2E82660AD00FF1167775DA9ACA0A58771698DA8F
SHA-256:	1FE293E1B6789578D7208B0318795D97B075FA2519F37B4C725A1228018D4544
SHA-512:	007627354B64CC8EC2D12BF6B33D83E1798B703E6480B6B8CB9EF3419805910052BD9075E8CCB59C2ED5328F690E6F415CFB20E2A8C99DA0B0A1C48C51A39964
Malicious:	false
Preview:	..'...1D..x..k.9%..$5\|.k.cu.-.%.~.....I.{'.._.....G.a....'...N.DhT..,A$...o..q..'.jo.v.....'...r...>.....5....|.v...o......M8.T4..V;m..E. .P...`....R.^......i.....{....e.._......h.....1(..{=...&..H.e.|1..B.dh.7.W..y+.....7H.2R.......2iM..U%*.. Mcl...#...m$l.`........r..EU.?.p...$..~.S..K.G|.9C.x.}.ne...;.6..f....E?.......'.^u..7..Q.....R|^ ....b...vR].aE...A..Y0.......V.....xXF5J..{...t+.\.8V...H..".C.^"...I........%..9.7...2%..'.......0..I..:....M....@.:i9..f8....2.. ...&n..."..n'.

C:\Users\user\Desktop\GNLQNHOLWB.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.849972617192274
Encrypted:	false
SSDEEP:	24:euSDvCgmmiJUki8iopLQyjxPq8k65gqPsYR1jWUkAEvuutrkmVU:eTLCgmni3opLQy1q8k6bEYR1qDA8e
MD5:	0807DCA4A49506183B4FD3B0D8E40661
SHA1:	7441A19D4F0CD9FC67D089EF9CA58D3466BD5B11
SHA-256:	F1AED13A5110F89EFB5B65DF241A02AFFB82009B9E9F9167975BDC980BA547D2
SHA-512:	A0A4C925F6D1035B70791F8469A3465C8314FB13D186C4D940A0D2A23DA3E70B347A7B9977EE1EA50BE9F03BEE0434662473D6FC4045065C09FBFAB09398E3A3
Malicious:	false
Preview:	...Z..%..JDR.....6.Z...6.u...,i..Z...8..6.*......@.`..x..5r.7..Yq.S.......\....`.Vb6'.a.....R.....3....5.!....*.`L.........J|e.......bB.NY..C......u...A...F...B)......VC....x.h... 8m.W...... .y...P].>.9"`.y.....ru'.rq..1z_D....r...`._#)..._ '..J..4z:S..v&..q..?!..^l}..x?f.....kIm=.X`a..j....D.B..%........g+:...D......4.-&L_...H..YLZ...yV.b....)h.p..@Wv8.....#...)..c...{..,..H.[..k......j.d.......z'P...v..b.....R9...}...FF:.)7.'....bA|..fs..n~.O.[.....K...X8.=<..hp..)......<v9". [.c,%.+Z(..].....O/......Z..~.....&.....1.X..e%..?q.@ ".:.+..@...\...Z.....(..Z.u..'.g..5...".(.fe..]G.p88B.....w*.......`c.[5{.{....x?x....>....fN..q.....[~&B.e.....@.X..|=Ai.>....ZR...^.i......ol.~. .e0v].YY..N..;?....ni.H..8[....v.EC.... ....6W.+..:n^..=.H.$s,....n'6...8..oMn])WKqf....b..tH.......W.oy.x.Uiw..%J. ..|..F...2....?..I.{.M.......p..b].tE.MQ.c......23.O...!.....}...<.]....V..4-HC.....Z..+...C.rN............O..@..........?0D...X....V.m..rJ\nh.M.6.~...

C:\Users\user\Desktop\GNLQNHOLWB.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.849593120732565
Encrypted:	false
SSDEEP:	24:HMvfWAdRzhSR0cq+Te94EDLMGhDGlatiLRwKuutrZX:gt5a0X4EP/EtFx
MD5:	021B96AA5D4AC975AC33AD5A89318AE6
SHA1:	82ADEB34C7465EE6D4336673D66FF538D1B39FD0
SHA-256:	C4CC16A5535EEEDE7FE3F7155CB1B3B669486368F95DFABBCDF7CC10529E97CC
SHA-512:	28565E88F9D6A7153528020471914BD7799EC9143B8B9432ED0F4CEA63136A75F36B2A1372976FBD6E10D5CB52666023DD77AEE55B7BB254373E920EEA4EF03E
Malicious:	false
Preview:	.=Y..fp>.....H&...>..Q....-.jD.4.f.w...i'....is...$.g.....n....#...65a.W..y.@?&..t.1\|..N`%.$.1U...ae|.A.+'...t..<.I..&}....i.=...^.3.,.0.?b..).VH.D..x..s.........kbQ9..7.g.........RN)..w.8Be.'....'/...;..L...;./.M".....n.......gqsfi........ 5..K.....d.i1.[.EpmH.C.y.y..^X.f.A...v.I?%..H..R...t.-O*...=....(.@Y..8[.....}?Z....4.~..b.......*.Q...B.".Q...N...(..9Y.c..|..+U..F..].!..3...+.......(...m<A.G.5[..csPi.......2.....u.MG7.[...@_KJ..3....].uX..J.=O.%.^A..W...#D|.:. T_%?5..Wo..F2L.(.../...}q.,;../.m.e..g$9..p/....O43....X..K..oZ....J.9...jmX..y.n...;..j...m....u...b+.C..I..v..+9.O....Y.JxI.b~.7....d......1{.0..7.o2..xlIMW%2..q.(P..P..W..Zz'..-.i...M...."...j...@.dR>>...W..nA.....H..v.Dj.F..... .....i...y...4-.3..9i..W..ed....7..../L.0.}.p...........p71..K.R._C@.>R..t.s..Pd.4T...CXQ..7.9......x...Y.......V....|v..t..... ...q.3j.d...g.D.r..]...u..<.<N.5...bV.A...0..8..R]...5,....s....W.....H.Ed..:&......,G....]....*J@.u.(...e.cu.. .s.Ha5.,.

C:\Users\user\Desktop\GNLQNHOLWB\BUFZSQPCOH.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.851232615103616
Encrypted:	false
SSDEEP:	24:HEgwj/Lgh1rCdQZ4R6HzEfKHAuwv/LGGpFZYHdnuGDRKiy/8dpuutrP:HmLe1rUFRC2hv/Lh7WRhvP
MD5:	E657918B1201E4F52BAAD5B7E02EA648
SHA1:	6E987427AE98FCF0813A6B335AF4A0D8BFD0E1BD
SHA-256:	87FCB51698248BA84C6D49C4D45904C7E468E4010F1CBF993FD775B0EE94AB05
SHA-512:	AE1D7346EBDCA46DE0C79165702EA5FE9B8CA1229F410A6A583F9B2A3A9340638312A5D0AF2A49CCC176F612BF810357F4BD034BC98C6EE1CD14DCCB66CB5129
Malicious:	false
Preview:	t>.Nl.^.[.......~s..i'.(.N...t..W.M.....:.0.`...9.|Al..T...Y..,.7.c.....;..5M...z..q8..:.....$x..:..P......'..|:...c{......xZ./.t.....XP...K.Q].[.~^..0.U.ATq....].Id.....m.A.E..x..!...._5..1...^....n...3....><...|.-.?jZ.=K)..G.g.Y~.....2.}.Ol...U..K. .z]..c....i4z.../Q..m..C.G..X.:..k..U.qJ..^+.1..tE.[A...x.......).&..X...D.....;.>.....)^./X.3;........N...c...:.2....+aK.....W@g.%8j.ai.|....[.*..."..)..g....A..7..S.....E....<M.]...vqP9[W.J.....@...|..8....x..z&:..)..3.w.f...~o.......|.. ..+1...K...R.s..P.8|.......pil..%..\.....A....=U.n.a....^9...........H..I|.3Y._....z...L.r..x.......L1......X..R..k.Q..a;4._..4ly....z..d..&xjL.....=...)j....C.7..NR.R<.|,Ym..D.W...&z..z,U.2h&..bM.H./=.)._.M.....eG.2......8@.Yb|..uzh. {b..o.A.Xt..!.~J.It.ax.9....#...w.-.,i......^..*pOz2.cz..:..f.\W.i.}.n*../2k*....T....+N"..........x-<.V.u..... ..{.....-Z.I.Q.u..8.(..n5./.I..O.WOGIN2@S.}.U..v+.....e]g..W>.(IO..1.&d..K...%jr.!^/f..8....?..=. ....#....%...

C:\Users\user\Desktop\GNLQNHOLWB\BWETZDQDIB.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.853857791122457
Encrypted:	false
SSDEEP:	24:ki+2pOzfRAlBxMSDsNAlkeYmdinoldgp+zbv34G9uutrJJ:hOexDyGknzqdgp+HvnDX
MD5:	9C934FA4B02B044A10411B244D8019D3
SHA1:	4F5F3FE031EE001B614A9C79244863744F8D3E7A
SHA-256:	437AB7CB90F014ED41A5E81E371BF7E9B8CB49741681A306AEFEC655E9C3797F
SHA-512:	8CE94B3848876779887B9B5FA234F98B339DC52BD3FA94BF40D70B21FD634786A2EBFA41BC3BD0E41F6560A75CA1DD7C71B08CE999BDFEEA66782274862436D1
Malicious:	false
Preview:	..';Q.'I.F..Ux....Y....e.S.I.....kFc.xX.......|j.}.S...T....yY:.I...a...%.7\.O...'..n..+..F......5K.A..|C....z. h...$..^Y......9S..t."...=,.(.E<CkP...Q.....<....j.U[)...ta)....H...]...tJ.{....Whp.K..n........c.b...T8.?.i5......".^.Yagu.'6.o .....Z..y.z..Y>....6....Y..{..KI..}..1f}..rW...6....P.....o...5.<L...k)y...?B.....5.qK.P..L.......G..s.f.8.......K..B.k.~Z...B.\:..d.O.......*..D.."m....S...Tg...M..N...`%..p.....C3.#...7.#...?Bbk..w.L.=<...Z....u..^.t..O...u...5,s._.h.?.. 4.!....../.p...D....@....."2g...n..k..79..!.' ...4yv.j.{.#q.yL.ku..a.5.Tg..U.p.3.."1.t.C.p]......2..^6ul@R...'\.v{,../..1_..j...;w.9L..y...,.hl*.@..5.YW'..-...8y-.ml.%.H+Xq.L....p.\...9..c.M......V... %M......T..(A......gt..wQ..m. .s..5.O.....0{...m_n.U...}..K.~3...LU.:..........rt..I......0@.u!..bB..gnU.t+j.3...E!.i\.... 01.o...:I...'^...I...`.S\|B..G..Mu...Ak$.."*..Fwb>hB4h...IIT.t%;430.8b.$W....,!..=DE7..HK....~....O..:_~@%..]..2C..W.:EM...X..........

C:\Users\user\Desktop\GNLQNHOLWB\FAAGWHBVUU.pdf

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.838521669455329
Encrypted:	false
SSDEEP:	24:zaQ8nUkQba100w7OMporALX+hgs9lIH07bxXtiuutr22W:N8ndz00w7OJAShgs92H4FXtI2z
MD5:	9D6B67E63DEFF0D1B416E3EE179018E6
SHA1:	9540EA7666E7C87CF22A3A6A9A7550780AFBFD54
SHA-256:	58546844F6198FADA11E040B4A2144466303C2EAED454E6C6E503565F8D267D7
SHA-512:	8F5488E614B775DEE0FBB4CC2025ADC1746B02BEF6BE25E689D747F8CC818878839AA65897A7FC6560DF0BFFF300A06E7C6A0201613BC5C2908178759C5E5DCA
Malicious:	false

```
.V.Z..D..}G..u...q.fg..s3.....F.........B.M)@.....p%......N..PU.GA..E.E'(.0......s....g....d..;.@.e..x..%.....L..g6.Ng.....4u.$.".ep[YH,}<}.*`nA....z...V...#..G....^.a...98......W.(.mq..?Z...l 2.....c.Yk...m.&..!.......SG...5.k.5.
.EFd.7.s.g..5.[.O#...F..'.cx......../....E5W.Ym.x..q6..;<8.u.(.....?..\........Y....u_.q.L7...Ih..=...P....KR.B.....a.....m..(Mm..5.U....d.....`.._.y.G..i.,.v:4.!.n...w...~\F..."o.p.D(......o;{3...$.gP. .@...z...Z..zOQ..>TD...vA.
.PD...~....T.6
```

C:\Users\user\Desktop\GNLQNHOLWB\GJBHWQDROJ.png

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.862387841248518
Encrypted:	false
SSDEEP:	24:METOpJHBXhTZPi8oPed5NhQB7Cgfln/iqh2zEaouutrKF:MQOpJhX5x2PCjQBh/BheEFKF
MD5:	4707B555A620BBD2DE6FBF37E2F53BC6
SHA1:	3FC87F2A787E78EF903D84384010FD9866B5FFAA
SHA-256:	5A86C17D60EC50DEB470E03D3ADAFB2FE1614A11D09EDBA63944BA757B4310D7
SHA-512:	44B249ED1001138B2FB5F8E9F57A1754E456653FF56EDB02BB6484DEE36ADFE33A3EA6D29724B402DEEDBC3ADABCD09716773A64616C1A4FFA6A0FD49E04B564
Malicious:	false

Preview:

```
.w....oB.tq....|.5.p7..c.a. ...sg>.z..L.7...$......v...E[..... .d.=."`.8_..q2....BPQZm,....u.^..l.9HL.Z|w.q...y}_- 4..?.&Y.f.../=l.....hbs....p8.wh.%<U.~....l....=\.{c..MTn.F7\..s.w@. n.. ...........<......mbt#~.f."X.)s.........".
.e.S.....zI.I.Lz...I.?....r..~Tk...u.u...l..... ..qo7.r._X.a....h...Dy+.>.Oc&..&#N8..o.rW.W.HR.Rr.P...6^.>?4.m....:6...({..)..D4.kIR..b!......V...'....*.s..gV..:....j.....8+..s;0p.... 9..y..I((5.f......).`.XN..\..n]....E.Zp./.,..l.qf..Y.&*.
....3.....,...d..q..._\...3....o]S.=.z.r...lP..G..t_2.5X..`.pr.S....q.P.....:....".s.i!.3b..0.1...-.$....m..b.w......8...)...B<..EK.d...+.....Yq4=.n.<..L....,.5..M.1~Q~i.`...]...b.5.vuL.....%.e..7.:Z4.z.9..W7G.J.&._.km..[:d... ... .?...g..
..$.{...`.%..".....B4...*.Y.g.F..n....>G.A...s.\..[.).6...Rz.j..b+'....S.......s^..e...S.B\...2+( ....U.E!8..,}..d0.3Z>.Nh\b.S.^%.o.|...m.`..i...p.....{hqv3...0Df....9....0^u.~.k.a..l[.{.A..P.q...n..pQU..K.......731...y......bQ);.N..)...G.c
```

C:\Users\user\Desktop\GNLQNHOLWB\GNLQNHOLWB.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.813060497950302
Encrypted:	false
SSDEEP:	24:gPY/pzDgw7LjpUYdyrJVY+ciCf19WLOlAsjHET8/M1JHXvDruutry:gPSD9LjpUfS/rblAsjHWXXvD1y
MD5:	2863E9178B3508916489AD033DF996F9
SHA1:	CD8023495FB531DBF722965409F2DE4A02EE7EC4
SHA-256:	A62696F9399AFB6C4B9878A160DD642F946475FF6FFEDB8C51617E3FAF5836C8
SHA-512:	6F4EB254CB92D4E944C18D7C6B24636145466BF0EF1F2D5E91D3CE413E6B555164830EDF1A835DCA578726C42CAB34CD6C6DEF04491548C823EAF10149D13027
Malicious:	false

Preview:

```
Ej..!B..'.3.f.{.&..Y:.5...c....)..u.._....,.1~...........>~.........g.E1aD.....b.......(.e...0...s..m..-l#...=...*..<....t<m.Q.3?..(...l..5.n.Q..#-gZ.kL.cv..QH$.$..X......}Ue..z.Gr......k..7kSqE........^L.er24..i.-.<-....k..*y.....k........d.
}..T{N1h..e.~J....hT../..x.y..1(9.......A....S..m...8v<T.....=..2dz.M.u.(m..#2.%.I..WGb..,.hYU.....}...d....<#...0..*..a.....|O.EE...|..!a.;..."G.y..0.....(Knm..Lx....".n....~.h.e.........i.V.......rl..f..h.....7/....+.U..}=.'.....kp...
$....Ttk6.w..6.T.%.X0..=+...$s.-...~7v.T<.eG.G....6JL.......Z...O.........o.E-}......-..D..i$i....U.a.h.i.B..<....$.7Qshhvi.V.Te...4G....g"`8[.k5.D....~2!..7r..N.W.V9......&&.A{\...S. ....L....u.T........Uv..y.Px.%......e...)z/@."
.X....f%.-.F.bi[?.x......q^f..2\T..v.(.^.kR..}.j.c....v..w6)..D.W..W=......../.........S>.|..%....I.y.le.@...^..>./$+.IP...Cp..".8.R..E.....%..)..y)7...3..{..*.......AZ.-.q.....z.D-t.....?..2.1.w.....f.[.Z..]P'.....'.....<<.O.G(}
```

C:\Users\user\Desktop\GNLQNHOLWB\WDBWCPEFJW.mp3

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8630107198888215
Encrypted:	false
SSDEEP:	24:vlh7K4JYJbdYVNpab3suW52jHX2SHgvPJl2Ug7/JL/EDgnYuutrsN:ELYJGVN0b9j32niam
MD5:	3D774DB939A6778E7D4618E851DEB804
SHA1:	8CE092F41E14BD71F2D41E989499E1CDCAF17798
SHA-256:	A25429E176B1B9D6CA71AD23752AF17BDC384489BAC06A768F9AEC106A86A670
SHA-512:	3E35632563050340121BC879820E7009654A2347B559E8D331C12342BC4C0CDB0D506B8A7BE7E39860AF205A7ACF1B5AB17255D53E99847301B0A38E654F512E
Malicious:	false

Preview:

```
o..w.'r....0...}.p^U.N>H....2...I..S...).....yo.<.I;.0W?.V...Z.@.O...8.^.s.yH{Oe...T!..>Ytc.Htm.).X....w.....:.p......).~...M.......v..".C..........W.E.G...#ol.#u\..3...C....A.>~...4....._.`&5..X,-....d..,S;Q....m..aA.u\.i...s..;.
.t...3z....fzg........a...YW.D&/.:....N\..IB..fF..N:H$\.j.#..7.,..7ZoQ.+...(~.....3.Bv3......8W.H.|..........A....`.e.....P.@.....vP..A......:wE...s.Hz...5b........t..0....I.C....2gH@4.0...:.....PN=xS..dG+[.-V.Ik....S.[.E.B.|...G.
..e.).th..R\N...zS......(.......]& .9....W.E,.i6.B.Y.p....$J..->.,N..d.......>Nk..x.z...8.KE..4..M2......r~...r....=.c^.../......e....r2....e.#A..$..]L....*.......M.e..$C..u.X\.....s.K|i~...'O...s.*q..i5..?....%..#j..~..j..bc.6..........g@..
W+ai..b..M."..w...q.._.?...2..T*O1h%..Z...I.7...|#x.!(..D..8s..$.N.R..qG......m.D.'0Z.....n..0.'.A..y....Y.z.T/w!./.....d$.......B.D.].o...)1Sc.{.c...;.Z....D.&..Mk...`.&.3.E...Pg<.IO.z.G?.....3z$..#_.n..J....!.B.].H..{&m=.V/..t...
..1...R....^).
```

C:\Users\user\Desktop\GNLQNHOLWB\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false

Preview:

```
-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .
i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o.
.f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e.
.a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.
```

C:\Users\user\Desktop\HYGZTMOBZN\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3

Malicious:	false

Preview:

```
-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .
i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o.
.f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e.
.a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.
```

C:\Users\user\Desktop\IZMFBFKMEB.docx Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.836014894567983
Encrypted:	false
SSDEEP:	24:O4kzt45FBI8YfX6uUvf/Zfbwl4J6Tb7wmYuutrvK7I9:O4FfuUnRfbk4J6Tb7wm6yU9
MD5:	5C5007798F9C3D0AF877095A74B486EF
SHA1:	01DD96CFE5137019D282DE2B15667C16ED471183
SHA-256:	69202D8E02BA91BAB8B135167E22818B54058E36CAE4AF1F37D10E125F70485D
SHA-512:	4D77DF7542A4333AC85A2FEA6E2464C0D3FF5F6B3717B5DC1771BC696ED84579B08951BFDFF385060C4ED32FE0BB052964F659AEDB06483F33EB7ADC3CD0BE3B
Malicious:	false

Preview:

```
.kd.......as..{.M;..b0...3.....:0f.6.jA1i.qY......\......&.t..@..0..)..$...K...0...>.....R...L..1:.$2.K...e....3T,..16.........G`1J..Cn.....|.....:5Up.<.I'.R%...>0.z....s...i...\.Q!....a.I.D.yv.n..~...9.s=.T.....>.....DX.</.....X...w...'I
4..r.A......G}..$....Y[..ze..$a.71....f......).D.c........C.21.8....N...E..XP.....YFjU..^...tX<f....f.....oU.xe.r.p.T.|7.!...7.@.9.-1.I#xo.g......W.xG.sU.T...t...8@.[......k.BJk8..D.]`7y.....S.(...M.g.....4........t.......|\Z..). <...."0@.
...;......c......(......A;...B...n9l........q.P..Y.L.=...h.....26V..!.U.A.R?.T..<....&..o-.....\..2...P}.S.*..I.  ..(.,.PJ.....V..|.jB{..y.^^p}..Jz...W..x.g[.6$...z.V....*..Vs.$..nxA.....e....=jZ.7=..x.zF....#......2.0.M../..D..8l..4.m.Q.z..
.j....z.'....%..t;.\..C.0.8.N9.....v.....S.5...U.Y.!......8....!...f..,.E.D.....EAN.(.t.xy....yy.$.J........'....O...n.w`.f.4....L.'..cE.-.&.4..M..Lg......b.X....z_j.6..^=...+3.+...cT`....}..*..Q.z.....s=.<.1.k.Fd...V[..-..
```

C:\Users\user\Desktop\IZMFBFKMEB\BUFZSQPCOH.jpg Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.844609816281185
Encrypted:	false
SSDEEP:	24:KJjEJ241QYOvciKzRR8a3molfPcxTYBA+Jl+ElElOs5uutrAN:KJjEh1QYWQRKa37WsaF+3Ebeg
MD5:	D468E70E5F55ED54EEDD599B08047768
SHA1:	398E9D7529F7653F0215A6C8C3C305D0C95AEEEB
SHA-256:	5FA89346F2983AC3CC9B96AC4F58470BD42EF6DD5B5B29E13AB2A75DBB8B7084
SHA-512:	41348E80C9F38FA28997C173EC2232B002BB746007D493D6B5934079D29E540E056E3686257E763AB2913861F2D0249B90F78163856FE5F26CC60D455285892E
Malicious:	false

Preview:

```
0...s.e0\....o.;..N....W0...W(.0i.....9........$`(........n../...v.*.^K...d.n......;x.(m...4......0...w.....D.~..y2..(...j}..:M..  ..u.&...2.S.0.Z..H..fB...,.0.L.z.....(....aJ.D..{..T./.....j...G.EzL.I. ]z.......&..........+89..@...Yt>..@..
.....H57.At=g...&6.....3.E.k..P4..P...q..N/.].....e...s?...aX..J..}..."..e....=.t.y....Q.h...? I.&.r...}a...E.fAAe.....:!...&....w].,J{......^.L.2..UA1...SJ.m.ff..55..6e...K..n..A....*.....C8.fk...\.,..2.T..3~.{........@>-..>.I......]E...n.D
........D5..*.7.h.q.Y..p'..'......7.Y..8...q...s&/..2..8ClR..s......9.=)]q.Z...Ll.=l.6....._...mj.`.-u....C....K..SPA.O#-.un?.;$.[GLQ.q.6D]..c..\1....Q.H.........^@.&\...8.....H..%$...L).;...kn...$6B...nO:)..i....d..3..o...$-.r!........-.[N
..R.......hX.b5..B(j.M%...{..MZ\.......R+..$.O.&.g..a...mJ.!7tv..I.JDz..i....gm..m.......w85...J..3...(Eh.....N....ur.D.R)..Vn.F....l4P......A......<...-j.8...A."....Zb.O.......:_....;Y...!E..~....S4....V..M..3......\.
```

C:\Users\user\Desktop\IZMFBFKMEB\BWDRWEEARI.pdf Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.838859058367471
Encrypted:	false
SSDEEP:	24:2Fh1c8taz4LyK8UzMXxAyU35wdBMg7qdofWymXybuutr32i:qw8taz4LMXTquOriGi
MD5:	F2D5257F867C3EFC6D94D96C6810DE47
SHA1:	19DE2BBEBCD2AA06A0DC318C9DA5604B891FB3FA
SHA-256:	017D4D1392B7C6C603D97EF541A6E2ADBDA412986378A356E09B17FC40F077BD
SHA-512:	5CE7FB8196DFB44DCB7B1D14F2C92240C4A1EF63E37DA1F017A41CBAEFFC275828D7A6D6D57E3B320EB1623FB7BEBB1659602D0BCE8A0CE5F0760EFF487BCBD9
Malicious:	false

Preview:

```
.HR....n8t.........i&$.D...i.r.>4.%.kZAx..U...[X;8.y..l.....d#B.{..%?...w..#.} ......g>.Vb../t....5..8..._g9..A..v..KJ.cce...]......&.:.H..5...........`...q..Z..z..a.TQBl..<.......I%....t.....Q.;i..n/....o-q.q.....L.'.C....'.k.K.5.D.,..A.
B.T]..K...r....R..84.jd...;8......$qd.P..h.VFW..R.%..S..+Sr...$.5.K....I.X....}.q...N+YZ..G q?......).&.L.....h.(..6=.M...o_..d.|...K#..jg....XH ..J.Z...8Lfd.LNZ.*b..c..U.Aa0...I.Z..GpD..g*...Eb ...\.g.....k...T...?@.u.....u`...f8
W\z.>......X..m..,..I'.=...O..;Qd.Q..++...w.X.u..........CG...'R.....W..^.W.u..!p..H.}9@....O7..W./.7.........@O3...V.A.1..jq...4..Z|%..\......C..].K..WM>........6.7A.....c...)...0.5.~B..F.s7...<.|....Xkb.......U.W......X..p..q..
...b.(Z.....q.S1....|..W..0}..Ci.GY.4X.QF.#...L..!i..W.{?.!.9.=+..5$.S......g'{./.....<O...].!s...!......Z...L...{.6.o1B$4F ...@n.4.;..v!.2l..F^...q....p...;..j...E..:.b.(@.qQ..QS.....V....O=.SF...gX....\.uNi.....(...f[y.iJ.,...G...w].....i..~#
```

C:\Users\user\Desktop\IZMFBFKMEB\FAAGWHBVUU.mp3 Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.845142998311012
Encrypted:	false
SSDEEP:	24:XdpO+FyVH5jBI1TxMAXS2OEVbh6P2rT43TCWnKus0xjGel2Juutr7X:XK+I5NVTxtrr6P2rKRnKYjGe0v7X
MD5:	61269757FA0D873D6CC67E9217176276
SHA1:	2C783412649BA2BC612FA9E0BD17090BC4091214
SHA-256:	81ED1BD17DD210CFAF2F146BDE02074071C7B6D2384D4F3B673A3100AD5C76EC
SHA-512:	F1628E877985A910F44B7A8B09A2B1BF003AF072C8B2252CC0915F27F388F117FB7227373032FE1CA8D489E1BE42DF8BBCEA0B8398B78D04A9AEE24EF6C67BD5
Malicious:	false

Preview:

```
...{=..f....JL..\. ............EI3..w._..J2l.-..,efC..Q_H..O+)Q..<p..G.I..n..7..b.)!...m]..\.<.h.&..%.s.P.....i...w..r.rg..I3..M".Z\..n8...{v....rz....eG.x..O."VB.M*.Z<....t..!EW.8.h.m..b....A...T.KpP....d...$.b1.>.9,Qw.0...Ll.....
[....h]j(.....`..m.7...#"....L..H.....Pd)+.K&=.|p..y.Q .....f[..........p........t..T.T.RR....gT."h&.Ix....M8.....y..*Y;V..W.....h.Q[..=..........0.u..@.I[..K....^..[7;..O....B.k.].n.W.S5.g....9.......h....s..........N........#p..|.wQ.1 ..
..RV.fk.....EEB5..l.j.2.~..t.CH....%j'W..N.Bq.g.6.oJ!..]M.y.O.:.^...T8...7....U..._..>.?...E.ZU..k.... ....K'..>.w4..%.2.D..]...u,.M...|.~.....;...[..\..""..S ..n1..7..(p.ZJ...[..+f|..y>.........:*....9....... ....K<.&.S\.al._w...o...^.47x.
{..V.Z.v..U........Q..L.K.n...u....p.I..T:.H...;.He`.G.e.G...H......L.BS.H...\~.........:.-.....[...I.m..hR.....=...f=7...Y...X;.@7.....L....&#/.\aravEz...CE}wk..|`.....I..N....9..O..H...lg.\....G[].m.4..).F=..S..v.......S...n......4TS..
```

C:\Users\user\Desktop\IZMFBFKMEB\GNLQNHOLWB.xlsx Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.819386921804163
Encrypted:	false
SSDEEP:	24:PQBGwrZn/QTlFrB0tHmb79ibiuDFVqvz6tSVuB7/LiQgDPuutrG/mnZn:0VYs5Ys7ANq7oNDiQgdG/QZn

SHA-256:	227D0F69735D37FB5A432B8D35FB0C198AA0CD33BC267E862DBD15687D1519ED
SHA-512:	1F058CF228B9CE75E0CAEE5A9125C022243DA7FF53B7E56DBF1410B6ADBA6BE538AE3D32950007602545D24EBB6C455218707BB253202DAF9DA7E1C79BA3157C
Malicious:	**true**
Preview:	r;.{w......`..c.6.E...I....~^........$R..-.......L....3.....R@.Z..T..7=...YWm......ku......C....v...;.....e^..3(.cE...(..Y........2..)#.o.N.t....-.!q...VP.........}{L......J..:..\.\.z.my..W.I?* .p.@.`.^.k=g.....\..R. ..;.._.-.....Y..9.o.xY.Q&. (%V.....<.!..W.....]..&.Q.ge.].C..t/H.._...;..<..wT..E.X..E..R$.e...r.Xs..L. D..,~.v...~.....tq.~.x^J.6.Y.s=f..G>.......'....p~.......kU..2......X0..X.C0X9...d.s.....!..fj.{+.'Z/...E..H.....W:'....:..&..z+@.t.z...7u..>`.y.0..../.P.I.GF .. {H............w.....g..~.Am......".D..t.a....=..M.Xh.Qt.:Y.F.*$..&Y....J.*.2....f....t....B.QE..N&..."S.....&......=..U..y;.<.h..or.pJxA?......y.. .j..<..Q........t..o..2Q....;~..#.Z....0..8.'..........r.@.O.]\|...$./.r.T..k!.#.....)..s.|.2....2.. ...f#@.s.n.WV...."pp..yM.`.S....."..../!V.....<...z.%..%....1.$...#.......bv.cH.u./...t.........[.9&..a...,...C..".u...='q.{h..I..;..Oo2..n7z3.u.c.Y..w.].=;...p+. ..y. .yi....P..\]@.?\xm.L.a..-a.E.......p.g.[.<

C:\Users\user\Desktop\IZMFBFKMEB\IZMFBFKMEB.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.835791913758512
Encrypted:	false
SSDEEP:	24:IQk7tkTl3PJKgVm+KPqv1/pIDlFtAg8HFszzPmMuutrOQY:IQkZkTl3+NqvflRfXeFS6uOQY
MD5:	36EC31A6130D71A7B5289F58E9F1CB27
SHA1:	0BA4C0B05A43C173A18917A7F252D7FB4E6F4252
SHA-256:	D1520B650624E27B6B555B04B9718C4A247A533F0410A4DEE53E68218449F37A
SHA-512:	66D4229F50B88FA860344EAD197F8AAAA020168DCB93E0550884784BBD09D513DF3098AC0E9D2CF7D3417257A6D22AB377232FEB8527872E312CDB95D673E8EA
Malicious:	**true**
Preview:	.fzJi..IW.7.s....a..,....{.&.......,1rSL.wJH..........xr-.....$..7..w!.m..O......Jeu..[.}...y..>........m{.b.......3.%QY.1.........Z.j._.#...w._..?..@r..d....ws\L._\|............!....i..`""'........\.GK=2....k...[$....T.....)...'.%.1.I....;.*...?...... ;.HE...Q:...)sD.........dGB.KcfF8..f.Yf..7..+..`..h.zhW...8...3.HY..1.._.A.L...$.Z...d\|>.....4.dn..E.2..8.+...?N..]..[(.'p..$....2.e."..w..2.)..-IM.......2..'.... ..T..s.U'.}.v>.'p.I..h.s.J.V.....\....;..>.^...FS<.......B.+..NUcq....qa.>..' .M.....gS..._.?...,..Y8..'...B....... i..WG..X(..;..zw.....B.+T..O-.GQ7].......*0.@c.......,.J.z.3E.Sb..;.a&\bY$9k....9.....TJ.d...!d...|h.U..f.;.j.Gd..+'..o"p...k..`...B..N.....B.+x..nc.s."...[..q0.W...So."..9\...0u.Q..oT...~!.... D.KO.:d........*.[.........U...3d..X_j.Q..K..".g.^>.v....H..J.!R..V\'...P.h>.x...j..X.. n....2....].N....C....]e..G*..J..U..S.T...d.[.q.VF..S.5..O./...9#^m.fj....z2V-L..,1.^..&t........O..fk.,..K....W<Z|rj.............a..L..[.=.m..

C:\Users\user\Desktop\IZMFBFKMEB\UBVUNTSCZJ.png

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8476212145753665
Encrypted:	false
SSDEEP:	24:EgNlqM+oXTvL01G2lsYlquIOCCRahFGlNs78hDi06UBrbCVf8IL5HwyuutrU/qYA:VIMRU1GM3lquINCRahFGlo8EfUB/C64b
MD5:	42A06C67EDF48C5B1711587594607F49
SHA1:	FBFB81114F93A0912B622248004B09E85E5817DF
SHA-256:	53948F3A851C502012572CEC74BC5274920653D067DC101A0EC6D59A99C699CE
SHA-512:	28D1A8BD6FA2E4974C123769C750575228487E51C4CFCBFB5A7CABEA9993D96CC8996055CF2E8DCF168E3B91E6EFB42BA6EA65EA98171E6C76D2D52074E25195
Malicious:	false
Preview:	..........I...".6m...(r.I1e..I.%..1...L.I.8........z..*<L.G.Q...klj..Y.K...g.w..~@..q.......A.. iYd_.#..p.~...n..ED.P.%....U.....,o"..w..}..O..>h......z..P....0.A...>).p._q0Z.ia.r.7...Y.m...!.WB<.Q.+:^\...1......e.Xo5*Tv..IK.o~... ....Z.8..&.#.I...~..;.\...U.#E&.....e.<..V.9.%.K@n.DU%....!......$....{...F%..".Gf........K$.-......XM.B..$..D.J..z.VB.o......~....o.x....)8.jM...)Khg=...I.z2n'Y.D...d...qqJ......@.D.M.%qC.......Jc......FbP...O...nB=*\|..........t .T9q......[.....2...C^. ...bf.D.......<...Z^...9...... ...x...P8.q.f......N.@....r.....Gd...KU*.g..0....]....P.S8Ed9...)/.;..w..J.Z...N?*D..m..>.P}.......R.7.@ wZ.....[..g..!..rP...-..;..;..j.~.....;.KtF...Q....Ly..*.4nz=.+`.....Y.v.....s. 1QJ.uXXt-..n&`i.@.._a..9.%......k....E`...g.ZN..I...L........8..R.2B.....z.....;...y........qG.ec........B.&yp.d..H.T..4.U...J_......;$.\{.z]0.LR.."..H...<..I..n.".j...L.a.7....+|...D?zL.(....:>b....C....h.....}7.U..r......O....R.-,..X..=/.<V

C:\Users\user\Desktop\IZMFBFKMEB\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Desktop\KBIFTJWHNZ.mp3

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.833053406107276
Encrypted:	false
SSDEEP:	24:lOqGrSt8qayYI19NT6mc6TtfpJeRAy9Hp6uutrReZiW0:oTQ9NTxc6TtRJeRb6EZZ0
MD5:	D7D7AE1F7032BE0030F61CEEE5251D2D
SHA1:	C88B7A4AFC24C48193BE15283515E4AA3459F953
SHA-256:	C2F9479C8C4A92AB57AA72B2DB4FE5EE98E03A0A0C058E91B383128D709E7B1A
SHA-512:	F04E3CCA1F77F06ED9E73B286DC17FBB0FDB5A2354DFE7D8EE565C7D6366F477EE872D66D9EF76BFD638107B25457A89C8E5E26880412FEA7439257F1CBDE152
Malicious:	false
Preview:	...I......]..F.~x,......+F.'.x.L..w".IK......d....P...]..3....2.D.G...rz%..-...*....Y8$h..!?..B@.......W......7..)...:.C?......i....H.):L$....n/Z.}*Il.+..?O6..j.iZ...M._o....Id......K......?.j\d......y.nV....._....RE=...>.".#|...~.x.....;.. ....4W..k9..%v../.5.#..N..F].BS......9.......F....X...).....T.G.......6Lo.m.7...X.. y.....J.V....]....n....B.*`.S/|.....Nr.gM,+..B=Z.Qx..(.+..^V'....I...F.Z_..?Jf....X.....E.~.G?..G.~..7f.. ..........~&@bT.......-..N..Xye~...?f....Etz...2 .v..o.....U.o..j.le)..W.........2....2.ea.56..S.>.G$...9..h.LX.K_.z.`.......(.?.C....=.psI}L*v.....7..B'Ep...0.4R..V...Qz...~....I......#..{bjC.......S...K..K...]-f..>..@.~.E.b.D.....r....$.d.!....o...w.[.......N......S...mrhv...PNT...Qa.G0 .G...5..9..W....5..8.{H6b[..4.~.."........`7}..fs.z....{...c..}..T.w.=..R.....1..y.?....;.?u....cQ..u..oh1<.C..Wo..wT...ZUf.>.T..YFB......[.j[..tw.l.t$.z..aN...-........w.".j....h)....C..),%...7$JYJ.N.<xm..#....]..o.8q..&.E.

C:\Users\user\Desktop\KBIFTJWHNZ\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363

MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Desktop\OVWVIANZH.pdf	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8479010740826824
Encrypted:	false
SSDEEP:	24:TYFw3aPaMT4bdDN6VGBPF/xcAUHvtMtd4bljRjJm05df0NTcwTPMDxvuutr55O:TY2aXsbdDlAZUHvqLGb1H0NlTGxJ55O
MD5:	642605EBF770A2E90BCB9F44FF1DD75A
SHA1:	C3F71CF48EEDA0A994AC6B402B078FA000FAEBF5
SHA-256:	ABAA9961E0D4341652F82D982C65A9536F8E0C717E891F41BE366B8B2788E95F
SHA-512:	899C43BEF09D1C0539CE530F63EB9AEF6CFEC28D709156976444B6C6A38807FB3C76A2917D391140B5A18D0D40606249AEDFF01CFC4710B93F3B3236D8E94CE7
Malicious:	false
Preview:	5...L.l......X.. .....<.Q..a.s..w'.. .t.?...YF..M!....1...(.x...OA.NK.j..?.........D.:T.tt.q....3....#2r/.r*.....\.S(..-}.....}4..L'%B}.^)..{K...{6jJ.a_..ZP...V..y...|...F.L......Fr...u.)O..}.\?C.....Hp.....k..T....&...V.F.aa.....E.k#.$Uy.& #7(p..8....gB.C....r..l.r...v<.......agW........J.........d........-yqk..I5*../....W\.K....ub.K.T.d.ghk..;.........M.....w... ..B.@^....I].wM^.".e2.g...c..`?-.%M.q..^;...!.Vj..."@...{...B.6.(...w.....).......I.....P....%q.Af.nld...-..$X&>.. ....Rr..e.[.....Y2.v.@.f.......].5L.~\.............!.8.m/....'Z..E......(...f....5.a]|......oy.>.l.#.#.Fn.-.f}d.#..Q1..itgX..}..........z.}.....,r ....>>3.4*....D"~..9..I8.!Y.M}...Wg..x.}.w.w_=.V.s.."-I .p$...U....I_.6._....5Nd......V....Ho...:Ut... ..Q..le.....%.._.9,2H...o[.4n.......0s...8.8...O...x...O.\..h.=.S.{....r~.\|4.H..n.`..p.5. ..3l...........B)3m@.0,......h.Q8.'9^>.....8. ..~..U.a....My.k9.R.V},{.s...F.."..:u,..[.$.g*...)>.HZ..........7.0...\U.-.@

C:\Users\user\Desktop\UBVUNTSCZJ.png	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.863609341529593
Encrypted:	false
SSDEEP:	24:hdGzVkOxJltR9gEMILYkCVvAtLDvaw90Kuutrey:qzVkKtb6CYkCV45LaMd
MD5:	5CA8188DA26309B359E176E5DBD5D82B
SHA1:	1DCB4F29A89FD5BC25EA1F612A42069CC1426026
SHA-256:	D4491002DF774E9C2D95B14B8CC1186F7144B7D0E8CDA51E50837F0384658B1D
SHA-512:	00D7966C1D87BE4E04C57EF9C1829078BDD3BF7CF2C437BBFB2F0E67CFA8A64DCD6755F3AA2CDCDDB1F17CE1A8740B4CB50A6B1DF84A104A08D6500F2C6B4994
Malicious:	false
Preview:	I).....K...w.j..rY..K.......^Y..5Ka..kR!..a.n3%.'.q....9K....uj:Xz...b.St.%.;.)...^..5..L.k..S.. .o!.q...J.]S.dJ....d..g?..d.*A7.!v......~b.W.......6....qt.q.(Q..+.I1..O.S..y..\.z>.O.k...Y.cb.'p3.....`[.i.n..[s.....3.t#..........B.....c..,. .."...........H.F..@j....p-L.v..s....W........5..t.tl.")p.V.n.Mb....0.....z\,....=.._..F,yo...i6......tG....(..z....<..S..Vj...$Kc..<....h..l.MrMt..`.............z..@.r)./....nC3..*!..h=.v.$ZM.y+....&....^..w.....QzJ..6.'..._..=T..#....e..P.BX. <.VF-..<k........ex.d..r..VS...........l.....8m9...r.v.H....W.|`N".T.g>..r.f....h........M...w.q.F..{h.4#'....k...f_...&.d....+....1.{..v.P/M-]...4.....I...>...|...Kl}..........|.|u.6o.y..c...6....;..`..Lu+..,...8...6x...t..Yx.8...b.M..Z..._...r.Z:~.. .B....j5=.......]d.gT%.......F..).\..9.C1.....o.,Di..QLsa..z.|KN...n6[X-$._..m......D..Q...a..B......4..S*=..#Z.-.e.q....2....A..C.u....*...03..W.@+\.7~81.....l.i.....?..,*...b.hj.V.r.E...=1..2?.._....v.!.e.wp..\.

C:\Users\user\Desktop\WDBWCPEFJW.jpg	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.865626602356193
Encrypted:	false
SSDEEP:	24:9snZd1zSb4/pJ4hD1waG4Ff5MCO++8GsTlfc6gFZuutrCw:yZbSbCO1j5FfaCO++8Gjg5F
MD5:	865BD5BE774C3F9167D81DD070DF7A78
SHA1:	9AE3E054D6BE6E78DD230B61D0958BCEADFA75F0
SHA-256:	0208C453B667C27993EE15E4A342CCB160612CAD38A50B77573FC146A0E07A74
SHA-512:	BD0D47D90D16530A54E00CC91BD99A69007EC47CF6E44BF1A7307C085BCB29827A8CBD514E97FC37C1DAE972496BC58D84F587667485697A5A017BE8C90D6F51
Malicious:	false
Preview:	....f..7C.e....i}.c9..%.....|Cn.q93.!$............xS.\|W.p#.2^}..-#.!H...X.....!.7).N.w....c..........O.q...h.......C&.Z+5i..qZ.n..Xf..V........p.9......$L>...d....C..o....;.GW.to...m5+..$...Er.....V...O..5..4_e.L....4..R...'<.qj.>5L..Hi.). ...H.W*.......@.,.-..6d.......<..!@@P....'.m^..Y.M~..f._q.$........v.j.8..Qx..%}.j;/...L*..B1_....:).b./QR}.PC.,...FsT..#..P....@....j.?...]i6.-L.q..=.[...:y...{.&.r..e. .Yl-...K.1 }@...DG..gN.L.7\.|`vY_.n..o.[*.Cp~.#..H..6.v...". 4X.U....-.n...{.....[...){...3!.f..D.W..K*+?El....w._K.#V!G......$W."N..g...sU.....b#.n.-.. ....)..z.%^.wa.Y.k...z]x...j.......i....Z.9.?....Zc.W....#m5..u.IFC....J....c..{]..s..?P..rv....z,%)X.*.M..XB.Y1.".,.xS..]M.8..0..R).4.O.. Hs....4.!,...F...bB.....P...r).c.j..*.....N.t..[.R.3...[a.**.>..#..@5. i..V.H.I}S....m.O(........'.X.!.RL......l U.X.c,...!Jp=Q..D]..<n.)."...."....B../P.....q.Y.\D...o..BY.wx....z.U.e....$....*..N....S.R(.I..=...b....Aj.w..u@..Q9.'k...... ....r..9rP}.n

C:\Users\user\Desktop\WDBWCPEFJW.mp3	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8212195685564785
Encrypted:	false
SSDEEP:	24:ZstxAmLgTEPSdKolP35lrYTb5d3/cCkAcZZuutrRCWD:KmCv5mK5d3/zkLdRLD
MD5:	18B92A24BA90699303D1BC6B7F89C485
SHA1:	2EA1BB2DDC90C2353D259620A29D0E14D5A61FC3
SHA-256:	1A752C4C1A6976D3A99F3CCF5629B6AFAAE5DE8CD95DBFEF60AFFB3299A993FE
SHA-512:	9301E8DCE377736AE418D55913CED9D0835C2A402C2C9477F522318A770EF0B07DEFDB3606CC5C75E057BBCDC7D19A6D389A0F82CFA80B9231355C85A5D9F5D6
Malicious:	false
Preview:	.4`..34..eQC......I..s~....sf.Fz..A.e!.pP.;.h..k.....o......2.~.2....V....S=3~@/.@.{.Ow..T..mr..X....0i...x=..1..s.`...Q9.p....D.0.`R....y....n..[.)Om.-...,..\.2...>wi..A...\......"B..o' c.d...>.w......nd..Cl8my.....?.^n(..".,c.......R..... ../.....N9$".B..Ll'...&.a....S..!...$U...u..m..cY.6.........hj...z..C.>$...r)..{.e.A0f....!.%H.c.P..n.f.h.JL.$.....;e...%..."$9...T......q$....1...}C.2....*..Y....u.....?.yd..0.Bn(.....d.&...xo..H.d>.ery....y.K....k.j.i.z.s..;.#Vv.C..h"...; ....>..{....X{...j..EL.......I...}.....#;........r...e.'.......Z.J....L.jY%..A.:h..)..g.S...V.S...Q.Uf./....].M..z.......PE.5.......&~..xR.....KV<.{K.z}fz.@6.K.......Q;3.3~.%068..;.TV...)`4=.E..../.).a..#.GRu...{A......h..aK]........9...z.r. Km..a...%=.E........e..8~.....W.a...k..`.1.....w..5".[_D`....*L...g.M.}..Up.]..#3o..fh.{..W.. ..+..YF.,.W..?>~",.L%.WFp*."F.0:.J...T....&.V.x.`..4...<..\.......16..>.E2.X.........7Y.b0.K.8..............[....r.S.6....v....

C:\Users\user\Desktop\WDBWCPEFJW.pdf	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped

Encrypted:	false
SSDEEP:	24:QGLFlbvQRjmomXX7ulSu10st7xWhpTPIbXHmhUJJGjiFZuutrrD5:TFljE4alSumw7UhpjQHmh+ei5B
MD5:	4AD8457498E7BF01995617F6B3BDF654
SHA1:	40EAEEA55781D358E8FA1792A0F2FF7F45038FC1
SHA-256:	354B0571FFA30B9FA20FAA67C05FD379C581BF6003ABD8032DF86958CD6F3F5F
SHA-512:	2537F7066DF89938D0D758286BC3BD9F4EC7B9C43F4C15305CA2136DC9FEC9A56F97D8ACECD1A665728A2D5A44B2CFF57A936D0FEA29C91F16EF9ABCB4B20345
Malicious:	false
Preview:	.<ZEdh.P@.....$..p8 ..O........'....8.........y..7=..f..d.Xp...X..e..(X.uO.e.....'.r.Yl.....`.....j..J`....k.M7.....3.$.6"0.7..1.U5......F.f..9..B*iy...{/.....U..."...z.].D....+7.........D...32n.T~r(....J........].{...H0yS.:.....ks*FK..K.......e............9mO<.V..k..V.!........P._../.=....UN.......5....&`.@.G...#.P...#..t.U.t..)X.....2.`...e.....\.....29WY..YF.U.7.6.M..XQ....X....g.j...dv.l.%.u...W.=-c......jh....@.~.../.....#.........9R.Z.\..[......4.^..+Wu$.Xl..)..."..L.hj`...Yy^ d..'.j..n...C..w.g...,J.A.B...D9.b._a.9.z.y.,.^"....6.u..+.......+.n"69.#.....=..)0".AmWn..[z...[......2-...Y...%.SIS,;<G..\|l..L..t;.."...!.u.pC..?k....(z..$...,b....}.;V.{......x{..p.$..J}..zmT..i.~..S.Y...b...c...P...g...)4...djl.4..#'j.. .....:....#. .-i..WNo..d".. qJ..b......G.s..%..)B..'[... .L../.....$...k..*ei....b..n.......{>.7r1.,BnZ.7.4..%..o!.z..A.R..0U~LU..b.u..2)...Gd...........T!....z...f[..<c,.......1>..n...!..@a..&%.6..E.....hb..^..6..i...

C:\Users\user\Desktop\WHZAGPPPLA\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Desktop\ZUYYDJDFVF\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Desktop\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Documents\ATJBEMHSSB.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.857927478487206
Encrypted:	false
SSDEEP:	24:WXJcWhxXhC0TZADgnS3E3O2B81PT1LpcyRee1HpQdwBuutrBnKo:WXJhnRWgRWPTTdjNGWhKo
MD5:	BC51C1ABF455BAB0EC5D16988CB18187
SHA1:	ABDA93FD95E41D3BA09CE1F40FA035936E85345F
SHA-256:	EAC6622B9B80B70569137E04B334EEDB8939BCA5BE7079E3A2186F4B5D2C5EFE
SHA-512:	065F632BCC886F0EA353D4543E94A30B08820073FFC25D02FA4EC2D06625E53E23B58ABCD6CC1FEAC453762207004E29A06E00826D62E3011D462D12532372CC
Malicious:	false
Preview:	.>/B..).._..^.~NX.......O.....,n6=9_. .^.7&.L...=P0.F...J.........lsErKtC3O5,..-`...Ka7J.#.>B.)@....+.$.J..Z~k....e1\|.;..........V....'L.W.2..?...1.OMx..pW..J.{B...D0....wz6...4.....c........D..ed.JG!l....O....B.;_.#*k.....}.F#.T3 ....21C......Y..@"/.L.lSS.S.. ....u=.H..~#...7P.....a6_.E...f.K.$.a...i#8....k.S...U./f.t...R.....1.N..Wx..9.FtL...2a....d.o.-..]Bb....>.......b.K..G% NiS..5Q...l..d.g[..D.]z.h.N.O..ku.......X7.#k..S.%H..;{.....U.zH>..K.f.K..... "..y...+9.....j.A.x....Ey...k..l$>*...F....\|.o..5..f.;.PsJP.......Db..K.h..J3.V...q....(x;.f..61....u.#n(V......l...l......(..+."..u...........k..o7t@Pq.+.#9.rc..`....~K..S.o....l.. ,.....$..+.d.dH.<....j.. ......[y....UZ{.:........)..} #."....|.3._D G..d........,Y..g......s..1.+t-.......QAE...|2.9....E.-pN...h.....!" ....5.......-..-.e..w.]....KVLO...`kK#..O.An{..%..N....ry.H ......R.<c2&..<.L.n..^.....~..\.~.]!......c7f....J...M._!.....D.H..........^c..m...T0e:._..B....>...

C:\Users\user\Documents\ATJBEMHSSB\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe

Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Documents\AZTRJHKCVR\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Documents\BUFZSQPCOH.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.849125659232638
Encrypted:	false
SSDEEP:	24:1+5Xbl9spJnll8vffQBjq1mYD3VbJ9lxihKw+xMuutro:1+NLsuC3DFb9khKvxuo
MD5:	D8B5A662C792F96BE08D8C157E6F0393
SHA1:	063609480BD5F82DC33F602874332090C0BFF5E0
SHA-256:	104B833A7E464F0F158A391E3BCD080AF680A283A8AECA77E9A51EF8B7A39EE3
SHA-512:	6F8951C8356ED3081BCC33991D7C5CEEEA4AD6E7324E70E9FF40C26510DC7EFAE1482A35EA297251DEEE3C9C42332DBF910F0193DF29F5D8285415307CC3B6BB
Malicious:	false
Preview:	....u.TX....~....~._.tl...^.....}p....Bu.8.G.m.......O...g.3wZ......H.....).z....uc.#...kc.7......q.\<g7.......c..c1E......3.%.Tf.x.1...>...bs..6..Fe..o.@.d...X.>.^H...?...^O?&...v%.-......./.LO.U..B..qN........F..."..g/u...~<. G..0......f"2.........y.4.-....}...`....g.<:..../......Q.R....?._).3.8..C2Vt.r..C.?{hg....ft.L....dJ...wSe..B.%wh.F..&. T$.'..Z~...\|...}.k\|.....K...&.v..dL\|.-..9....#..F../_....{..$..... ..).x.....8.*.H..^}).~p...e..pH=R...)....i...uK.}K......5...".< ^.p.G\...........i...+......)p,.s.......;R."?i?....C=&y..N.>.zB..a..i..E.ES...x.>e...1}...91..j\t;..{.....<.e3.{8&.s.!Kf.R....Z..R.?....{G:9.."G...ZF.X.F."\:.......}.^.(.....9....`....j8..J......F.~L?..7.;X\S..NK..<...M...i._q.C...W......0 ....K.u.m..\\|y.5../*...).......I!.5..dQ..Z....F..k/..b>......;...Ylc.!.,*a.X.....9.Nj.. v.].*.gA{I.P..E.U..B.-Cb..-..VQ..U.........YO./....>..W..S.4.[O...?U..Z.0U.v.i.,.:..R...@........NA_..W.u...#.%.H=.....p.%Us.>hN.f.

C:\Users\user\Documents\BUFZSQPCOH.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	SVr3 curses screen image, big-endian
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.863952304507402
Encrypted:	false
SSDEEP:	24:Qx0/onZf/KKdPc3DpjFwHlTzypEOj7juN8rfHAuutrmfb:E0/opKKO31BwFT+5jukfHC6b
MD5:	2010AD4FC99B5D215DF3F6DE0CB97D8A
SHA1:	369A7302995B83B9D1629E0BA102EB13FBD30BAD
SHA-256:	430CC112C049B268E664C7DEE7FAB87F121EFAA9F651AE521E6D847878AB04AC
SHA-512:	DB78D3DE90D281D709335B2390E64032A1429A8056B42C6589DFDDEE027FC34F88E9BB90E1EB4E75B7E891DDDB548C5A1EAEC78D7FC3A477A364993825B8C484
Malicious:	false
Preview:	..'B..SP>.\......m...(x..>*......qq.<.aU....~..0......>.*z...M..PJT.V.(.....u.+.'..a(..xg..].h...M.b....X6ow.J*.J;.M.L....9".A...t].....jy.*.r...U#.]..u..6....eN..n....W.F.j...d+....h.%..)4..A$..X9..j..1..1}V.."..9P...Q..v..27..&&.f....iUe.)Z~_..8.9.@&.O..e8..eE.&..=Eh~:..#.uF.~dB..(...H..4gx....^n..D.(I..^.".)...Twj.....N...q.........t..9.....t...,.....;..;Mb..#e8..^..n....ZG.....5....A.1..7.6.@..W#.<.....$.5...8..S.....4..b..w..V<1.._...>.].~.6.{n..rG.Y....3IZ.C.. &...|....c.k..?......x.<..<{..H.|......./u.n&.cLL.....U`..rY..M"...?.k.._o...`BnQ...-..p...,O.%.3.....V+hD........o..KX.E.=I}.=...`....T....E..B..{O{.>m...X@.j.e.|.#.Tcq..n...\..(....X.R.C.ufQM...0o..p..+..g.......6..g...b[.n}...B ...='../...T..<J..D/....:.8.`...iQi.1_i{K......a.:T6=$.r.M.%....j..........0T.g..,)...y...`.,IO.....h..%.F...f.i....|9..PU.P`.p0m.....Z.g.KO1.m...ldw.@......;]C....E.....hy......Fa. .e....S...........z:.qE+...Z........m..3.7=:..|*...n.

C:\Users\user\Documents\BUFZSQPCOH.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.853717200788676
Encrypted:	false
SSDEEP:	24:cnOssIToQKkI2M/zLTK1Q3binrpysQ1cF5uutrBk:coMQpMmUspysR2
MD5:	8F7596D73F1BB85EFF16EA37D7EE6461
SHA1:	DAE3CE7E9EFC210901E325B09615A9C22C5380D8
SHA-256:	C3CCC15F643E03C03B7105A0DD8483959AB6F979C2EF5AF89046E1A58B4D12F1
SHA-512:	836D62172C651DC8D7DA33DB7627837A9B209544C586B8EB78E0B2F7DBB0063332A7ED848651ECCB4FD6BD71078D8059465D78A80905F5CBAC3DC624FABB05A3
Malicious:	false
Preview:	..I.c..M.ap..t...._8..eNa...{A.7..P...3..#..4.t.L."....)..eO.@;cSu...u..?.....cb.....50...RB........^..z.{]..^...b6.;.......K_.@q...M......e...u....0....=.G.....?.....W..gO...mh)...7........'..2."......Y.v,&..`.,g..........J0.q..$.q....B7v. ...L.0...X...1.../.\|...iLT&.....u......6........cA....&d.Hs.TOwh;:.fE..B.A!~.ICx..rjd.IG.."..DCln..2........0.Nz.3q...PzL..`.c~....-.B.s..a......D.0.... ....{ReG. .A.~j].H.i.....B...r...8Bv.yg...u..I..AA.&.....{.......Q.f..P.!5c.7=;d.....9. .....[ZYgC..=.Uy.h7.SG...I.*.0...<.....Z...7........<G.5h.....r....=`..e?9c...R....8l/.Z.:.<....Z..K..7k.x..QSG.j..i...\|H..#J.s....,..h....5b....x&y...D}..O...N&s.\..)L.ciJlr.cq*%...=.......k-jQG...Z.eBB.4i.'zl.!0.....r.x.n.?d.... ..H.....w.<.:.U_%.X...k..>.H..t............x3lV..bG.v.u].H..=@..$....J..ym:..Z^..].:...=....7...zM1.X...,\. x.....S6.../%o..z."1..`.9..6.W0(.X..#l....9b*. .}.....n...y.4..W....+f.(....v....|...?Z.k.!-/.e<H}%..)1.0.gU.....vA..y...}.

File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.85213680044442
Encrypted:	false
SSDEEP:	24:bkmH2wqFbzBIJ/s5NvJFFR+cN+eyRbA0UJ10rmuutrGt:bkmGFPE/s5Nr9JyC104Gt
MD5:	E3ADD11EB60DE7294ABD561147778705
SHA1:	452C7F8D477BBACEAA14C2ED4CF5C9DBEE93F0D2
SHA-256:	00EA365554A04AEC02D529EA0D5C32D1AB9EBC793B3A08F29CE883821FD23648
SHA-512:	0B13CCC27E33FC5E957B69EE341A19087B67CB3DE752C5043F7DD7AB180C08199F9360727A1923397854C559702F8DECE270BAEC55CA3B0C4368F1654700982C
Malicious:	false
Preview:	I....6.....g.Y..\Em..Ex..P.k&.dk.....2+.:....]..I...1VK.._..Yxn..B..1z.?.Y-.&......AR..dQ.....).')[......x...y}...../......,.{/..2..@.V...rV..a.z..y...rL.p..S...!h....Ts>.5....~0W...."Y.b.nd........e.......gW../n....o..$..J".k...u......I..j ..Q....Y..s....~E.y.....MA.\|..-vk...~p...k".....r.K...?...........w..\|..]..{.*LO.E..........?P........4#e....>M.....1...QY.M./@...c.".?..w4)0.).1....c..9.....#o........@...N......&..?7...w(.%zr.>.FQ.S...E'......C..+./...+p.A.p...AvT.Z4.^*.. ^..@...U...)g...*..\ *.!..Zr...9.C....$.;.>p.}M..4An[.b.,...I.c.N....6...*.....%X...2?X.3..!..^...C.{.+{..yX........4...r.Y.......S..Y.3.....^.o._...J#...O]..)j.O4C.G..FkZ..KFJ...`.GR.?...O.......o.%..E_.u4.Y8.....j.2...x.6.B.Z...@.iie..J.. .:j.....>p.K.}"](Im.C..q.\F.... ......sN.....s.AY..[IvQ...W.c.&...n.^Q5.....O>...q.O@g...~.W_...+.Z..g..(.v.[V.U..m..q7.....Y.v..;.$...|......2..=.g|..?3S..b.HF.{....O..E^....Y.a..C.p.....5.K....o.=..If..=.S...E..\.~.

C:\Users\user\Documents\BUFZSQPCOH\BWETZDQDIB.xlsx Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.856852113960079
Encrypted:	false
SSDEEP:	24:kGuOQtDRuXlb4inowuxwcnL/Jx3ouvfQLrRbHeVSuutrODsmL2Hh:kGq/u4btot9x4ugYYOD1Lc
MD5:	30B2E614724BE032ECAB2864F0A5F6EA
SHA1:	0C397F4AFFDACEB45443BC2561BF0DCCC5F0FDA9
SHA-256:	6EBEB01BA5B0784EA9B47F6B6935431D446981C47185477A6F4D8ACF899B9866
SHA-512:	81EE33341AE88860D80FE7890D277ADAF3F70AA586A8A4FAC2D6F5F606E1D6D644BB59D1A1140F44D0B42E69DAF3288AFB3A78152B91E3760D99BD81EC83E2C5
Malicious:	false
Preview:	...W;=..?.uoH...)".o..=.*......M...o.a.3.Z..I.....5. ..?C......C.T....][......8.y..+P.Jk.....)C3.V.f?.a.X)-.~.._\1p._4.o..BaX.....i\...=.k..4...#....$`.....O...p.x....@...!K\|.A_....=..Z.:....=5.-.;.'.[..c.q...D.....s..Iv...W...3.L......}......2.^. [..?Y..$Aa......0.....zr.,@.> Q.......M(j...6c.....R......G._...eo..C.....O..A..ox.c..[S+e.........._....7...V..zF.\..:y.0._.v..vt...>.Gss..,...|,1.XK.t.....b.y..w..a.*.B..V1!.~j.R'....}.T7-t3N._..(..[.f..J.WC..;.|7.G.5G...e......... .Q......U..c....U;?&s]..$..5....RA..!.z....[.....V.ZW`~)..V..../..M+[<.]..........o.(]m7zKL.5V...".F......[.fq.=.o;^....&..Q...C~.V....z..Uk.cq...W#..]..I.LI.,..4..i..Bmm_n.Zfj./...F...O..b...M,....<.*...xU..G.(..XM.du$.q..6wck..T. ...\pl.....P....[....m...._`U...*..~..&....)=#...{/..:\.U..~.....@.{......T...-}.'r]...O..X..k......q.N,s.L.|..2...-.....&[/L...Th.{.!.P..q.......`[....,.....C..... ....s.%.............:I.Z*......E.T9.j...*L......FD./.'.^2.Ly.

C:\Users\user\Documents\BUFZSQPCOH\EVCMENBQHP.png Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.840721403167979
Encrypted:	false
SSDEEP:	24:TA0t+dV998bP1SnDdVS2jUn6JMN1PZlWdB7SEOAjguutrnz:Tf8dVH8Zu/hgNdZQnz
MD5:	8824A94624AD3D2F6A7693AA86CA8FB1
SHA1:	BB8B577C30DED531078E71E6831D48DC152FCD45
SHA-256:	920534EA56E8A23F98FE4DDD2E4FF2F6FC85ED7CDB129DF1C42CB9622C61278A
SHA-512:	3A65DC9EA6AFFE284786B732423E996A26417176FFFB9872DB072B5D4C61311390B5E6F5967C1BC526F3875EF097B1300D273C7D05F4C239D59DDCA21427BC8C
Malicious:	false
Preview:	...,$.,z6....Tl*..$.H.g..n.z.O]ET-g..{....}-Y..Ga@...Z~....>...=J;..4k3.#....1.f.....[MOd.x..Pqeu.0..;I..qc.aA.o.pi.d.w.....c..:..No.XO...s9..3......K.f....Q.pD=.R.. t+.....U.K..I.....,C....,..>..44n.+^...i.....2j)*.=r.vO..U..,A/.=a.... {.`9....N..E.J..n...4...h^..KM...&N%....YEw.H...:...)9X.C.a.9.V...r..f.o>.R6.c.."{.m..E.....D....#|...R.NDd..'a..3...3O..e7....2.8_.K0R...^....&..0....e.RLy.....i..bf...k.Lg.....I).vlD..W...r.......5'...x.}..o.;oz....<iI.9wK...:.pD..& ..~.p.dYz..\c..M...F..=...V./.!......5......=S.U....,....*f..-../.......,[.....5]z...a.((U..W..Y_&<.......}.3...]2......F..gtw.K...!.:jw.~.Yo5k..rU)U_.x..U.2.-..5E.r.d..0u"4.8gA....c<..:c..ox~.(.gT..ot1...J..r.-hy....fU|k..p.+.a8........K. .&]T-.1... !D..g.j.-H/.=p5v.d.-7r..6Y.\..aD,M.PN..,.........YM.YA.......Y...).S...]....U....2.E%.oy)..{..%H.prZ.b<V.'{Q....S.1KX..E`..[...z[U.,UC.....F.iM.TU'.@5.."...0h9.c..@.r.-...[...u.D..=z......M..c9.....pG....G.2..[........,3

C:\Users\user\Documents\BUFZSQPCOH\MIVTQDBATG.pdf Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.84216232222916
Encrypted:	false
SSDEEP:	24:rHlmCc73Z2VcCBflMH6Dl2TfUv6cxsvu2HeMYuutrKD:rpJ7pidBflMHX2TEs6M6KD
MD5:	3B319455C552B222BB30912EE4230654
SHA1:	ABB5A4C5B4432A987E74DABE06780EB6FD2D8B5D
SHA-256:	CFCB54C666A984C4B02536F331C36504E58E0730AAFA2EF5897ED2BAEB997158
SHA-512:	6610A40C74BD11C956798B751C04DEE43590D20D072DB24E2A68898E9D80797E8917842F35CD27A1B80CB40FD1A9ED449BBC2C6E539987F21EA42575406F8915
Malicious:	false
Preview:	.D..q....C.>.q.......A..%+ F..B..........n.6.P.-..)v.^..2..4H[i.....m.... ...f.E.$..6.}..1;......{*...s~l.j.h..t.d ...*fV\|.Q.....Q..Y..;Q_. .X...T.V.1.d.Z^o.>.....<.s^Z.b&.AX$.AB.ek[.YT..w`..".._TEu..X.La.*5..!'..JNsEZX..5....M%.7. ...W).2G...U....)..k`<........E`.c...j..p.id.v......H..Ua.C.......Q.e.&...o.....p.s....>.wW..^i.3..\}.Y.....X..*...D8Zv.[Am..w.J(*..1....&...v.-.f_....u+...-.J.Z...k.{..Uzw..O..;/.I....>..e..].~.3.M...1..u...#..w..G.p. ..L.....\......._...f A..y......E.....f/...?*.M`...\..>O.Ss..M&.`....~k;.G..7@(....:..i.;D.U.iA..{.I.">..I.Z....MN..x....H.J#..#.....{I<0.v.b.$ky.,..t......{........n.C...1.(..iZ.H.4BF.7..[..{...2-..uL.4./......Y.}...].....+....0.Ty.%..4...Jn`..}?%..j..G.....~.. ....q..f..n.b.S=..-s.K..*.d......a4....u.zI...........P.W..h.TR.8....(...$......7..fpg...\..>/..F........;f.@..........f..s%.x....nTh.3|.....C..{.z.W,%u|.F.^^P.....p'..6%{CL$.B.IG.-p."...r b...f..._.yJu.q...S:..ph.....YE.

C:\Users\user\Documents\BUFZSQPCOH\MOCYNWGDZO.jpg Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8596202826606945
Encrypted:	false
SSDEEP:	24:43n75bbGT4/4Lz8Pagd1fzi4FgWV+alph/y8GbrMrQho2D8uutrH/:4X75ba8uACAebW84b/y8j6z6f
MD5:	5C01D4B4C431AC74A6FB0A9E35C5F98D
SHA1:	CEAD6C4416534089AE27C4A95F9B16145F5BDBC8
SHA-256:	ADD433F298E22DCB0C239F475BA57D3C0E04081CF4780231B0B949AD7ABBAB75
SHA-512:	8EFFC8887433BC49D6A826666FD3E948049C8651794DB438AD7CACA8D8B7E63D5F87A509F8F7BD0BEA715073BF530EBD141C83C265D83312ADE7B52D5F4B4FFA
Malicious:	false
Preview:	.x..~.Ei.{.....<.{~....H..\......[..WV..D5.....IG....W..J.&4.UT..."Ex.r..H.......].g......if.,..5....k!2Z.Y.l.....gd<$.#...I.3?.rx..-../......H>q .."...x+ N......>e..A..I.......T..+..w.{.7.}.nq8..y.^:\.....f....\a]9.I.b...!..K..D..`(R...M.QU.... [.m.\|u.......b...x.v..II!E:.f.^.f<.[I$..}C.q..F.u.m...J....33..<Qz.....).-.....UTJ.L[.-....j..~ .M..A.]..S.;...|.E+...[H.."8? ..{..d.9.?..k.7........VY.se.s..N...1r..[...el....^....bz.&.9L&&.B[..9..G.........k.`Y..Y....v6..?c..'M....I..n.p.!9me.

C:\Users\user\Documents\BUFZSQPCOH\QEURJOJQOH.mp3 Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.869445735260569
Encrypted:	false
SSDEEP:	24:ovOqgTp5WRRJK3SOier2jwcj2w6FRe+uxwtkuRnJMAWguutrmD2:ovOwRvsAjwcj23ReZ2tkuRJMdim2
MD5:	F324CB0BFDB11E67DC56D76D87CC0821
SHA1:	6CF063CA59CBAC026E17C43DE556CFCB1727F699
SHA-256:	9E0BE9609236AB95AE16484D6FAA4FB9F2014B003D3C852E739E98F017FFCB22
SHA-512:	6F4BBBD622319842103D57538A13DBF7F2D13685C7C101877FE9A0FE537DD9B4E3A1FE9A2A8AD36D350CC8021CCA0C891647866976539872706 55F3A06CAAF9E
Malicious:	false

Preview:

```
.....X8....-...<.p{.....Z\. A....5..p......G...KM7T...;...<.v.T..&.*F./..H..........t..T......U..ua.S].c:..&.NC....~.{..gq..u.l~G.X....&..`.._._.._0......\.l.............._..@aj.H..3..x:|....G?j.n.....tf..:T....q.......6.......... ..0n.9....oh........T
.".d...N\.9h.lD.|.;t......y...i?..,..Vi....u...'Q.4..o........sR...$..8.P...>....S...8:....a[....._?>.....c.....2].......PwwQ..?...VC..O8..W.=.n.e........&..U........c.i..P...h.5L....jgTx-....'..@.;.C..uU2F..a.7#..W..io.6....J..........l........g.
<G.S.3...EM.m|...<...*.Qn..5..J...h....C%.....l21..../$~.Y8..^...%.$..i..%..L|r...lc....Q.[..7.y...rd.n_...p...03.p..q..+y...'E.u....!.f...  .MH}.7A...,.T....\d].]...u.....:<...ej.<..+>...x..|p.(.R7qt....p9..*..?..t!4a.l5.Km.p..f...z.g
..R....&..3...J....Yl~..;.....a.DJ(tK..9u.....EO...sa~.z.z$...l......8.....#..sX...>.......Z.#..y..v,.".6..&6..`.g...l.>.).D.B.K.1[J..>*..|.B.P......E....o&#k!...o:....88O..N..|.G.../9."\R.c..".T.A......
```

C:\Users\user\Documents\BUFZSQPCOH\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false

Preview:

```
-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .
i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o.
.f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e.
.a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.
```

C:\Users\user\Documents\BWDRWEEARI.docx Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.851160577932306
Encrypted:	false
SSDEEP:	24:tpd7U3T6f5EPG/NlfR3TiVZWmyfdxnnfBT946e25vB5aNbZuutrr5nlcg:10uRTFEjiSnfBJ46Vp5eTr5lj
MD5:	49EAD17343888625525E483F6DFEF9A8
SHA1:	F807B7D2C1D581C3C598E0C187B731214D652304
SHA-256:	5E3696BBE65DBAC1DD4F93471DCC1CF27CA1714281287AF60F482B7F0FD3D5FA
SHA-512:	91182A13130774079B008A647A56D0F05D6DB7EF152FC387043DE382FD6617CC25F9D7B283365F85A7F0FCB747CE93FD2457B9D016DA27BBB55231447930845F
Malicious:	false

Preview:

```
.cn...)$qR......Q....p..O.k...,...y..J..2a...1.C.ut...4.i....*..z..0..t.Szv....u..~.!.~w~.c)c..1p....:Z...v..^?.#...G.|.$......)E....j8-.wJ#j8....5.....X..R....7......  ........s n..-...bf9.$Q.(.}..[.6.!(..V.R...e..N.G.#..a;.< 7.9..YuK..@..M
.J...3.y.y.l.K..0...MS].....=.1p.C.F..:px...k./!.....0.f....c....o......UK3x..o.g...J...E..r.Q.6..!..s.E..).-.q........v...x..(...b./.X....T.{lMK|...M.N...[F.wP....j..zm* .......[e'|..y..p.VT..U .......>.u3x3L.i.O..a...'..w8_.1r..B....v...$
G.......q\.~R..WO<....".Ww....)....~;;....a...6o2^;yOM}Y..[..)(..u&d...3.K.....d&`"...5'~pv...{..."...P.g[...h...A4... .y.)..D..J.l..*....t.;....d{6.B9..B.v!.E..R.:..3ZXU..]....F.z...'{n.a7..[..d....sT2;..pJ.8h.L.%R...X.o.V.8b.6+4
.....,I:O/..:<....}..c..S..(.6M3z.....h.~6^....R...f..P&._}....j$z....K2Dq`>._.r.`...3.0.p.k.`...H.N&..v.,.S1wp..XA.J...&.h.....E...S....N.+y;D..".&....d..#.|......6...!...p .......$5....A....g>R.....B.]../P5..$s....`wOv........{
```

C:\Users\user\Documents\BWDRWEEARI.pdf Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8586010024663535
Encrypted:	false
SSDEEP:	24:swqHDL2lzamZ/hTMyIVXv38kGwkEdnXB6p4BvuuVGqouutrGmn7:VqjLSVhTrlVX6Edx6RuQqqGmn7
MD5:	24344C75AD43C4B5D8886B4036CDBB7F
SHA1:	674DE670659442804975C5066E7E652379D83961
SHA-256:	D79784A67E937F37F3CEDDFF48B3F5D40360EC4AE6CC384351A019E9FA0403AE
SHA-512:	5199A5DA8B77B79EC73EDEC9A059DFCC70C31E589C557107988ED659F3052EB0E0E590AABF5A4B66FF97FB53B5A5D0D89BCDD95D805A19AC57C90379F15BC32D
Malicious:	false

Preview:

```
p.....^..'L.B..d..K.V.}P...5.A.....N)..>........_I..I^....>.=+....|%XG..faa~....d..E....r....t.)2..yY...GT.._w ........J._....6`...R..CG..WWeP..F$..9.h..q..0.l..qt..Sl.............{.|.@v.(.3.HP.....TLY..s...l.qm....l...K...'...`1 +.v.,...y.
n7.Q.2..cyfd...@.l.....+c...|.p*E:.j.r....e...1.+.b'.......s-..5.D.{S..t]..."].R.E...?v].N.....<.*D.J..."..-Q....F.>.v..i.v.Y..^. +...H..].''8....5...B.c....i.>....+..|.{..J.N....p....,LYG....U~...[.V.....|..L-.w......%..f.9w4.i..4\..8.<.J..
#.wW......y......T.{Z.L.L.57~.... ....?.?].m..1.[r.8.0...OM.i.x....&.|9%.......&...".bf........S)k.,...........-....Xc...l.G.*y#......z.u[.....l......  ....G.......  s........6H.;...."...L..._.........D",~&.DpBu..i..j...(...6..//..G.Q2].e...n...t.p..~.
.2.y..S.n2...~.LK......B...w....l+..A......k...9.`".....3TM.cH..G...a_. ...8......w1....k.z.#CW...a..s\..t..f..+.............l7?*V&..../.....W3.b./...o;.Me.L.k.....<t..M.9.w.C\.OF.m....B.#.s{.(..sz|.u.\...T..}..G...Srk..2nU&.
```

C:\Users\user\Documents\BWDRWEEARI\BWDRWEEARI.docx Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8499971466675875
Encrypted:	false
SSDEEP:	24:DJEuT2aWU9BKaCwQM2Gty768jWH0Zo6Kgvl4yeuutrPWh:DJEuTrl72Z768jWUZo6Kwfyks
MD5:	E4B845BED48AF917B8DF895A48BBE432
SHA1:	708E1860C63A647184C7DCAF38BB5279013DC1D3
SHA-256:	65539E60E9EF95B28252831858EC955159C7251AFCF79BE65FF69956C31D8DCA
SHA-512:	8DF6D066D9E52B9152F24048AF846FA4E360D7EBAB9E82413FFA2560DF1A0AA71BCFC449C5AD971CA32574B11EECDD62C6631DF7B67736C4352DCBA7F4529A09
Malicious:	false

	.Q.o..^M..V.'dR\.h<Ps].>;5w......[....<.b.R>.kCW.0x=)....<....v..%n5.nZ.?5j....^K~...cf....6.&..J.%....C....Z"L....c.['....E....MI.\<.f~MS.2..`..!IN.#...j.J.PIN.5..v.gyX?.5.%j.....nz....1tq.xv.$...k...&b^......}O=.^W^h.. .>....3z.=X....}./...-....>..U....'..Q.O..Hy..4........?.4?cM\|.rV.....C.....I.SH4..........P...../.2!..s.-........./...:h.......Z.I.Q...>....\......\|....k>...%{R./b.....c....0.....g%......_...\U'...I...K..u...%..;@..!...W..-{.!...$.......0*]8..%i."d|.? VD...

C:\Users\user\Documents\BWDRWEEARI\ERWQDBYZVW.png

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8295796129686925
Encrypted:	false
SSDEEP:	24:x8enwz7jgpkSsJZFDjdEV//h67uiIXjPFo7NCBIy4EHHuutrHLBB:xJw7isJZlBGnw27EH
MD5:	0126A30323AD660ADBABDB79107FF05F
SHA1:	AD1DBF568DEE1BF43EF14825A61F4C2F4819C8C9
SHA-256:	B8BA3B31CC79C749D7AC6A1737A0CD63935A26FCAEC0C2740CF512D2B70FC712
SHA-512:	650C7F7F185233EDD1F117821848DDFD86B7CF3B1809254549E4BEEB8342F8804A9D7FF1C95C77067B3B205DD8E68C900DB5B879B09BA626C5B8ECC17F5B67BC
Malicious:	false
Preview:	.\..;f..W....3.$6..z7..L..{....#..s...D....)4...w..A..t....v.N.w\|X....)[.......#N..p_...-.%....*'..I""CMx6.P.0....J..5.m......N..V..U... .%).Z.s..G.[..64...]Y.3/.....J._../d...r..&..A.......G...0.>..$.=....$o.r..`..'x{......&.4.'V'J,...k.n. ..)..:..0q..'...]\|D..[.."w......9...6@..G..\.....*R...,3WU..U.~).Z.n.F9.^......\|\.8...Aj...M.r.R.\..j..=..wy..d..I....W.......0fT...>Wu..s$....]y.K..2hV...p.#...G#...(....G.m"4_z.YeU...A... ...#(....Vm...w....a......E8..K.G..n{N.. .c......>$2f..._B..C.Z.B.{=....Rk#a....Y..I....L6...L..[...u..m8..:.......%....?9.....b...A.0..wj._......<..i....g.\|....Vu.u0.....=.!.Z...4.....E#..Qj../....y..\.ZF"9......."~...z.e......X.c....\.M\|.5..I....h...../.L.X.e.<.c..V.na...x_Q.H.. ..'~v.!}.Sz.C._.,z..\|.i&=./...B~Zo#-..O...c.)Z...)d...*..).....Yv..6.6.*.r<;u..c/F.@.....'.Yj.........t..-]..._..9.4.^.....[S..T[z_...'S...G...E.. v.q$.>*Bp[.>..{u=u/..s.|_.....SYc&......ef..j.^n.O.A. ...$F...7....>..F."......s.;?..B.*...a.2.

C:\Users\user\Documents\BWDRWEEARI\FAAGWHBVUU.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.844970396281411
Encrypted:	false
SSDEEP:	24:LrN2SUYfCE+++RVGWw8zegohy0g7BeBzky4NcrSyDBIHUb1v8MmSuutr+DSD:Lr1U0CA+vTw2L0gtLyAcrSyDz6mY+Ds
MD5:	F37BA37F86D403F1E4029DCEA4BCFB5E
SHA1:	CC4BE8E37F6D0AB9B0F78832607B8289A72FC649
SHA-256:	D4DF7AA06402F5EACA8170DF9F6A6F9E035BAE90DC1E49B813306866FCA39FAA
SHA-512:	478B3216902C6CC1F478547817565CA9AA79A3AF96FA4A5948679C8E2C44C63C6622870F78F96D5DA600E2DFB823C5A0FFC53A7AEEC0C4E6152437C0E61901F0
Malicious:	false
Preview:	$..hm......I.Y}.u.G...=.x..c~7.["s+..&P..q.4.`.....?,.]......V!.J.q.....C.........."[....5..<W."...4.B._ZO...s...3.L.5.\.mBU.)/..m.W.....w..$G..o......0.{.... .F=z.qZ......6j.Fq.;.....P..I.......N..9.h...V..b.tc....m......:.>+B.F..$.:i....*.. [},Lh.D..q,^.H[.p1.3.k.hy2^..{=k.?D@...O.~....45..o...>N.=.]...O....g!..9...w..&+..^g..GV....0:.$K.\.>..z.e..s..4JW...-ajk.....,:...D(..y....I..n.oq..Q+ .m.r.........I.!....q... <.....X.'..n.p.I0..1..L.cE...~S&....D&d.s.'..R.. .Z.n...#...xV..@..tNE#.t._G.....N5...d}K..;.F........H..I.......'.....X.Ui..(O.3.u7..`"_... ........n.r.^...:d.!.;.....)(.?..^......Ds...C.../'..........5]............w....|o.M.dHLw...i...\n'Nd...Q.!n>d.x...m..a..h.pdO0.xO(.:..[V.y....+...`..cI....c. C.}..]....:v...!..'J..R.C..;X'../..^..y..O.y...?>>...$.h8../.\s........5.v...oc...j...1......|.>.>_L@&!08e..Fq\..y1&.zX..[.i.1.9.....6867G>a..q..*..L..G.v..D.S7..0Y...':).......O....7...M;Q...E..4#./../...C.._..rc"..-

C:\Users\user\Documents\BWDRWEEARI\FGAWOVZUJP.mp3

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.836978774279727
Encrypted:	false
SSDEEP:	24:pZ7mtY3GjQ6VxGcsLSOdfm5W8wijHIKaKheUDXTRWuZuutrEE+:pZcY36VMbSO45Z7lKaKQUDXTESz+
MD5:	AAE37AE4FA0DB14E740EE0B4CF21FFD6
SHA1:	D32D91009D36C9B6977532B231046D0DC4B7946D
SHA-256:	9D35682BFF0216B2ADBB4EF7F7AD53B5D855DF82B81299ABCBAFBD865872C222
SHA-512:	D81FF2E324F7A1A035BB8DBCBA16C6AD09BCF12289C94FF2A237544EA119FF27EB1B397B947275E62E4EEE4AC8AC5D91DB352FDCB6E900CF5BDDBFEEF83A2D6F
Malicious:	false
Preview:	Lkyr......h.........E.T.."..7.....6/...=C..:..t...|,,qj.......A.d`8.~ ^i.N".^...|W#.R.~...X}.2...f.[.v...tX...KS%)...O]h...........4..!@.4i.I!..H.&....w)..z..i..........}....>P..q.q....k.J.I.%...A....y.q..I....b$].d..(a.IJ..IJ.h...."...=YS.Z......L.. J.4q...yJ.]..i..id./...I.8.....@.I......w.@.h.#.I..wli..6..q.L4WA...Z.$...6Ep.]4!...Qa2..I.3....s.v.......g.....9a7 V.\.>..6.M..1..._/.....:..O.........^)..ksm7.n..d.wE..^Db..t....E_..>i.]......:..^..W.......HM......_......O..6=.}]9.#...j.M 3.^... ..&!W.0g_ ..S.j.w.EYt.*.J.G......I..D%.Y..u&....J.qS'...f....c.f.............J3..d.......)....=...X........ay.....7......`n..1.....J.>..x../"........!q.Yq...._KM.v...te+.e6*P.....3.O..v.88M,...L....e...o...{:2..g.._...h..P...k.u...,..5....z.. k.A...i.-.!...%..w..R.S....r.<c..K .C.../.6Q.....n.......L.....I-.....v`1.p.....%=p.Q..pD@h|.S.R>...z...p....6.P#...tu.h....0....IW."U.B[D@.....I_.Z.P`O......j%...1.....5V.....-jz...k.v.<fV.>...Y.....?.

C:\Users\user\Documents\BWDRWEEARI\OVWVVIANZH.pdf

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.832291176219439
Encrypted:	false
SSDEEP:	24:JSo1L9Cg0HMaGTZCn0mW46EPBm67D5EfdaqYiP6cF4uutrTH:JSwibmCnRphs67FEfdaPjcFaz
MD5:	A9DF727F539B803BBD45C94EB1128B19
SHA1:	6047B3A25AAC57B3952C1E615B069B3827691F60
SHA-256:	3C6D99A4F11B0502849BA70C5E79F2B2B3675ECAD69170F1FDEDC1CE5CAAAFEB
SHA-512:	0759CE99DF3D5E1A45517382E153815884EDB8EE1468E67B32EEAB9ABACA80544E14D09D70CD51B1EAF82A2F802D602BC9F43B1920236B6B87BFC6401ED69697
Malicious:	false
Preview:	......C.k..?...O0....b&....x.b..m-.....dZSr2y.......93?..|.;.U...A..Q...,w'.s*y.....Q.(o7....f.Y1q>..A..h..}v7....V....!...-...|y..u*....a"......v.....D....u&.t....{d6.....R...w..,n...3.&...6.:..g...,.X..E....D?..*\.k(1.;C......[..Hl.ew..e. .....he$...m]....hq(E...->X..hS`)[.L....8..v.d*O<. Da...........C..45.....c.4...1x9...y.F%../.%@...Q....B.4A.u........O.....8z.x.{..'...1.UZ.......&.r....6.. .g.&.L...j.z.iU....>.....o...}..^vC...&..b.K...o.................E..xA..d9.*..I*, 3IP.h...V........-....qRg..^<*.~sd...9WTF"......K..MY..BE.5.N....N.b~..y.....`.....w...aO.....R.$.....u.Y..<..7R.P{..-.8.\t.%.-...iDUng...[.p.C...[.C. ....KZ.7...iS..... 6B.K..a..aE.Y^Aku...%...ZNX.1.c.'T...\...7.........P<P.I.y.. `-.Q$.j.pt..m.i..`Mw..f.O....+`..^a&20..q..,.{...O...!..9. 1...f U!....I.vc..t....;I...-)$..<.. H....d]..r]6...$=v.v.VS..t........$.T.{..$........r.F...KWRP\u.9s.Y.....t.^..Z..q...k.....~..A.%..-.4.P.|...X.r..R.a.@./.....%.D.....I5..Up..+.6 _.1FU

C:\Users\user\Documents\BWDRWEEARI\WDBWCPEFJW.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.85164442494398
Encrypted:	false
SSDEEP:	24:2nrLV23c58EWV/5xsobqh308BoPAOf33CnYC2yQZzyc3ABCcuutrM2:o3V23oSV/5HbYk8BYfnZzVycQBCeM2
MD5:	E5C196A48D8E75EB7C44077141ADE71E
SHA1:	B3EF788B3A5AC457A221A6C89072BC91F6DD2688

Malicious:	false
Preview:	.M.I.g..O<.4t...<..a...6in6...s&_s;#;r..;...>.`4:.D&4.0.?....A....C.y)i`.W.>9Z.Tje..{..f.5.x..U67..V.}..~....%.....J..zM...5H&....,..:..1v....J....5.._.U.Qd[+A...Y.U.qZ.>....C..C@.[.....D.....e.<..E7uW@.AB/..w.....wC...3 ..XBQ(.A......K....;z"8Xm./{.W..2.G.%...u=.........o.p%(D.q.a\.X.5.(.|......{..&HA..N..........N>c....75..-`SX.."O.....G.d.b..(M...j.Y.O._.....Ej....(j..iG.)`.t.}.su.{.M.... .G..z....m......Db...p..H...k?....`.]...L..L..cD..9.p: z....|B..hif.;2....(..KT. ..AZ>....T.O.nL.$...p.8........... *.k...."Z....^...i2.......f).~.^.$xH.21....TNU.2..d...f.Xi.{.2......d....P..p2.+...I.d.cQ....x.$~6Em.v..a.(....Y.dR{{b.`u...-.........1..yi\|5y..],28}. v.....*... ..!.<.....9..M..[...K....{. ....%n!#..,`.gO....3.!."".D.V..gfA.q&...../.H.......s6.y.).....~.6...q....w......7#P.h....H...$f.,..".o....F.e.\..i.....:........'nZ..[.JE.+.=.v..S`m.a.&v&....rgJ.w..h3.>.v.s..M`...Z...?..IA..R..)^i.gY..Y....y.....o.dhi^.3.@.K..S..+...F...m ..^..

C:\Users\user\Documents\BWDRWEEARI\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Documents\BWETZDQDIB.jpg Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.852918663607725
Encrypted:	false
SSDEEP:	24:U8lRWKIwoSBHji9zrViA401Hik7wpWicPYPkGyfKk8MneyouutrZT+:U8lRWqt2Z4P8GcPYP5yKklehZT+
MD5:	51FEF3A6C9955726C4F9062809D703E0
SHA1:	943A185B1F0160CFF0DB74B1D0DD4AFF40E2E9FB
SHA-256:	CE794500FC46DCFEBF696326C3CD80861112C40254D798803489D08A59373B5E
SHA-512:	F299AD5A0A81D406E05BC7DA06C21A75FC285B85534DD3C96DA04AF512C197011378B5DCF923FECB77539206C6B53E333FAA87A52E3C81D6AD09781502FC2420
Malicious:	false
Preview:	...'...|t.&tdr.T..t=....#.36.[...P,..#.s.j.!.......Q..+}.O.......:.........g|c..].-?.({>.....6.......$..N..L.n.R...V.....\|.....~V.t....C.L.Oy.]...8.n=.. .V4R..h..\R.9.${.....e..n..7a.I?.wX....D/....}..o.s..@0I2..$..:W..2N.{.~'i..}....C.@..\| I6.r..G#!...;.{.L.....IP..t.qs.p..w..,...sR%c.`....u....sW..cn......5Y...(...C_{............vK_..HW..x.\|:f..>...WK._.pf..U,b.1i...?+.F...\...[E..t...3.2..q...;.@..."......@..=..}......JV....e.N...h+H...]N9.x*ve._!...(.......iO..%/.Q....... vE.BMo.....F.....I.9../.]*...rtB.j*..q...8......I:PS....NO.H..e..zC..]8).....P...;...-a...."+..F..I..Z.e.........Rh!.G....J.U..N.iFn..3b........)..n.t52.....`.U..A_u.a[.t.=.i.{.....i.\|....g........4..9Q..^.q..'.........s..J..&.....3`../Sp..@b..!....G o.olU-.;.kV....I...R.&..O..qPd.'.sz....Ca..?...O...F6G\...X.^.r.@..Q...;..t...xA.Z.k....`z...$X8.#.%...P....1.'...g..p.H...@TF..5u+.G......|......H!..X/.6...%.......B..4V......t ..!..\.xP.o..`-...u.....U..$y.(......

C:\Users\user\Documents\BWETZDQDIB.xlsx Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.828931267352967
Encrypted:	false
SSDEEP:	24:ywrZ8Xfo1lZ5OSiw+z2qOUWVNJqlOQ2wxBu3AMOj1pnwdtalvuutrEc:ywaXALHi2qOUWVHCOjwHu3Gj15wTyJV
MD5:	ECC2F303FA045EC576912C075744A5DE
SHA1:	C8FED39A0E9FE3BF5A81A1074787012CE9BEFB06
SHA-256:	DB11DF6A274396DA7286DFEE3E50FF7A45B264FCF9511511D7CE9E47E84610D6
SHA-512:	6D367EFBF2839AE93E9455C8A63517B1FD893C12248A7005EA5069FA0F39139ED1C69CA70AD372B3021A4EB0812F3A5F0A69590F6F7F133D905802ED66F4F74E
Malicious:	false
Preview:	d..mW..W5...c..S...M..Z..a...;..q][.....K,..H.Z.......L;.Xw.#<e..'.f..3b.U.X(A]....w...E...4.u.r..*....p...>..N........r.O=i.<.....Z<..L1i...r..j..%.c]..8......o...."...<.l.....)..........q.-.....a..........q...7...:^.....g....$.::.G.~..>...*.y.v<.g ..L.oz...OQ.M...i..u..ar.3.)k ..6.i.. ..9.%...I8`..z......q.ccG.p...0..t..(U.Y`..b..U.=.yRs.)S..{..:.R.5}.....y.],..~r9.5.N.`..B.N\...K.l.2.*0U.....]..Zk.(....\%........p.K..F.......Q.]...u._a.bU..[...S9......n6@0.....S...A.*..2x..- kT.Pb|........h..P..k.....DA..)0&7....j..&.Q..Q...........t....5_.....L*]|1V...^.....4..58.).:.7...R.q..4....W...R..j.f..Q..k..0....]...}#..I&,....p._p......[......r...t.Q".. aG..]!<t..L.w..O.eku.!.......&o.p...(.#xJ....ch.(....b."...Q.....>...q.... ..3?..t`.....:+......s.o...;.WH.V.1..:....w..%..n^.pg.R...w...N....lk..w...7T...Z.-P..Wn[f2.........epr....)....dE...D........r.t....g..?........y...t..k.....O.:S..*y..=C.0..,..a3....J....Z.{N&.|........Y..S}Y.Y..?J..Q^

C:\Users\user\Documents\BWETZDQDIB\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Documents\BYIMNPJCRL\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc

SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Documents\DWTHNHNNJB.png Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.828088494617048
Encrypted:	false
SSDEEP:	24:QnOOj1mOiwZxe80e11TAPTGJmTq0iiEtv4bcmRV8a/m+L1WOuutrM9sGpM:UOOkjTzKWGJCq0iim4bcmib+L1LM93i
MD5:	22A637C542BC3641B48001C83C739BA2
SHA1:	267C0757A80124ADC79E49C04292FC34CDA1E64D
SHA-256:	0F300D08C422A1F7F737ED574EA864074E772C61689CAFF8962427CF286B8F76
SHA-512:	DF7FCB1A6D8215DC924C413E4E3492BC74BDEAF65AE62E5F11B6DBA7208416BAED0EEFD996C762A30AFECD319F24935BE101060BE1B9CDF87B433C1B917A970A
Malicious:	false
Preview:	Y...P../C.OW;..v.\.Q.v.!<(..F...7e.i.wq.~..R..L..).K8......I!....3N.......;......j.:..e..<.V.......U...t}N..._.3....N.H.td....-c.....qO5r.........w...I....T...........K.....n.P...z<U.......q3$z...*...C4.5.cU).>..6.@.%.*..8....b..4r.\...c..7........]..0....m.J.k.....j..b.8..b..#.!.}.\|+y..............S...(VT\Ndz..V".n.\|_.]..m.g...'..U.<...}p,.W..y...U.\|....g.H...Z.2.=.2F..!..A...L.w.3.C......W....X.......x.....'..z+....I\|6...y....M.Nx.c*.&.\|.V.8......_...?....q.5C..t..9.......5.G2..U....,.D?DS.#]=.9u....,/.P.u.oJ..QN.b........Y...6...+I......),..k....?./Oa..U.....'.wFStF@.."......J...j..+q...S.:....2....v.;.:A.5..Y\...B...E.N.H86...}..b.D.....MIAwb..#...R.....f...Z.............WeM.I...B..e.U.O...`\.......K~e..K.....;....W....pk..>.r.......-....g7......;..6.E.)..1.,...~.T#....e..%.4f...Y..=(......H...g.>t...i..<..;....2.^..B-*\|......iq.....Q.....k;..4.$]B...a...gS..c.......$.k./.Tx...oKhoG ..>.+....ce3.../....v.j.....-.Q...g...zN....V.3oBw

C:\Users\user\Documents\ERWQDBYZVW.png Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.846998844467571
Encrypted:	false
SSDEEP:	24:2Mk6jF+scHNxV6QLugCwO7ezdsHkA+a8ZcXNnpGes3bZuutrRb:2wJ9cHN3nOCOkAnRnpCfRb
MD5:	EED2FA30CC2D1DCA22246B53EB3CB628
SHA1:	4101B39495D5045746A761B3DE6B1EF9F763B598
SHA-256:	88470E2BB698B9C9E7BDE85E1C34C5023B91CC75B8B0CB6E4456C26BCE47A978
SHA-512:	33D65E1C746C57990F169E8C02ED7D5BA1A400D1001B781CB276C212FB4BC0C95E4047AA205B4A99372E7484718CC2627E2070800F7B7D02AC040D226ACB5A0B
Malicious:	false
Preview:	.3..4f..$....$.*.....k......{i].....E...^I...f.]....q.C.....n......s..D....|..cE....yu5....;.............a.i..b..."../.gK....T.V.Ne.eP.Zf...:.(..!.3......?Cm^..(k...K...K...0....X..t$...jd{..{ ...-..b.5?i...-.3^gz...(...!..."!..}..7...)d....4...0\|.."=....2..k0a..{V.).;~Z..;.Q..../(..IG...s.......~.......qU.Srt...5\|.2.h....5..#.W....Gca..-6.h.p.t.......j9..b..Q.Nz.....Y.jj...g$.........2.R.Oko.y..W..]1....k.gv.4myT0V.uY..8n...jk?FM........bb..+.XQ.z..zju.2.i..L..+...Q.c.Z.N..e+.j.........9]..-.0..<..~..N..O1)k...!].~V6Xx.4........F...W.D2:.c..pz.IK[..f..=.-~.z....x.......A(...m.U........^....:\.9 /..|...R.M...C..)...._. .w..!...}...r.kphcJ.....}....G.2.;e.|.r.U0..+k...w6.>A..XK2..xs....$...Y..7&.jP.!.y.0...$..r@t3.4n.;.~.yV....J...S.o4.{..{.,ol......vn...,.x....Y..4................v..&!c.`...&..|..Jx../;.qD.="..;..Uoc.......v 2{.#...-........].........)aC@.;.".q..:.#C.L.1..B...S...?6J.....rn......9.I.....<..TwWQ.$.wUg.Y..}..1x.....A.}..

C:\Users\user\Documents\EVCMENBQHP\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Documents\FAAGWHBVUU.mp3 Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.852981189201204
Encrypted:	false
SSDEEP:	24:rMokXs2ibnhH93DCrqzxjtJbOpICZsRK/dA/fCEWMI5kFdnv1guutrFdjE:oohhaqzxpJbOp1ZCWu5WMImFdv1ir4
MD5:	A09C1C099651DDD006451083F7D81B11
SHA1:	C23A5CD6967C4E17FB30461AE9C28B5F8C7A9AE6
SHA-256:	D61B4848D2CD9C359AAA4865650BE81648D2CC0BFE06A759580442616DB59273
SHA-512:	1202FE7F5147D99B57A187EF227876B9B972C7DE9F0D8B6718548E3FD7376E3B19FF7A04C77419543F8770E277F83BD2400F2C81E9FF5C9E5E962A0582A9185A
Malicious:	false
Preview:	..Y.../...B....>!.A!^.K"...e....tye...@....d.L.2...d....T7....~kB..#....`.;.`.....G#F.Q...?..{...i.?3...=.k.>...y....g}.z?.H.4......#m....eq........q..ID(xZBt....9.......`..(....D.r.pN..0...../.S.T.......r...... ...K.7.e..#.'...`}..4......\.Y.S[F.q.=...>*.. ..I.0....a...T5.w.....[...Q....D..6..57..Q..W..6.xv.......T..v..gx...1B...).+..8..C..-.Z..)).;.8.....`..S..._g>..n.h...'q.B..;..M.*...k.I....B.-.....P.t.....y`.@.o8..&.D.*Ad.0..t#G<R<..tt=X..1H6..A.0...!P. .[Xg.Q....b.....F.X...85....F.qK..C..E..1.eo...M?.....H.Ow`....?x{._..Q...Q.....3X..?...^...1..O.Y....N .7.&.=SSB1..96=.....<. ....W..o.z..!J=..R.8.yj.(.o5F...<v71.........F.b.gn.9.mZ18m..I..'.~.3I9..$1.$:.|)."Rh%..nn..c..I....z...9....c.....n._..L....y.#..z<...z....?.q..L.[..D.$,..rVv....}..i.....7..pV.o.Oh.(M.w..>.n..=.......I)+&o.I.U,.-...q..23..9Q..A..{bSJh...X~....9...S..;......%W../6.]..../.B...sa.HI.{.^J=>.....'}.YXYD,.YV..eK..r.....b.e=)_.........7.....?P../.F.......

C:\Users\user\Documents\FAAGWHBVUU.pdf Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.856673765896535

MD5:	9F7CD0BD1316672F15BD286251E6E92D
SHA1:	9CACFB74938CE48915A861BB36A9F852B5270536
SHA-256:	4223EEFA252E6470F174FEF0C63544CAFB6F59CCD0E715FDA147BF16A13D72CE
SHA-512:	0EEF650185B4C7130241C4648676FA822C1ECC0A74A9BD079215AF75AD4F3589489669F21CFD548FDA8322DEA6E3674745F135BB71FD9635184222B641125B42
Malicious:	false
Preview:	......^...y.../Pt.....f].'N._.#pa.N.-hJ...q[.......p.Q*..5...;;|....Q# ..cAA.K..nD.>.w.c=..6w.|..]...3.RbDA.J.=-.4C..m..._..u....i.E......8.OU=.WG.Z..},....{..Z.o..e..Y...g.r~.].33n..!.>y.\.NX1......Y.z,.......f........a.T-......+.3.....v.(5...>.....$g[&.D&.0.rY?.1R...:.:..&.........4?...38.......:b.J.lz........c..kC=V....5...P..t..|...#M.L..f.Z`.QV.JV.D;..!<1...S&.}s.S..^...ml.....F.W.k..h>..)O.l....v.Ty..o...4..s...........o..-.qX...l{.n..f..hU.m@......h.t.R..).l....Y....`..f.F4.....d8a`HqbAU]...'.Q....n.6.g.nmz.../.........W.e...N.N..l#.&.]...E..Q/L..a...k.t;(.6..Q.".....7..z...]-y........R....>7..MW....lVJ..l*.f.K........wl........{1..D...K....lS.Z.f.....].........0|..).....i....>.......Q.B.`........RB..v...fm.\...o/.....z .O.x....~l.....f.....{.0.. ...@........y......^.{}.4.].....*...H.:c.[.BUy.........-....5.=..C'rl......*.......N.cb..ua...Z-.....&..i.......7.. ..y..W.L..w....<.rn2g.r(..N`.U....!.S....L~.%-.3.5.`.:b

C:\Users\user\Documents\FAAGWHBVUU.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.865058587097625
Encrypted:	false
SSDEEP:	24:s+AOofThG3ef8nvlitr7YLf7xXrmbF+4brw5sw7qQtTMuutrPm:s+rofVlykafdb9J5sw7qQtTuu
MD5:	82C8DBAE6A097BC139D28FC98AAE0D61
SHA1:	DB2026C6CBD16EC7E9971531B7F4925841CC5A49
SHA-256:	4E28B4AA2EB3D57016F7883CB314CB7F5D58B340E141C6DFA32E0F1870C6A17E
SHA-512:	5B43CAE1EF45B920C2F9ABD90FBE540D2E5E1EE64D131A52EFE601E2FE15B54BE097899853679B6785F500C19D3C0ECC523C6B6E14C0D5113630DD31AFD5CBC7
Malicious:	false
Preview:	&....<.....l..{..B..Q.7..-v...fTL.....^.z;.._..2.........;u.........Ne..j.!l_H.=../.l...+p....U..yZ..zH.-.../......Tqq.t.C~..>.&;3....DQ.:V........Y...1...mO........!v.&.....!...^;Z.".@.j:....M.%.E.m.)&..aix..o.R`(..g.Ze.G..S{/..Cr.....V..Q..0.&r#..y<.-...H...o.T...O.l8>}twj./......j..:...2z........a......8v..G..n....8....F....A./Z.W7...?....rg....auO..D..L..X3..$.a..-.&F.....i '.>.......FC..c'k...c....V.$_.M.h.].LaO_....4.l.=...Y.Qz.7...[.p.|......}X.g2.B.@..e.k...5>9......b..O4...s.FV.F.B.K.....B1....A.[0....*7..........Bd..).....NRj..&.)..t.........v6..G~S."0Gu...q.~.@..Jv.i.a.....l@.S.L.....x.....#..'k0..U4....'.._$..1vg{.J\|.....l...c^.qg...v.j..W...w.Z.Q.KB~...S.c....c...:?b^.r.2..{....@ J.K.N.k7...".FK..g.!.b..Cd~...+A3............B.T...J.......pWy.....-\i..m..va.Y7Gc3Q..Q....<U..Z..Z......~......N._...nx...<...flU...w....\|.%u..K..Z....=....*<a...K.!.6._H...L%.b...m...W.S/..y:....G....HBf.$k0...3......V...6W.+.Jlr..X.z..M.

C:\Users\user\Documents\FGAWOVZUJP.mp3

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.840829790949455
Encrypted:	false
SSDEEP:	24:C6rCqnYrdfu2wlDnr9KFEYtWKDLlOkQmau6+Z+9l9d+txuutr9W:CQ7YrdmnlDnr9KFDt/93a19lz+t39W
MD5:	CBC639C7D7CF36953B21081E6AF78D1E
SHA1:	BBA832339C19A239334F50B79FAAFBCD2638531A
SHA-256:	2FA2943DA0EC9C9D05A1EA90619D8E91B3914F56D3C0AEA22718A027FE05743E
SHA-512:	772C586A7CC486E18ACDB3D4F5EA75B7E0F67C5E943FAAF615E5C203F6E2A5748DE9195243696BB5C2ED85476EE8D1EECDF0D0510FB57DF8A94BA77EFAABBC53
Malicious:	false
Preview:	9:.6 .>+r;.b..~...,.^..V.8...e..#.hW.QV..h~68....lw4@....p:Ef..g:.k......j..2.]...xw}......h...;.....7An.8v.l*...v,Y]q^R+..:...c.+.?.....z.|..O.l...O\..........<...q5g{^.F.:.3.e'.........Z#..g.>j.)...$..n.+..@.i.`.....@.cg.'..xT!.+y^...[(...M......re.R.....ok..%..e.F.M..N.2...... .....':..o..ES..l=.9..mB...m.A....~.0...6J0..........u.Gcivy.Kk...=7....<.?Eb...yj5}...=.]....#.g..k...G..Bc....V$...r.cP...!.ld...g.>.5sY_.J..u^t.....u.B{.W..BS.3...`&..Z...|4-.n7........*i|...iV...K%..C..5.}....-....8..!_..........=~.Zl...s......<...C.=T......0b.~?.+%^..G2.HB?..(.J |.Amux;.2.y.+U.ZNRR.e..Y#.R.v.e.R.R....j>t....%...f.C.b.0..#H...<.O0.@@...!ZD..h.^^....g...K...t...c..1v.{......K..k........U..L.N.7t.f#......"....$H......d1.d.rU....Qq..%O..t>Z.T.B..#....<...t."O.#k..M.V...W._....v._....Ngl.7..y....x@.........R.W....-....+_@8.Y3.....zuc\.m.3..TTl..d5..........n.........l....m.;...F.`a,.......].....i.N...OS.G.%.l.2mp...Q.o.'%.<2.._..!.k

C:\Users\user\Documents\GJBHWQDROJ.png

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8442053544294685
Encrypted:	false
SSDEEP:	24:rCtOCb7/iejQDi1E+XcqLR/1XDRPJ8T3k7efOmdgkmTnOFYWG0uutrMIE:Sy0JP/1xJlk62uGjOmWvQ
MD5:	0428641875B67A7236CF35A6B3BF9FDB
SHA1:	712FF93FEC7C7FD20226BF7D0201410A9110E05B
SHA-256:	03F4DC55DA51F1097DB6BA2258014196462877B6FC886A4404C075B3BA8D7EB9
SHA-512:	D5699B64F0551705371BB35C9C89569C2C7A98007F856C02BD45562EE66F325B5BEC4C4D56A27D9CEB01DA5D6DED6047F1CF97C3D64AAA4661FCFE83AFC893C6
Malicious:	false
Preview:	..Mit.......r..Z$.b..Pr..sL>Y...y..t.X.R.q;../..u..c:H..G.c9.f....v..k..t:....1.....S<.(..r.>K.W.{...N`...#..-..._.Kq...gz...,'..dm?.%.D...... .[.}.....a.]u.4'....,@......=.l~.(uL..U.1.F.V(..h.d..:.=5l9D.+M..E......7.vX.....;U..E.s'^.i..M.......G..]]s...u..=..T,.....5....A...}+.EVx.P....4..s..h..-...f.W.2{...k.p....R...W.6E-}.8*5..bC...t...{.B2../..A...... ......#.~.<L%...ngC.;..K.h.5x...s..C.O....J..n.....)......d...Y.SQD.A.:ksa.n.$G..6G.a..C.....q...@C...]Cl...C.A.}....3%.V......ru#.h.uy.`.?.W.\#....#a...D.3...U..Gb..7(CQ...N.bh.L.../..r.../...q{g.K}..F.p "..w.......S../s.[;..L.+.p......e\.+i.t..i:....~>...%.m.$.Ze.o..[....e+.v.q.. -M;.....4'.&.xc77.$......bP....L..N.|./l@...ha...K_.]......X.5...V..*ZeR!......c.....r.)AG....oC....d...z.B....B..4..he.L.M-^*.+#{.._....v2kT..{u ?!.+YW.'..m.w.P.X.."...=.3../.2F..O..c.H.7..`R.&..a(.}.....e.......Z....f...1\.5....aW..n.m..c.lA.....\.L.3.]...}P.[k.J..,.z.w.<.W..0.+......D....S.O%y.$..1....p.f.

C:\Users\user\Documents\GNLQNHOLWB.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.823227991232459
Encrypted:	false
SSDEEP:	24:W/Qrqd0zXRrXSAnwikQzCNCcdBAkNVjzSCrQSfqn3uP4lc5N+VNw/LuutrJ:hrqazXROfnGClczAOdXQL3Jc5N+VNwNJ
MD5:	44BD7E61030B36F8F1527C3E36C40A81
SHA1:	206D22D2DC72422A390208821DC1BF51A44FF270
SHA-256:	D054D59241A236DF98F036F81CF74DD9FAD84B64A5A14E3910F9ACF5661C68B1
SHA-512:	9410DBFD6EC7039B467896EAF74827001B33E5F7CB1B0C1BB4DD7332280170AFFB844F353EF3E3802FE8C6B9ECB3505DA27AF6F82BF00C8E500C61C8CD815A20
Malicious:	false
Preview:	......N.w.c&..j.K.......=w(..r....C3..Q.....y,tlq.....#.~?......A.%Det..U.:.6.<b..P.c...cR.......`....hsZ...z....w@....H..SyT&l.."P.F.ZG......;-ye.tF..E..o..j.y.J...g..&..@......KR>Y/..4pF.......u.....6J...y..[1...b.!8....."'.#..q...Qw..P.o......@...2...q.T.Yty(Eh9....s...N^.J......Z..70l.2..*..~K......L5...*.1.zl#..#..{...-E-..#'f.-....lP.r..{..BF.o.1...r..%.r.....TT.."..r..Q.<H.{......e..W..W^..'...m..F.W..[..t......yY....cu..e.....W.....'r.ik.. .4m.w.....1....s....E.."R.YK..........5..w....?n.c..$.2.b...FA....1..2..tp...l...d)..........bvl'!E..qs=:.......pmyc.."j.Z.....yW4.C ...*p...Y.W......+..]....^...$6...o..0...]{..x]4.U.O.&..c."r9M%.xC...?.D.Z.).D...dK.W.f.l.......[5|.....bRk...b.VsE.n..{.~D.C7.e<k....Jm.G,.E@..........C.m..i.q...._.-..[.<pg.0..9m.8....Jl.f.A&.D..W-..FG.?.Q...1o.]......A...~U......hl.7O_8E._..B...0......9..-h....cja.XF.......'....Q...Q... ..K.D....zMl...+9.W.......cRz.<..0... .(....h..c......>.O...-.

C:\Users\user\Documents\GNLQNHOLWB.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe

Size (bytes):	1258
Entropy (8bit):	7.835427049097968
Encrypted:	false
SSDEEP:	24:STz5UoW1gSRqKHWeS7XXbMjVLSngY1DKVRQUrYmtuutrJUU01:Sn5UoigScK257XXbGVW1cPT901
MD5:	70099DC44278B4951BA0E875111B6F24
SHA1:	EB7F07D538FFF22A7603A202BFECDEAB098970B5
SHA-256:	08530BBC21CB8C18A19FC93BD5E2A40F6DC0213CFBF69CEFD327AE241ACD2BB0
SHA-512:	5DDC429759A93AE936C6D6B10EDC05EE0B77C19EA244120CD371FEDD5FBF736919D53D4225B4922DD2260E4F5840C5DC91B7129555AFE4DB47B58DE644AE6CA9
Malicious:	false
Preview:	.Q.o580.?V`....W..`%.<ZR.uZ......A.(.q...%x..._.-..f.s....wW9.L.<...M*..U...F..5..;0d.S]..v...3...F3....(...S&..+d.Z.3.B|...;.`\..b/].T..B..}.\......D9y;aV.v.<_A @.}6.O.FB^.[{`...k2...b.....}.,..<.....v0..?..p.C..,........<u.T.s$ ...p...li...Zu..6.&...../..............h.W..I.fi..I..7.9..JJ..5K6....+...s.}/..I.D.\tP+.F.&^z.gs.4m.T....9..0"..^...u{...$z....v...[.oP.......^...._b;.J.......em...O.....6..C..fr...4......D.y.`.Y%.k+'X/Z... ..{..L-.wU.oo...}..?..K.!..+../../..NX.. .I..".B..\..$......m.#p.... ..<.{x..t......t.(.X]R..A.BYe.p8..ut.m3.(...9..P.+[\F..zU.,...:.s......w......'.6.^m.n...&.,dd.m.`.-.C\.2R...m.N..........`7.|.&@..3.[..4.S...2...@.y..O...nW.g.3kX..l.y.....p...8~.y....k.N.LCc...P?x.t. .d....#...'7W.W....6....d3....B..O..U{.G ..o.</......`....oC.i.......\Z.S.X...V..... ....bG...w.q]PT..*+..L...H(...J.M.d......wF...#P...JYB1..9...I .A;..^Z....ru.T..>.#w.......I+...hY...z.....u....h..#y..\\|.yt0...L.L..MN..Z....O..g

C:\Users\user\Documents\GNLQNHOLWB\BUFZSQPCOH.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.82318802002533
Encrypted:	false
SSDEEP:	24:lTkDEuGi5JjLNX32O8KjvXL601lySeaxuutrEcE:xtrjhX3DJXG01lDea3EcE
MD5:	9403407D02833AE1687918584C8C6DC9
SHA1:	648FA519366460699BE098E7525B734EF44C0E29
SHA-256:	7BF57C6B605B4C554BF745A71DB60878F3C324448EA213919F7160AA8AC292C7
SHA-512:	0BBCCD0829C4F2095BC186A2397DD98D9CE19ADC937845FC4D0C66491D0DB88D02DD414F06F2AA24275D488CD97D1E1A846916753207DD1279703A3F7280BF16
Malicious:	false
Preview:	ja.l4c..r.P....pp...W....nL.;]@@..J...|.wf..].Q.q.f=b...`/TY.%Who.#L....,.KZ..~.J...1J..=..s\;P.5Q.1..1.f..W..]..4...z.d8.~%..0..E....s...OH.%. .Q...}.I..p}b.v.`...-.._.Y...C..e`.z..\;W.....|.w..nGA...4..)...[..V).B...._...f.yx1.B .../...*.hWu..z^.wF...f.PY1U*....Uc.k..1L....1."P..F?#...H.S:H.v@...m..'5...v..H..M....\..L..A4...q.......j..E(}.(.I.w|Ev_K./.\....E.Sd2.>ZS....#...?.Y.n......*i..a..w3.69A...3u.=.@.|?.je>..%....a......Q..d5.#..>.4Aj.2...-.3..|=..- \.Y..l....^=.9.....B..~......d...N.lj.V..?..,...{.....4bA..,C....U.......t%F1)p.i*0`.....>\,aM2(.N..BD.-(..:...`.....E.w....J..z...aQ.M..I%C..Ue........UG.....|T1...^+...xNL.I..".I..._5.&.{."..>.t..>.........:5.p`e.qt.(........~.........X O.H.c...q.y.0.......4......z...........iR|H ......i...2.PK.,.D..;..21.%1G~....k.c...ye.B..8b....l....#.6^.R...A..........{.i.BPc%.,FJ .z....}P..^_)..c.8@...........x......t._...2pU.......,.< ....d....V..-.q&.....P.....-'....}.R...

C:\Users\user\Documents\GNLQNHOLWB\BWETZDQDIB.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.855351613994428
Encrypted:	false
SSDEEP:	24:UX1mK2CPtnGlzUX23Zu6tqw7OOSXuogmwuutrmXc:w1zUqHqhxd7SmXc
MD5:	4E54FD44EC288983C88E759AF4200893
SHA1:	11EC57833C9E1F28F23C83F087E2D56FFF1DAC65
SHA-256:	B0AE1D57421CD1A9831C15DBDBEA4B0572F5C66B57DBA05364F5C73F4FA350CA
SHA-512:	BC2C655C5D183144A0DF33B5A1594472FE836323BB899ABE830936021537E55B46C5322AE7197578749C19706BD2B18BF6026F33F8F06510042F7839719F2FED
Malicious:	false
Preview:	H..<.W0J....0>...=YP....5..%d`..x.4.y T....;62/...w.2N3s=qW.Z,...P...k...g...q...../...M....&......=.EE....V."'..O..s...}W....'..x..Q.P........[a2..x..A..b+.._..c%M.L....>9/.E.?..S..DjMJh..Z..NnA..X...@..::..\.,.rq,.qy. .B.m.......6kZ....8.`I...m.....1..t..J_*'.;m..Z...&.D....$..}_I..S..V..V\|SK...]...A.\..&...\..Pl...G......=....1. <;A.M.d.%d..]............H\|..q.=.7.?n.>.....bTV..p.v.,H...c.Zc......L.#.a....T....e8..p.M...\........;..I......H.\..k.~H.3.v.. \U.$Q\BU..x..+..H7.I...A*.....I...$Xe*.j.._..\|Y.s.c.h._. p...^....u.."...V..L.4..<..M......A3.2......\.PC.a!.j..5...o"....E!.....RW.#`...q."f?.pv.:e.z........ *g..AP.._bb_.....<..X..i.*Z.qw..x.D<....$U.C"T..J.r,..X.?..C.0H1.@j.. $.=0k,#.Z,...\O..B..a..i.aE......Z....;Nl....q..l..a.4u....5..../..fr..[.2...i....t....4...<..d*Q).Y.GW...t...){..$..+..P.X."*x.+kn;.&..kV....~(...cyE...=..l8."N....^.{.....8F..emKn-.K.....w{...l...o(6..RE..OW.DH.v.u+,5..9.L...+C.!.qM'l. [K.:H.[...N..e.

C:\Users\user\Documents\GNLQNHOLWB\FAAGWHBVUU.pdf

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.837859361967677
Encrypted:	false
SSDEEP:	24:qoFWWRHOul4gXe6PChX4lq3HGl8nCNdzr89ddiLQZ2X/hUUhlUuutr7RbmNA:rtRuTguQCNqmlcCNdX8gLQsDhl29OA
MD5:	43E2C0F0894554AE9E219099CE1632E1
SHA1:	9B75138D3EC13EB61421CC10F37AA356906DA5D3
SHA-256:	125EFA19CCA79D851BE6D81659BC9D18DC8A7E39496FA5E67A2C0ADFF3CDFAA3
SHA-512:	387EC75DAE145F300F8E7493C84795803E082270F8190465809D0125E2EA6DE760C485704654CE96970EC49FE033E9454127D6142F35F7A8D5A741281C99892C
Malicious:	false
Preview:	m\u#lg......@.....=......qd...^.:.ht..`.6p.*...kC}.....C..x).'..?..{.<.M.<Oh.#M..+h.-....v...J.p.6..7.2..Ap.....9M'=...'WA.WG.22...?G..&.....wb.n..?..7..D..C>..... %=Oq.u......X..#.T.f'.1{,..w3......#yY.f..@P.;...]4A;.I.~....]... %....o.T.UY.mr...v>+..... S"..Q{..Y...^^Q(|C.^.\.`]..%..*...x....6-..)!z...k(.eX!.....r.4![-U.....pr...q..".2[.b(.><...p.......S.$.~..0,.....'..RX/.D...0...Hm.........>h.....~..q....g....p[m..qQ...M...-..../.D.%KP.=...f..P.}Y......?_.2*9.x.V. (+..FF...69..\|.W.. K..]....g..dR........ ....ZN..../.....cE.&..lo.l\|.6..{.B..70.../. .87.$...4......[.N94)k.&......+H-........g..k....V.O..~z.q...m.).'%..A.......t/.9..'....A.X<..D.s..E..........9..f..u..A.I....T...o.U..C.K.!...k.n.h..t fD..6;....oi........M.^..F......k=..# .@...X..:X.^Rk.YP.g.sw..t.U../.\.9..@..T.?HX..*p/! .p..~e.~../.V^m{.I...\U?IM..Ez..&J.N..j.....I.....#..$i.k...%.zV!.%..c./.`..1..b......Z..z......[..~..Z..u...,....QR..<L.Q...7m._.

C:\Users\user\Documents\GNLQNHOLWB\GJBHWQDROJ.png

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.839821363791326
Encrypted:	false
SSDEEP:	24:t14HY54/3q+H0wkYoENjm3R84yIdCi3Ol8uutrd4bU/:f0YQ3nH0vMIsiLdWY
MD5:	1CDBE8A6FBBC023BC9041C3F077D68C9
SHA1:	2161140EC60D29DEEB28BD01A314EFB96D592923
SHA-256:	00D222B06BA72F29ED328784DEFBB2CA13240448E7F5D1DC2EC9439226CBD11C
SHA-512:	080F0B5D631910421CBB9EBD64584E6394C24A34AA3CFEF32F010550C10EF3841A1C7263D8CB3B93084EED16711B5104A52E12D955A93B8FDEAA46EA1270C5E6
Malicious:	false
Preview:	..A....fu.-..|(....V....h.$.B... ....N.k..7...-.BT../>..:..j<...GV........,hH...5.\..........03.@g.K....qrl...u..^62....<e....%Q.@.w..O..]H...;LLV..Dn.8.....<.\|......>...`Xaz?.A..B..sC<.d=....7.......n:8..%`.....Ed...o...{...._9.. n\.#..%.b.a.......D..~....p}_"...Bz.I...#..xd..`../!.\.4Us.=..%.q..k..Yx...`J^........H......a.d%^.s..vR[..Ah.s..vD'.4)h_I..x.C.-.3S.{..w.7.dN7.Fa....i.io.g....n.5[*N....P....;....e...o..0.sC~P...4c4.;9.M.....\]rP`. <..)...:...... &..Z*...3j...4..iX..4...k...O...P..(........,...N..g6f..#<..r........x`jR...I.&].KX.....Ted9....M>..%.j...X@..&.G..V.2.g.x..E..2...(...4!D....W...v..h.>....p........D..y. .Q...4c).y.J.P....lf..lp5..g..=..h)o.. ...J}l.k;D..-x.3s ..=.<..#.~.. w..Yow.M ...h...........RG...n[J.2t`..X:..`Y...*.p.C.G._.&WOj..!B.}s`..%.o.O.e5B...X..s.9[..h.c..\|T;iv..}O$......d...!.CQ..S..J!.....O+b.....r.%.1g*.b7....>n.....r@..#o...tBp....F^<......?.........DQ%P.....U...."..V{.%... #Q&.a.X..CG...s.ZT...]..2d...R..1...

File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.855801281823326
Encrypted:	false
SSDEEP:	24:jFdxxDWeBtk7aoYWeV2RYbxvOmVLv6sikg4MFRicD7fhjzM/88s30QZKuutrT/:Jdxxw7gZV2RYbZB3Rg4zWpjYuhWj
MD5:	79546B9435121AE6BDEDEB98F1C4A476
SHA1:	5512D5362997438D44D691BBC297F1D351E679DA
SHA-256:	E4D7E95611ECA02F775828F5DBEB5184685D8B0BE07F826652A72642797257D9
SHA-512:	50F1F0FB2F81278B3C08E68D740F31172A34A25C2347B6C24AFDB23F7D91B72B9306FB61F9485F8F4CEB1227D43D9A5C36742238E7342C8DE05AD4DF25B04D0B
Malicious:	false
Preview:	....F.Py...5...k..X5.I....."..o..0...<...........-......s..,2.....]#.2[.N..........X...J.../R.Hj#.k...>.^..v..y.XR.G!...|..]..>...$.K.#.imn.a...JW"...w(..M..F.+.a...&......f8'.w...0...u.......o..z..T.8...pQ.&......q....IQ..<U`Z9...g.z...3.. ;.).?.Z8.\`B..<S...M.tHl.n..}..d..3..S.-PG}.[...N.][..1.xI.O8.(."h..\|......M6#...KR^.g.im8.)..,&...E.......x..\6.S....o....1..[U.U!,8........B...@......2D..L..z..N.PO...3.X.f.....T~S.`...{Z3Pp.`X.r[]...&.h\...3..@.J.cq..)-..TK=... [C.rO.....&..cf...F.s...`....fF.*C1....S...h.H..x.".I..#..'3...$....4...!..~.U..L..W.E..ZCdz..k..hJq...M.Qq..k...t?...T..cl.........../...."....0...~.,6-....:..79...Z.J{...<R4..`.Af@...(^.".B.s.e.J.k.]E..w<.:A:.B.q.....g...~.&.&.-.......y.. ....t.i`Q0.f..,.<S./.5.........}rgj.b.vs.1.O....A.&. `..=..NW3=c}.k...~.X..$....i>..Y2.. .>-.!_..].i. .PtI.d&o......oE....nZ...+.n.....u..7.oZ...K...W....Z].<K...mym$..GP......s..Gi.......h.M.y.#.M...~.>..cO}.*..7\\|q>2.7..... .j ....A..;d4..W..fQ...

C:\Users\user\Documents\GNLQNHOLWB\WDBWCPEFJW.mp3

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8538433910730685
Encrypted:	false
SSDEEP:	24:E7Fr8qkrxkRZM49laVR5uqpbWicNjM/zo0cQ9Yof9vAVWoOraTZZq8iuutr0l:KFgqhZM49R99laM/M0f3YWBOIlLf
MD5:	E8E5F469E0E7CD4927D95ED288A3C1F4
SHA1:	3DA0B8BED5FAE5B424242BA01365777432D70A7A
SHA-256:	61CA291EC3D5FAD3435235A1E560687B66008659D982CC4E4A15F022B1F587A0
SHA-512:	F75F385FA39A5A2EA74CA2ECB2ABDC14CFB05ADF2DE52B711D9F2ED6AD1C14378A7AE5BAEB73EE7B1177D59DF86A572D5A2DB94D89B9E55E288CD6BB0618403A
Malicious:	false
Preview:	^.V...(.F.........(.....u0....^..8....mv...\../.a..*....u....x.AC...]....d..w).Jc..0.p...{|q.0......r...[...v.{.6l,S.$T.[0.*l......s.R.QP.1.W.....F.'....\.?p^..L.y.ei.i.p.....jl...e/.=..q.m.z.H.C...QP_.8h..5\|.c;...sq.v.K%;~..#....l.cl..ut..`\......I. H:;..4`.Q.....w=NL...K1#.=.....LG.K[!.nV.....>...1......n,....a.....,...ws..j..(..z....l..i......."m..0.UA.t..O..Yr...o.p@ .Z..wn.B...@5.Ze.q. W.Fx..*i...K...e...g&k.+#l<.A.....A....r..Ab.../..VM.2LO.J..FM+...........q...S...6.y.! ....k`..}...p..8...7.....U3.3\|.w.c.@l..~.".B......\|...U..._....C..$...^S..Y]..ou....+.:.I...7..yi.......}.].X.\...b.X..$\|..b....M1.(.}z.......,....75..eDe...V..Fj.4..8....G..C.....>..*?9.........../.2,.aZf/..b..6YPP".LX.6.O.....bX...%+g.G *...-.._.#....F%.....M.L!.k....^Q.ec...a^7...\..-...S....<..;..%3F<z..Zl.. 5.......E9p.....C..n..`.[.x..M......g.by~%...ks.n....e.f:f.c.9xv......6.&......:L....!F.$ .n...X..Xk6...8.I.'Zy......u.k...Y8O.c.f..n..4q..L.o..sn..].C....0r

C:\Users\user\Documents\GNLQNHOLWB\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Documents\IZMFBFKMEB.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.833152781595371
Encrypted:	false
SSDEEP:	24:z88HhZDKCTMMVmqaE9cUPzXo+eiUvHOdhHn6uutrlZ9bgn:o8HfuQFJzPzbeZWdhglZKn
MD5:	D18CB31EF336523EB59DB9EE003D94A0
SHA1:	130CD33FB05239105D9DE05603C4387097BB78DB
SHA-256:	F3E0CC75B7245401AD641CEE731D21CF6ACD76743270D5C6C4546BD3A424E398
SHA-512:	0E39E64EF81CE5758398D49ECF21F8B7AD7922793E3AC5CC307C8B1C0018BCE85764A76BF3E50ABF510B61558EFBBC544899B28AD3C7980978B292F7D63BC481
Malicious:	false
Preview:	G....8...L..s..+..!....0...Qu...Q.?..8-..mqN.4.....I|.1..[...U..k...d...S..0...(i..)...0.. ..X.p4?5...._+..u.'X"...l4.........Y..0VO.>.S/Yr.I.y~."..'v(...I./........]..3..?..%i.....y"....x6q.6.P........./h.....nX....q...T........;..).6.+.i..n}.....D ....>I..q..%.....[.hdlk....Gr.:....uS.{Z...[)..2.%I....8....H.u.q..4.Hl. t 4.D.......M...mg^.K..R..%Y..%.[...^...w.._.....a.B.O*`..c..Dw5.w..+;..BB...2r. 0e~.."m6..pz.....@.L..iM.X...F....B.&'.oy.$..C[/.4..K..O...\.:.d.i5c..X .e...T.K....:..".1.\.!~.hi.....p...+.9bp...L$...c.R..O.O....}}".%..m...7.90.c.0{...*.Ymf.."......5...Y.'....t....g=<....I.MFq ...#.'....Iv........UM...wQ..Y..".>.S...h.....#.4vh...\"..~...i.5v...........u..t..Y..E_..j.o...C..........v..%.pt..7 ....b...|.J...s...[sB.d...R.G.[.&...(q...P.>P.. .....n.G).-l.1.A.s.....}....=.'.sp]v.4e.<.....T.]..T...HU......e........F.........N.<.. .B.>.(.G..#.(..H.L.>.Y...B[Y.#.%..V..y.}G.r...!i.p..<]'.XU...\'..I...Tr..!./i.A

C:\Users\user\Documents\IZMFBFKMEB\BUFZSQPCOH.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.820947881086198
Encrypted:	false
SSDEEP:	24:LOe4qGmZtCB9yCKUYo7HqPBfC7QIQH/ZqTeDUynJGDFEKuutrdN4Z:LQUtjCKUYdPJCQHBmEUynJ4Ffdi
MD5:	B7035C598A53CC20F8895DC5E34BA7EE
SHA1:	75EC65DD7A302DFBEEF97E8D5C692336C2EE0454
SHA-256:	BD5ECB172FD4DE86C85E2CA8D548DA90E7E5ABD4F5BBDDFDD12E1FDCDDF382EB
SHA-512:	3618640AC0FE6D270236C1689223C9B8D33ADBD30199F4C22D76E9CC6E4E4C27288913B8FE94722506F305516B6D524F8EE8A592B4AFC41D8608806D3934108E
Malicious:	false
Preview:	.,^O..y.N=..K. ..J...{.......^v4.&...U.O.9..J...=.`..~~.&#.Q...P....H...Z5.@8..S.F.$..`.....C%....+p....,...V..zDB+.9..2.5Evr.^..m..f..%%.....q..,n..v.Q61...I...F2J.X.....0..K.9....?......5....V...-.....T.....p..9.=H......X.%8C..]. xzu....gW6XV$.y..f.......9.....eDr..G..>&.0.4..6Nxw:.jL,..Ji.7....S.\.v....8..m..Q.~.....j.b.V.{-..E.[oS..mkn....X.@;.../.J.O....Y.W/..Ou.0...V.."......^..R..&...........W#<O.8bJ?..t.,.k.._.m.jM..7..6?*.E.c.).:.m.........%a.r.It=

C:\Users\user\Documents\IZMFBFKMEB\BWDRWEEARI.pdf

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.828001580059938
Encrypted:	false
SSDEEP:	24:1ikkbdWFcsz5Wz3xcHs3yWDJqsz8ETDE9zLVmrsD5h9KuutrBY:IYWGU4z3xhVA0NTiXuU5hKW
MD5:	455DD160BC906BFC57091CCC45CFACF7
SHA1:	FBE384DE433752E2E3D5702CE9204F3C49228EF3
SHA-256:	B95FF6200DAB8F50E8BF3777556C23BA2D5CF3FCB5BE0075EF02FD73CDF99A84
SHA-512:	490042563AF527FCCBC25DC73CF5E83861979A037954EDA4856FCE65F362398B87E78C2F7C6D4EF465FFDE5C5157800A20DEE36D08DD395E21C2B77A7B9B5DD2
Malicious:	false
Preview:	..}:6.j.........%...FB.E"..E..A......Ew......D.....x........9I/.i..N!3.`........px...6.1..pkR<..../..j...n^.B^ R,x._..e3@...GH..k.tqRF,.......i..CP...4..S.....a....._0.O@.*.LL.R.....s.\1wz^..f.xk.4..N...'.9.Fn.?...c.#@..X...=.F1= ...../op.HD8.v~..2h&........e..&.[...Z..m=!....(..).u..I|.cWT..r....[$ .B.@.8.>L..... ..c......W..b..R,G....D....R..vb7.4W.. .[..~y#t.p.....$....._..G6.5B4.g.(.D.f.......a.%.wg.}.!.v.og.b_.d\|.pu.N.~.m.....%..t..{..D1....S...9..... .Ss..ZQ.].C........t7'i..WO.4"6.h.C.M..g.......s..vn...$..Q.;,.J.d.._...[.>p.p.......3..*../..\.D.....y.[.JIH.K[...d.......7ym.-IJU_.i..6xLv..u....a..Qa[.q.....'..s....K..[.......=w.......2.I.J..J?......y..e...+}.P.....&.A.F!KGh......^.FX. .....X.cl.....@..rh.{..{'.dp...La>..t.....x{d.W....VF-...34...xx..S.0......2.9.G3c...."..G....}...mX.B.c..:.x..^.....C....Ap....f.._....3.V.....K._.dXs.7...>...*...N...w..'9.~...XKK..K.......b..n...'..BG#...j]..P.=.inu..J9W....u...M.u.(..Y. {R

C:\Users\user\Documents\IZMFBFKMEB\FAAGWHBVUU.mp3

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.843784279168074
Encrypted:	false
SSDEEP:	24:xweGCKfUToKpOG2sXTul+u15t4rD6wWR7NYrdBCO0vuutrJ5:CeCefHm0rD/8iHCO0JJ5
MD5:	CB5DF2BDEA381E79C6441939242D1F63
SHA1:	4107C291C60B756FD9FCBD3FCD50575C6C058114
SHA-256:	8BB57937FF16009F0F9F2082E890EDDD86B616DD6D9007FFE0DFD34AFF79C8FC
SHA-512:	ACD8E93CD21F69687E4E38D54F6D62B8B9556D1517A56DBFF4EF45A37B8302F4CC516C5AD276BD3E7383FB738D6F19498356A4A35A16F15D97F1DD14C6BE0023
Malicious:	false
Preview:	..e.{..3]l........_..(..q.\...h4a......L..p_...i#..#.W.q..w.i4n.Q..A.#........O.B@LQ_m>....D.N.6.3.PwU..ZE..v. .C..Z.&^/....(16by....]..=..~....A ..!F_.%0.E.Z..mc@.....:u....Q.$.b(G...T......e....v...wA...fq.....E.....zqN........ ....X.;..cD...z.A....Z.\..6...}....r Q.@nrE..l.vJ./1l....J..P.....u....l+.t.D.RQl.......^ ...Mq.4.X.sO.._..9.s*<kjC,sk>@...8...]:._.6_...Yxe.%9te.i.P.l(..y."*.N.H.:....(R>..%1...C.m.~n.o.zAD...d.l.....Y..^_..z.L.......G...O+...4-M ....f......R.k.4Uwx....\n..3m....7.AQ..U..v..e......f..TX.wm\|.1.K'z.v4....^+..u={t...N2.]..m....$Wk.".R........#?^+..{..r!.....{O..O.s.Z...J...^:..!..|.mp..p..}D;.tH....-3.L._...-;Fc..wv...0/w..u....-.J.......<.e~'hA.1.G.....z.I.9.9..:. f....v...~fH.N..s@J...~'n..r.g...4}.6P....\t..J{.E......."C....$.8..(.t.7....m.<E.QD...LJ..N....'...o..o.-.. ....A*..s./hz.....B..^.E.jHV...........Kxb4go..".z\...b@.qn...)....?.]V2...\.......*....;.y;@5Z..68..~..#v._o#....0.....Rx...". ....5r5 N...

C:\Users\user\Documents\IZMFBFKMEB\GNLQNHOLWB.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.836762099659229
Encrypted:	false
SSDEEP:	24:O0FiRUnUcMKf1hRcmPDlFJ8UZNKk6jbYOz/YINPB8lfPoO3LQ8Ru5uutr5lpY:dd3hRcChTdZ36jbYIlFB8lfPowLQUu/z
MD5:	B9E61A3B6B3381B3036C60921326B9DA
SHA1:	E352A00FB044203036529E36CC5B8CD4FEA131C3
SHA-256:	61011E2E131FA72FC65DD4031EA9B191C7C64722CEB7E7A37E973C66A85547F8
SHA-512:	0DD7ADE7B90C41F53494491947BDDEDB1457C4D01E30ABD49B3EC6901494980A0A9EEFA91352E886476B1E922F21973C2FF7CE22EBF12B54EFA01E03C68A968B
Malicious:	false
Preview:	U.V#Y:...'....1...7.i.......j......g.......G.CVI.#...|.......j....*}. 1...z.7J.||!.Z....9...ss.nR......+.3e!$.2&+.@2p....V_.d:...._*..#X.....Ot.....%.|R~.......fM.e&..v.m.. i.!..PF...D....^2..M)........zw...wa.......6.I.........a....T.7^.X. ...h:.wz0.e...._..Z...P.....b..I..4....g/-....f...g..UC].T..vG~.&@..k......F..zH.x.]...P.{.o.v..M>.8.k.,=..HEY..>.E....b. ...G..=;?.}.G~......-..o.]...(.._p.3T@TQ.:.Zj...e..9..T.S...[......(..qB...q7......}R.1z.. ....D...8I.M)...E....=.. }..Fq.<R.^.D.Se..3..e.[. AS.>P....V....?...,.Z...I...C..;j....@!C..~(g.....m4.>>L.f.0.n.(.)mm..%.#S-.:.?;S[G./....Jk..G'Z...Ah,.V .7...XD.@..2.sI..-..$0...b..T&..r....=#=.e.......wU..q..,.8..pm...D.{._......h._.........?...9.I.. .-.....).H.*..R#.0...e..2....4....r.9..X/x,C. .Pw<gm...xM.._I.......&.......V. Q%d..`.:,..!......./.+....m.4...........h.^j|!.m....48.s..*.....6B.......sa8.....i..]...F.K...1.yn.....ZQ6..P.....G...i8...?.....,...k....- ..|....z^*@..1..\.

C:\Users\user\Documents\IZMFBFKMEB\IZMFBFKMEB.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.828000339745627
Encrypted:	false
SSDEEP:	24:IAKJYi2SX2gHe43d5FgD+Ls7Pp2OWg+KLgpxSZiRBZuutrignMWa:IT0SX28e4Vf4WgbqxSZiRlja
MD5:	2FD650384FD7E4F03869255AEFF726A1
SHA1:	AFFE26505B303058EA82935C2596727A3606CFE2
SHA-256:	794D4EFA782F05B5AA33B8E15B1F0DB83CB1C03691CF13F06C3DF5B587C03CD8
SHA-512:	E952CE03A8B3C09F5CB252401395D497EF0EA51C237C80D9C4D1D978F325A53B94502A8C87A4E37B13DFBBC5A1D1123FA8329BF0B0B6A1EC6AD04923EEF316FC
Malicious:	false
Preview:	'...J..iUk..F...;..5.. \Q....@.,.k.Q...q........Q7!J..E.=w..M. ..F.Y....`.B.KmS.}..V...o...Jms.M..*PA.`. ......Q*.....tt.....}...#._.~b..d.vA~..Gdh...c.[.M. $R.....Q+.4U.S.$.I..&.....R/87..x...(.....=.7.6...{.}.$&8F._.....X9..Q..N ..q.4... .p51....BV..W....3.k.&..[..e..&......&..!......y..t.o..L.._.F.b.5^."S&.;]{:k[2..(..B....:..o d..*.+c..S..6...1.U...].(3.i.B.+.-....j.k.5.....L.w.......j.kl...%...K.H..}.CD....t.!8...;.....b..q..8$......)C.5.......@%..Pm._/...#...... W..zU.*.6.......`....A.S"g}..!Uy....O.G..Jz..`c_.....&..r.\,...+...oo;Xl..T.?....2.Z0B..RN..1.a.......0...d.P...D..[.B>.z2.b..IL.4........+..I<.\...X....(&..R....,u.....|q&...Q.qz.TV.........P.g.w.......>].7..m6....t..F... ....J&...W.'#H|. .....b.ab....e.\r.'$..W.U...?..8.....1..:..)9.}K.*..S.y...$... X.T'....+..:.-Z..;zo.+W..P.:.,./..%[.3.P6./Z.G..sc..Zw.6..S..9..Jrj.;...%.v.4.........?...M..v.e.Mj..........4..>A.."..I.I..|4...-....CVw.E*.nM..0H........DL/).=...s>I.2.0

C:\Users\user\Documents\IZMFBFKMEB\UBVUNTSCZJ.png

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.817160685546267
Encrypted:	false
SSDEEP:	24:pX4HEmUPyxQJQXjqYK+LljBjrYSVZzyZJ0HNg/0cqQuuutrbc:pX4VPxQuXju6h0C1yZJ0tncvUbc
MD5:	6B2D18372A9EB4C24A871B1E02712090
SHA1:	5653BC9B1F5C77AA82B678C96A40142FF62F8012
SHA-256:	94BE0C714247A92F5E5A4AB60AE193CCD70FB6D6F5C38AE3240A6AB1508591DF
SHA-512:	68D5A0862BCC8A4D82453CD0E5AC0EED2F21FC9B116B741C5E263A69ACEC1B838F7353AA9E3CA41662FAED268684F24C457BD7AD96F647EA6DE05BEAB9365813

```
.l..Dt..E.1s.l...RQ...].Si...U:&N...?.Is.......,._..ih.....V......GJq.h..?)..,..v.....L.n./D.s..._)<k.W'. ..x.J..&..V.\...7..N..d)q.......5...c.Z.Z....s.U>.W.:0.F&jvRV...;...7S....j.i...{.y1.... .N..N....}.Zk7.1...p. o.G.c.>XF...q.R.gE....
...0Sj^eM..s8Al....7.!..lk....&.R..v..`.$.N...3.}.l..}..J..d.%P.U.....E6.Rw:l.........[@8:O.j..T_6..w/.o..Rj`.@..D..l...8SGE,.j....w.....O+.n.#....D......RZ.rfW...R....!kQY..{.....?..dP.Q..5Q\;..WK..rz..7.....:.2.u.O.B|R.=..o.....
x..L...fd...r....).R2.Km..`.;G..Vesl.k..jVn........T.r...lg.....<X.M...UN.Fm .T.....n..K.....-....A.N....m......O.........Q..7.dl/.]lo8.E.5.[....s.y.8...,N*.J.@.....TD#8..C".>b...}.k!.K..P......V.qd.%....r.f\..1_....1..:x.4.1...9l
```

C:\Users\user\Documents\IZMFBFKMEB\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Documents\KBIFTJWHNZ.mp3 Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.845531215760393
Encrypted:	false
SSDEEP:	24:Nazt68hoem8HPgT6e6mNY9SmWhO1tAZGirkBMKuutrK9bn:oZoeHPa6exNY9SBhO16GirkBX4bn
MD5:	12EC7097DA9D799CD6031A37D1BBD6C0
SHA1:	FDD2D86C5A6F0ED03AD9E93D8E78206C325AF909
SHA-256:	3526D740CCB6469AA4F9530212191DB2C47E249EE1D61C8E7411CFA30F2BAF65
SHA-512:	5168CDAB7A190727BA3D30FA2203F51506603F98B761FA5F4FF44982BD63EB66AA7A97050B4FD174E1F1E2619C88DA4B811D9ADC1DC22BE458E38AF4347CE86A
Malicious:	false
Preview:	r..h..L$.x..R..U.a..}+...*r(E.q.....bO....E@......)3.!<..l..}..i.......H..s......H2.T...K..r...lTk}.JB..7.....3......].6zF..\..!..{Z.O.3Wy.pY.g.....PF.&....%.7..=.:.2.............R.E...}^;@..Wx.i&]..I.(..W.WA.MF.?....}...>m8c.R.. .sq6Q%...c.4..le4.*j..tt..GM..M....R......8.[..k.M.K=....K.Xe....;V..-....q....W..<....%....bh.$...D..j......?=U..a..h..W..Sr.......W-..h.t..=..:.8&tH.....4Nd.+...c..oJTKpR8..C....z.&Sl..H6[=..g/A&.zT_|.C..N.....OQ..l... ...6.J...;.V.~..@..O.'..+%.~.p.m5wF.,..8e7........%L"@?n+.6..)y.o.(9-p.B..6Br._..mf..5c..UH...........hX.J.V.#..l.....;'.F...Vm....pf.E.....,"O.S..L/c.u{...U.W...R.z.E...o...T..-.R........2R.....3X...)......\...P.3j..1..8H..k~.&.. ..A..V..p........n.8....S.Jf.e.q.....0]..n=......>2.u.D...?&ZWk.ql.t...B...:.?.!.C.e6. ..t.k.g[..w.9j1m=.~..1lhlL.t...vP..=..blN>.....>E.e>..d.Q&'... .....T.XEv.]..e..7T..Bu%...../Q.-..w.Lc.=....o.b..p.A..N....*.p..^...FB.i.%MO... U5.$....Z.GU^2m...l..]X..p.A.#..D..

C:\Users\user\Documents\KBIFTJWHNZ\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Documents\OVWVIANZH.pdf Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8487928610237665
Encrypted:	false
SSDEEP:	24:TPpwoCYNAtb+ARSJHuRFXxIl20hGjFBOFReAHHVsLwo3uutrs/G:TxwttKLJHgflehoBO6A2wQF
MD5:	07716FCF2FCE3B996CA6525958E35DD5
SHA1:	F19E1F9C248A04617360FF28C84D67C8B919B4B4
SHA-256:	BE0838D8C25541F57FEE31FFB0E0DE78625D537AE41F25E75E3CDB1ED795F26A
SHA-512:	3F597DE2611AD4686779F164351BFDB70DE3E7A41E1AAE7B68BA5C904B26086DC7329429D12FF4817CF4733FDB4C21195BE644ED2A7E9C084F57D9D4A0C403CD
Malicious:	false
Preview:	,..K..........s..[....3`c.{#2.K.rY..E`).m..y..JrbE..Mr..BTo.&8B<DN..e.....b.i$vK.-.........2w._P....b..'..8H_.BQds=".....WWD..[o.... ...8QvR..4..F.J.B.....1v7.u.8-=)..W8.... .u..&......\..`.^.z.....j.....E].c..'.+.&1.48.B.WO.lm.A O!._..d>Z.d.G.(.@..).xS..:T..f..\`..A. .KS.3.....?...].\9..=1...l.!$..:_.3....?.V.....w....U.1.$.-....y....F...../..8<...q.fv...9... .5,...W....H;.<.l.).j!.NO..(..-..O...O.R.r-..E.]...........~@...w..U...SG..NnoG6.....i..?....#o...$..o.Hdbu .W.A..*...+.9...:..Hxld....Z..=.......pC.R..A3'..#.....i..%.B....,.H...@x....-.}.......F.G...|fN..%.zl..z....7..8w..B.xn.U....m<Mv=..^..^.GQ..n...\^.A....V.j...Z_.4..|...m(>N.....0..o4#..'7=..'}.......?...D......{f...}...u...9.iq< @..%.>..@]..qJ.....A.?..l<...W.6L.[..!....2_k..\...........]......T.p.c.-.w..-..C......1.(..oS.i.b$4,N}R.8S..}...L^..G.q........9*t0.qt...Hk...P~.p.P*zf#e.....Kzb..o.Ph..+.5...Z...Mc.}.8[.t...(A.bdS'....^...3...b.H.C.Y.P...G.Ce@`. ...../......4

C:\Users\user\Documents\UBVUNTSCZJ.png Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.835493668987136
Encrypted:	false
SSDEEP:	24:SR89p5VCUJLzCaUsktwEMEGlgGnzz5B34tFivKSqOb2iEhlB6QdqJAVViZuutrl3:SGKXGl/zf3EArYxdqJmifl3
MD5:	AA860460588A6B1594DC4A1B8A4D66FF

SHA-512:	298171A6A080CECAD8E6DEA4B2A321E0E0C60B6E149AB7833EE1FD5ADCBD2897908C28B0E51D4548A81E63B8A39F12AF7554A324F9866B864E3972F9BDCF96C5
Malicious:	false

Preview:

```
.\.f..Z.........#.........4j..3ok.........Z..@(J6d....%g.|.....nh..,.|.r...>H...$....Q\...E.T...W.$g......q...[.O..jE>........Dzg=.{....@..H.9....$.....A.m....:.g~...,.K..\2.Dpl......D..E(..;.0.....FE..r$.Kg...?T.X.S..#+.F..4].!.`.y.+yfR..
..V.T.....>..J.t..Q^...qY.+"A.X'......^.w..............:..m;g.*|.-...:..`s..1.-T....3)...P...}a...1*X:K..Rj.z...$.9./.u...tV2.GK.O.!....e0_....=...GW.0.2....%J...<...W`.~.}........@.LCv......t.2.r..-...cV7.=F,..@......A.F2....?.....|..p.
.....9....Q......M..^.%.}6o..a........?G{C2.....y.v..T...gW....L7l.......V1!:..H.).D.f....9K.m.e....-...0.W#.F~.7.A......{q.8;...J.....7<L>.5..Q:..T?!$..p.Tv%:...@k...e....K...!.9......~.[R.Rx2.!....j.\...K..t.w.Rj..F..w.....h..%.
l..X..Gl.X`..).r....VS....fU.g.w.oz..Ja...<P.....%)..l..6...n.........R.#......-...o...ng"...h.1....g..Q.iT.. .....&hz..].KcpU...H%.A.(a..........5.....'.DT.b..'\".VQ...P.~ 8.=aQ..#..!.y`........_...zp.0R.[..M.N4..gM.....:S.-...e3.=..p..9
...
```

C:\Users\user\Documents\WDBWCPEFJW.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.847842190267915
Encrypted:	false
SSDEEP:	24:NSMHDyozqnbS7XUVjk7yRo78wvZh3ELefJYsfF5hKuutrayN:B5zqnboWjpKQwASTf3yayN
MD5:	C34EADDDDC1B73B5FBAF79B7DCECC0FD
SHA1:	BD09D9BD63C7D38B24F24ABDE7758E168A33CAF9
SHA-256:	5AB3EF9E58C5562BDD47C45C255E7033AED564ADBABB7A567A9F8782AB8DEBBF
SHA-512:	3802F7D20CFF95F7F970C6104F25CC18553591E3E9143C991E6257C1475E439882EC75FBB0A88A7AD1794C2A952915B5995162CDA1536F61042B282019D00EA9
Malicious:	false

Preview:

```
.O.l.....F....DH....:.....FX:.}...xo6....#....?..e.p....FG}D...t...L.?.Sx.x].l..utc...h......G...&P.~.D..F.j..la.t.*.s.G3b./.?,...-. D{,W...*..?Y...?JR.U...y.7....V.3P.B.h.g.b...1.y<....@....2$l.5..S.F....'...zx.L.\..`F..}...X....n..S._m....
........>t..<.3G...TSu\ll:...M..+.d71....3GF7.`.f..@#&.uIVH.&:...|.j[N..v..`.u'.V?...5.....5...o.F....q......?......(.?..5.F.(y......Y....r..D.D...Ot..&.z.JF..D!.m.j..aU...x$.....8....v.gs.r..fU.Xp..^........B...jq....{\C.....B..".^ub...y.
YS!.P........2.....G..K1i..q...7..{.~..0..$|3.k..0.Q5H......w.Q.L...Ce8.:......_..XP. .../C.....g.].c..e.........Jep...+jr........" K\.3W...G.^....6..+...Q.....k.K..........z=....c.].{.WKK.Ve...J9.........|:.5....3M...EU.... ..*........>Z..
...y...3...B..Dk..N.B.7.WB.........a.(-.%.(......E.6*....L.G.FeC...h...|9!....c.......l..3.......8...+..JU...]........<..{Ye.b^@hu..?..`..!.9.......X.[.tP.s!..MD.2G..j..r.......=.)(..*po..@.e~.P......}...dU....)l.P...0.Q.!..b.b1g..Vz...lJ3....
```

C:\Users\user\Documents\WDBWCPEFJW.mp3

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.844595445655026
Encrypted:	false
SSDEEP:	24:g0yi+hYkHucKGBuiXbAIWMJhJdVaMX8zWJUJuH9uutrL/v:g01NcKGlabStJhJdVam8GL/v
MD5:	B1CF40E9F0452F974AFE03EDA747D3C6
SHA1:	F27507E4A6554E26D113B19547E92384AFE2B74B
SHA-256:	C4BEEAE77689848EB5A20CB46C03F46DC9FA9C58C8C433D819B885B349224EBB
SHA-512:	3581B3D1E777A7E6D417CEA33D21E380FED62090E8CD7983E168EECEFE908A381A431995FA2D7570AA528FC619F3535A0D01EB76C8AEF9797C8EF462CBDF4107
Malicious:	false

Preview:

```
..8x..*.m<h.4j................D.s../.`.*.c .P.MF..Z........C.._.(...,..t.!.i..l.D.....lT...._.A..E.O.5F.p..k.a:%433O.g..$.,.+}..n.s..s-c?...X.j....N.0^,%.*......*;...ri..c.)$....^..s.V19.To.x..>..r{....Z>.V.pl.).5.......y\.(..YG......BbQW.
$..W......?...F...|.O......KX...;..f...';...s.W..*CYn......O..L.q.].:qQ.=."6......(.....9..b./.....z......&.p....O......c.5uQ.m>wj.....-9...%}.].&c+a.|.......l. .tN..7.' .[R......a...C...E................K...%...o*.....t.u.."...Wq.......'0..`...t...
..5<.._....U...%_/9...i.).N."..Lq.$.. .S.^.. .(2...H..Q1.q....C5..H&%8.>.u.p..ed..K....+....U.,O..7.!x..r...h...m..g...s....t.D....u.e0......L...='...#...A.K..-.?.p..4.W..V/.."....S.d,/f{.z.>w)....eS.Hq\l.T^.i.M_sk,........BeJhD..
._.Kl..h...K&.H.aW...t].a.|z.....`.*t-..m.*L.3Fr...6......P.......^..}.....Y.m....c..m...}E0.....i....6.n.._....#1..-...,....W.1=.F...f.r.4....6s.%Eg.@M..l[qD..Kl.)8....2.._.@|gn.|d.A..........&.R......./tT..P..m.z? O.1..Ca.r........Q.
```

C:\Users\user\Documents\WDBWCPEFJW.pdf

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.86067886360151
Encrypted:	false
SSDEEP:	24:RFGsWwAEjsbMNr7fLnvuycQDW7w5vOscHiaqn7sQnyNyA0GxORuutr7j:R+EMMJwunQDW7wFOTfq7HyN/TOXv
MD5:	76EF52D731C5045E5FFB2C8C8E171B92
SHA1:	6D36B4317D50C84F2B26DB3AFAA98C7B99634FC6
SHA-256:	0FC8127F12F26BE762AC97F27924C4DBEFA7DDAF546FDCC2A16B75A9F0B6811B
SHA-512:	A9121DACB5D11C6BF7DFC30CAAE5FDED657AEB7ABA7C563C55F4F0EEC9EF252C0DBF3E6F45C0567388A1670A60F42E80982C5EB90005FABDE92E20AF1A9AB5D2
Malicious:	false

Preview:

```
.h=e .{....Dr...A&E..l..|..^.W..P..)..l...^.&..Q.[...|..nA.....?.....S.p.... _.G.?..s..ts..%...&.;..V....1....*.i.G..a.A. ..K..S.......@l.q.q9..nm0...%b22......n%.tN.1.4...ET]..u8...w..W.G>...N$.RN.G....1J..j.J[.<..w....?.7.xg...
r..qsb.`T.v.F....Si#....K.L..5f...}.k.*...2G!i..O...H..o.....^+.^|..r.lU*..\K5./c.n2.=.'.T.._E.....T....i!.....\.../.S.b."...0_...z.....et..uG.Qi..U.....N.......t.mE9;P..6T..J[.G.X.O.k.*f.).......,x..5 $|Q.,......}.9'..E.^.1.p1,..R..{...>1...
Y.....&......u..w..Y....y.....xK...@uo.Rs.....h%.#..wb\....q..6...3..J..@..^.)a.WD..4....^.!W()*E..s>.....A<..'t..[^.".2#..n7<G.E. .1....Y.M...d.@;..8.jc.{.UjP..q...V....j..b.b..=.]...lD.{; ..0b..v..)P<.\.(o.}.A..M....>.34..E.Y..t
.haY...5f\s. Fg..}R....]...."1...D2.C!....\..l...l....\...+.0*Bs.+.hF&.9..t...F.....@.[..8.....C,.......4|\..&.C.z.^*.x.@`\_._.....@.w.$.q..../.. G..Y....0..........}....j.F..V-.\?.~~....Re.........KF.j.qr.M..<.9...F..]..c.....5.#.d...]>2(i.(o?.
```

C:\Users\user\Documents\WHZAGPPPLA\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false

Preview:

```
-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .
i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o.
.f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e.
.a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.
```

C:\Users\user\Documents\ZUYYDJDFVF\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false

SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false

Preview:

```
-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .
i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o.
.f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e.
.a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.
```

C:\Users\user\Documents\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false

Preview:

```
-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .
i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o.
.f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e.
.a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.
```

C:\Users\user\Downloads\BUFZSQPCOH.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.832797741784629
Encrypted:	false
SSDEEP:	24:5LAGbxS+9K/B6rcpBnpz5/K+mLYyWtdUJVc+gbVa0zgLNCNeCJvrGauutruyNn:57bk4K/7pdlsDwB+g0sXNeorGguu
MD5:	1714F64C9608DC4664EFB14CE42E932D
SHA1:	A8252AF3D48F4D4C2B007CB836BD17F5DCFF4FAB
SHA-256:	E96139A67723485AB19FF4D6A58467D5866036D5DAB37C81A25EE157FFFC204E
SHA-512:	4CD262FE3F7974DEA26301957124A5E112BE3E5733E7F0B3322DE4985E5F7D13DFCBBAC28F7A1E7C17601E7EE227C697995A1AC3613D9CC2080028F4D8217F3A
Malicious:	false

Preview:

```
7R.cz.k.eU|.l@^..~T...R...}...6C.<...........(.....8@...#...j.dXd...GS..........E..(:o..4...G...,.....S.L.:.i.fb....../.b.m..S...{(b...bM.&...".#t..:.{..n...e.....8dc..\J.K".b<.V.Ew&..&^..S..,)...Y...9/.. ;.yS...>1....8Mc.z.....!i:....?o...
s..N.x.H...j..2...Z.!5.N.|....{..+..(.Q.tH0..nt.V6...m.h)...1.....O.....9..@.]}...[.U.@.m...8.....\.......I%...(T.pi...Dm.+....H..P#....v..MN$4.....=1....MN..Y.hw}w.....p..K..ic..Dgm..K.i.....u..6..<....0..0A)..Cl...5."V.......,..F
.....D.+.N...M.} l.L.;v..n}[a..2h..J....t...Uyr...q.h..b..]...i....w.m>`...=....%....r..):J.B{.E.y..$|H#..{.........hZ5...W..h.5.J..........H5.}....."............v%./..:.......T.o.....Z.......#G..oc'+X.....w)j{`0.\...Q....w2h..O..=.......k..dy:.....
.U......n...@.6.%.E!).o.p^.J.v.$t.W...}sS.......nM.5..e...([..#...........`..<.=H.....p;p.IW...Xz..5...R.[..n.{CX....F.D.......f...PKS.XO.Ul......!.P...6...}.%.......+.e...&...........~+.dU....+.Y.`....+...g...l..~&9..td\Q&i@...F
```

C:\Users\user\Downloads\BUFZSQPCOH.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.810584949720822
Encrypted:	false
SSDEEP:	24:rCy0TkZFqeTaav9Jp0ZTVHlJr+o7O+HZMB8Pg/xAzmMqZZj1Ft1/Onuutr6g0X:rCy0TkxWavJiVHlJr12B0OxAzqZ5zOhY
MD5:	9E40EFDE9256EF4D11F89ACA0D434061
SHA1:	35B141550075DBA717FB2DBDC8F8426C3835239A
SHA-256:	60DABFB1B583DB1E95E34868A6015E7ABA1488A07780E5DFC4D2D00BF72214A2
SHA-512:	5EF573C64238F756268DB0F12D6EA257BA773AD711BA3CF986A81F959DFA9C2069C91439622D555DEF68E28BC4E71B9D96A446AF1A3385AEBF05D84D69A7D854
Malicious:	false

Preview:

```
..g.*]A.....R.F.....A1a.....j&..,-.5..j.l_...S.*..2;../IQ1{...~...%..[...E2h.p..K.\v....z.....|g?.Z.^...}........E`.&&.. u..5*..b.b.2..O/.. w...j>.y%.9..k.S.[,..&.#B:a...c.%..2..r...c#..d...GpZ.t..:..cpi..j........<h0.D....qX..fX.g}M.e.u.x.
.......(%.$u.G..E....N.xG.&a.......E.7.5s..4...B..+.....<..|6!...Y".n.......=..W....S<[b..:..$.T).v...g...C...h....cy.Ovsq..W/.......6,...g.....b.8...._..>..p %$.,..W.B}b......k......n..KOG.B:aq.'.."5.N.......X.j...@R5.p...h.)P.".
..4.i.up.u.H..n-.w...=2{.f..../..bL....u+...uwp.N..x'|lb...2.4.R..wXsv..L^rt...{..v e.h.l..+&..p..*ylL.h..M.EA.0.x.#*u....l..p]...X,..HEw%$0->..a........yv.~......G.....L..G....R..V...Y...M<%....."...0..o>M6.....Mc.+ml.x.kB.o7.7k..
.+.C.<im.......}.*..8....."a...?.......s&....1...N.8j........E.....-.5z.js.p.q.e.._..yo.~.c........? . ..!.BWn..{MA.s.......b.. .)=......a...QrpB....JP.p....X-UM6.:..A......"......$Z..\4........?.uh@..y./u./....k2H]...]....okR...h.S.....9.T
4pC|...
```

C:\Users\user\Downloads\BWDRWEEARI.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.847363824613609
Encrypted:	false
SSDEEP:	24:dTMJiSAFlxqaTwCQQX9ZK+wLQNHKBFQMY/nTGkw8ksmzN4uutrGXFj:ppSAGxqaTwQZKzLYH6+3/TGlb0I
MD5:	EDE3371DA55EC199919EE44609BBB289
SHA1:	DD27EAD2316B5CC0AF0F0BE0018539E7E33912D4
SHA-256:	3441CB0D2600EEDBAC9533C391ED73160581743D7592C70E79B6F1FEC5443699
SHA-512:	14F47E2CA7972C3AFD9210F2C3802B2201E0579F3DA55ED6F61D2994036BD4CA9BDA9151C6430DD17A1394311B1ACDC2595761CB5D404371026E5646BADA023C
Malicious:	false

Preview:

```
.ba5.9....K.U.zhZ.YR.z..0....2..z...7...3..?.y....h.........K..-l.....h...>u.zk.@S.o..N.{?.F..r.&.%........'....Ezy.o9G.1r.2..8..St}%...2.a.....-.P.|...;F.G..U..G.=.;.^....KpZ"l..~....ng...u.;G].".X.y..[..>.U..A....L......vd.t. .
.b..2%o.i.)..H.....o.Hg.t.A....AB....._3.......?..H..m..^B....q.V#.T:...0e....j5....&.H:.G...H...%..F.sl[..F7..)gM,.'...K...C.2..l.|.i.fv....]q.l..z..N.4Yf#.O*i.c....Q....=..n +..~A...U5.)i...e-.....c...X..n.."{..O.G...$$h.)C...b...,...P.z
.A.xj...~.......h....-=.F.M..{j.....m.A..M...........^8C.?./t.|p...>ls.^&.S.*.J..F...l../P..0.B.._Z3....(,.D.7.X+..2j...J!...V-...w%....+S...{.=.q..~60.E..s)Nqa9.f..C#...dcL.ei.e:.* bgd.?H....C..Y..t..c=7.g.qi..i.]...8..]M.b......X...\l!}d
......'.i.M...LA......m...=T........&.zG@g'.<...z.S7.u|......l.MR..t&.s/!H.1.l:.5.NTR#.5.......L.g.'..iA....>..........aO.....C..($....9.)oF...r....(...R.'.S0@#Y..^Jy.M._$8...Q..,.d...x.#...V.K..y,..J.."hH<...,.e.-o6.....P....K\D..
H#s.f.W>.s...-t.
```

C:\Users\user\Downloads\BWDRWEEARI.pdf

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped

Encrypted:	false
SSDEEP:	24:z3MYLqCdn0tJeFglE+3DZlbN9vEkwGNlBnAwkcxjUzJhREt+pmyY7Kuutre3A:fqCd+E+3zRFEhkAYhdbQwuA
MD5:	68D72E3B5EFB7B6A491AE8DFB2F5735E
SHA1:	991AA45D4887FF8128A0967C38B0AC3B623F2AF7
SHA-256:	9717E6275BB7D3B2B8AFB407322F9192BBD09DDE12A927D3201EB5681BFFE936
SHA-512:	B673D3AD3D7D3D00EE3AC6850BE21EA0A6827C33F391FB55EA5A648119F55ADA60F15EEE8751F636AC7EBB1F7D624E5D12C146350E8C83628FE3517F3EE29CD9
Malicious:	false
Preview:	?4F.......q...1.t...GxC9.6..`.p..|8.|RT..|./.Q..*..jA....Y..[...:..#...@2~2..!D.8.#e...W.....!^M.MR...........Xl.5{......:fW.A.k.t.%..W.L<P....k.p.#....W(,.q..K.3.(.....cL..9.T..-......M^K..+..R..p..7.......:...p....Y.....[Ap.B.E# .~..g....B/...Kl.s.]h..Q..p...C.K..W..%..):..._.@2....A..b.F..4.9..u.H.w."<...s......b..x,.J..5<EKA.].c....3..K..4.v.u.&..n.A5a.7Ls.......+sk...5O.c.1.q...4..+..F....S&....~..6..F........El:.;5x.#t/...uQ.sG.2'.0..T..UX...g...u..A. v..\)..[.3..*.%t".Oe...?s......;X[$..@....`.YxoR."p.E..'a.Z...c....C.;8Ts~f.%w...N/l6mp.d. .w.Q/V/....>kp}.nJ..._$...Z.wDj.....%..Q.0+M#.8=.U0.VE}.`D.{..@.tY@S*.......d...]9.$5..0P...F`;&.<..j.2.%..);.KV4.......+Y...\|T2 .....R..<..R.Q...VK..?[...@%..i...y.........$.z....x.~3Qz....w.N....8....Y.%...iC....32...v..1.(9.Q.n_)6...%..3.K.V3'........>7....$....X.....b.h^(.U..W.N..]*/......Z`z.......B.k.1.....:.O..h&....%.iZ...h<...%K.G...%C#y........s..y.l.. [...l..,rhA].....y.bN7Om....8

C:\Users\user\Downloads\BWETZDQDIB.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.849812445858133
Encrypted:	false
SSDEEP:	24:rvA2ewxja5CKrurfwhyi5wQG7u2497lvPGHqBj8zCouutr/2v2P:r42xxjacKruDAw4/p1Bxq/w2P
MD5:	AF678D419481EE5D955C1D6274FF4BEB
SHA1:	854B562343AF7F3710D02B6302E49472C73B3809
SHA-256:	5BEA66DB4BE4793EF25A256F6ED93D01015F6E0AA0B355DB121AE45FB96E0F76
SHA-512:	742F06024FD6794126D96733B384A1001C932130E20454D1AC29B4B8C84B9CA7CDC9D9B63A5EFBA048EFF33F795D41AC7AF2B5CD9417699FBE7165FF3B929A83
Malicious:	false
Preview:	.....F...W].Z..T.....A2'.......@W...voV.M.>..,f%t3...j...rQ.k..G..:.K2X."..p+.z.GM.._....,y(w.X.*.9..`M....{...*..wt,.`.}..'...%..8R+.rmS^t.Q..&......$>.E.7..'9.......C...z.,"3 ...o$.gv.U.1/....m...a.1..Z.rK?...V..s3.R.....!..d.. ...7..T.Hg..d.......tl+oW.....R......L..!.Qw....-,....&.-.?..j.N..Y.y].F.|...v..Y...Bz..7..f.R..7.D2..b.<=...TiN../?...G.yu5.R.....e..4'..."....~].|.S...j.Y>.AX.+..#.A..t..@PMe.........=........P.0....s..I.E.^P.....!...B.:..*Y....`...I..CY E.......R...p....F[..;<.!..M..`....@.m-..|.}k..:...:....'....M...}ClK...d.#.....\Y-w.mk#}u.G.."o(....o....`.../....4Xz..Eiv...bq..z.W.G..g......`....@.w;.......m.a...{.,.*x....S{}...#(*.u.......f....$.r>..L.......Q%c.2........[.Ts..~. /..g". ....@l..q..?x..j.Oi0.9(.}......C..]Z~.\.'k..a.......r..V.$+...y.enl...c..^GhL.o.....yq..~...t.B.......l.7.gP...2..&..S.3,.M..#..W.K/...p2.J.pV......%...@.~VaU..y.b6....jxH;..@..).8..rN%...|.N/..|..K.CH..wND.|!.iZP

C:\Users\user\Downloads\ERWQDBYZVW.png

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.864462607746137
Encrypted:	false
SSDEEP:	24:39+QqT2pekI2s9Qa+M/WADpwBipXvGnljPbt2uutruu9I:38Qqi/IVB7/N2oXvls/9I
MD5:	AABEB19A57BDAEA637F139AB66478F22
SHA1:	EAEADC44351AC89103940015DD50D21A2F8583F7
SHA-256:	F5C919E985F3F192BE32AA68FB7B5C6DEDAA48D361D8742A6B245ADAF0494828
SHA-512:	1B5D827AE87D2502B61973FD6A0FFB41B89EFC52B963466D9C4560B13ABD192265A6736F265BFAE7D2059BC4EA5113D530778D517616F4613B39BBB1DFDC3A3F
Malicious:	false
Preview:	E.e..W?.%.B,=.,..v.....}.....~y....n.aY...;...sr........,.s...V...|6p.K.x.U.e..Z?..u.......*E..<...^..P..U..'Alp..:.E*1SVp...y5....<.r....Ng.h.r....)..1.C....'\....#......L.@.<f.....=..,^.........].....bLt....cilzor.., +u....|2c.p.H!....e...t.t...*.l ..;.U.Hs....*..j.......f..T....Z.D..... ....7?..~..>...1.{.~{..l.6.Q.._........fl..R@J..*7....1&..=.y..n_.V...+.Z!2..~.K.L.Zk..$)..suT...=R.A..XR].)..:lz....;o.nr.....p...t~..^..].3....ek\.T[..,....PSBEw..V\|...~1c....9c...x>..Y.._.2..C..v.5 \K.Y]DAb]..8`....Y.j....ML...q....*....$...q."..;...+...O>......|.s~o..*.@.]i..../.!.HC.CT.KD[..G.w.z.Q..8sP....Y.^~.:..S.....5g.[.......s1.......M..W.u..X....4...J.......3..A... ..o...O....D..C..n..<...t_.....lR.q...l8...4..H.H..a..l...fi<^ ...O.r..._.LF.Q..D.bKf9.`..K%...r..T.........0e.....c{.t."...Q....0. ..J....x..T.~..1l..|R.J..(y_...luB.`t.J....lS.Q5..d...l....q.....,%....Y.Z+.W.,:..?..[...#Oh.m,;..5,....ECUj.......z.}.J.3...Jg.}.&..=..:.../.?....

C:\Users\user\Downloads\EVCMENBQHP.png

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.827362162263186
Encrypted:	false
SSDEEP:	24:odwPC8LwmadLDN+8Yx/IR26TaQ/7CvH282VJnHcFouutrmG:oCakHw+8YK26TxzCvhAn8FqB
MD5:	0DFB3121F42CDFC6A1640201811A8A15
SHA1:	BE16159FE60221F68C9682673F1F7C38BDBA7A0A
SHA-256:	D673CFE0BB0E39DE90787BF694CC2F7AA78B9C38DA1D33324B4D7703445C3646
SHA-512:	F4229665776D490C379098FCDD784D0C5C19DAA9D6CC4B1585F3A0885572C38038E9C3AD14E986C484C582C0267759E884F1878BF6A3504F4785FED5C97D7382
Malicious:	false
Preview:	$.G..U..s..rFSJ..~..>..i.D"J.M..t.K.+.M#.....;7.z..D.[..?..C..L._V..%..<.v..n-..o...w4.WX..srg......0.*#_..N...<.L................{.].b..\..\...;.E.....M....o.Zq.7`....P'.3.i..4.[....RC.+F..@..s'.>...y1f..../..E_.B\.J.M...T....." .`LP...jno&9._B..6.P.....l.....W.....0?..d`...FBL.?..J..../{.....<{.(.`?Q..L..+..M3....V.f."......n.)$.Y. |..1.c.............#9..\.;...[3..&....n.XQQ.K.ZG.r.F97...F....~l....J.(; {~{J..c.g...\g.w..x..M..+.`..AN...J.......(..J...Q....T..&.. @pv...x.Y....6:...c!......u.d....d..._%.T....R:-A..'........}..._..)..&.`..9C..$...H.<.v......?..,<.."........v..w.....R.[....l-.K....7.2.w.Yz.-V..F.R...J.M`....feQr.k..M. P..x.j..J....mv.Y..R.kP.f.y..T..iRo.4<..L.....#F..`3..@jJ#=r....y.._.n ....aQv..e...%....K.l.6.0.f.\.Q.X=:x0h..}.E.jjxw....R....$...G...R.2.(0M%..Y...'.z.:.<......].vn.{:... .[..r.......N,..i.1....V'.a-NN. S...;...>.J.E...j..O).C0M.......N....+..d....B=K.T..,~.Yow..H.g.|JC.\n..p.=..U++..\.&...<.........WK.

C:\Users\user\Downloads\FAAGWHBVUU.mp3

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8259567853922976
Encrypted:	false
SSDEEP:	24:uxEdryNcbbD7aw1wz1AZluN34qybmXw+Bz37AQ+hJFuutrgv.uCdWcnaxzN4qi+w+BL7fiJLgv
MD5:	9DF435B4B7DA575C36419724537E2A2D
SHA1:	7A9CAB31C0AC3C75B77931EACE15B53AB09F8C29
SHA-256:	4D009706F59A0F3A120FBAB8522D908E09868D4B267032DB278D8C9242B86D86
SHA-512:	AF7375E2F82B76D37B16B3452129900BF32817C5FEAACEFE94677F9F7618DEB70BE1E7AB50327AEA1BAD6A950C9BA94E90B99E0E84D781C7ED64814714C12C38
Malicious:	false
Preview:	.d..C.....u*.q.f.S...L1O..d.......f.:..>:(X,....*'.#.~..-.7&."6....ib.h......mejAG..N/.Ca#...DQ..D..._v#<..:8iw...ds..Ah>}B|..~P...pn#.,-q....,..w....Y...z..g.h..1.S......O6..2....4.W-u.B.6Zw..{..#Z...()4..E.w)..j....X.FA....M.T.A... <...P5.D.K.`.>...=..Z.....b...rh...@...@...Z>.P{?K....X...g....z_%.&YH......._nm...!.....?...e.(.......h.o...2..Yq~.....H., ..Ds1U^L....b.3.\k.....w..S.QG.66...x..)k.?.y.x>.......X7.......+"..e.M...S..&......;iZ...a.^.1{.6..N.| .v3V...>.-9.~s.MK..d...X]=..bq>......$.23.".c... ;].....=x.V...^.ZF&a.:.0.."$....=O.(M.0~{........v....|T..P7L..,7..yT..rM}....3..J.......8.$.....D;8....M..B4/|......c...C..w..5PnM.B......m..l......1...........Nj..{....6.C...c ...O $.Q...2..&..7..-`.g8..9.X..Ab.l^Y..sF..1X..Q..M..p.e..<.l.az....u.b...M.7......M....5......UxO....1.opP..TH)&e...}.e..*9L7..?CK..P.5..o..Y....C.-#.].....<.Wx....s..8c.~.v...,.Ts.~.%l.K5.....q.p..z..5.S..WS.Bp*}..+.n?O....nu.. .jO....._..7<...5,. u.3...1....j.1C.lZb. ..\.`.x

C:\Users\user\Downloads\FAAGWHBVUU.pdf

Download File

Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.8457640103200275
Encrypted:	false
SSDEEP:	24:THdD6AATwlXK3r/R2Ohvi+0Q7FHCnljSbctuutr8zsi/:JuANx7/R2Oh6+Ti7W9i/
MD5:	9EE64EB32A5DBFF8A429190A03F657BF
SHA1:	14D6474E41016F06095A712AB92F2508A06D1429
SHA-256:	6C7CAED763F9A2C0329EAF2C5A19C0F05087B7B9CFF44F16766B50B44BF1F7C7
SHA-512:	9102D14E933148D375F702880FF96070633B9A59D1FB2E65F8296D717AB4EBEF399CD3A55B951139BCE364EB49F12BDDA0C793005567C75F8BE1D2C18F8E39E9
Malicious:	false
Preview:	EP.{.S..T.L.RR.7Wp..-...|>K..f..w...E.0f..l.....*....eE[........0Y......[.+..........b.x..}z:....7d..-.']sHcd.N('.1.a. zwJ..u..r..1u...'o..A.......?.&$.9.:..t...8TZG.uq..Ss$,|'a...T..m.97.,...w..j..X..>..cq.,.6i.x.7Yjw.o..P`...k.J...H.!..A. x..T..z..t{...D.R.p..../.4.t...r.r...26.*..v'.dPT....)..v....q..CQ.h....D...Q...2,8R..........c.........ll.i.......G.QQ/.e.9..._....:Y.z8G.......A.s.......:..6QH..@_8uE.FJ'.d5...f..........D....-B.yr.U.h.)......\........N.....`.f...&..H{.t.1..B/K.(.. .Q..1=dYP.....6D..Q...$.\|V..?.tt...B.[.........W.C....r.keKV0...P.f.d.o%mk.p.x.K..P0.7.[.......(O+..c.$%...F..c..7......m..FP..iN0.?u.....3...72e.....6l.[.9.....X..+N...0l.6..A.A..Mx...:w.......J...D^._.S.<b@fy..t..=r..2 M~gR.2..j .!...l......Ms`.0.....O.[.....{6U..l.......$.}.....5.......[..9.-.+..).R.$wHt...($5..s.........k....B.......[c.jb...}..%.V..?..M...S_.)3w...~.E..U.H..S.....'.3.....q....\..k[...O....<~/..0....|.=M...y....}T..=...e...?L....z:..TU.5R.

C:\Users\user\Downloads\FAAGWHBVUU.xlsx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.846699878327895
Encrypted:	false
SSDEEP:	24:DbdBF/lxh2NRTKvmuXFQDTF6fiKbrrCUC9FFaXsHulAnuutrH2:DbdBnxwNcvBFU4dbrrA9/I5lAW
MD5:	531D3B7E095AABAF67DEA707EDDD0EC5
SHA1:	79774DAE5198DF3B59808F4CF716CA4DCB7AA08D
SHA-256:	EAF744161A6DC38959A7F2ABB124063DCAADB0349357D23C735187BACFFB49F4
SHA-512:	094482679F3A5F325344F69F337A95B31C132CFDFD5DC7DE99993177D017D51B672BF2CB43B82BE1E96A3448E203C8F098BDF4C3FD54A927BAD56D586C50ABBB
Malicious:	false
Preview:	..Wn".=4........cb7q.4m.C.K..`...5|$........!.`;.....u....){(...m.Pj..@....Y...q.Z...U..bA..Y. .f..Kc..dM....4ZVN..S`.....>...8.Of.........>...........u..XZ1.0.......A....9J...Y..k......T*.X/....~j...`..J...o.....{......1.~N....uf........4...K}l.:- J...s..B....$.5/.........._.d....y.*K$l*..ca..;.... Q...)..,.......!...ji./....]&Y...Fk."Z.92..=....QR.G+<.(...B-B.5*.=.7..uz.kf..Jg#7G.9&`fx.[..v.........hD.1.C..L.&&YPc...f.d-.xP..5.C..pV....Pe.~{8.......g..>.>.......$..._p?.(... ..u.ue..'..)........X,E&...C.}.R...)<......:.<n......\lbt.B.[...g.......L....^.u...Q.t.Wn.....lX`(._%U.6.|"B.....,........e........g.mO..H:.....b|q.URl.w.$..p.:.;...g....g..*....o$.....L.k.h.,...L.. 2.J...O......X.X.L......fY.l..m.vx.jK... v.&.>.4TC..O.P6{.-..C...f....!.<.7..6j...........gD).V.Sbh..x...g+AK.&Q#s......... ./..l.=-...M...b9r....1.....4.....x....}da\.jH...E.q 1d4[..[nX9x:5.~..f_b..5n.\.%d.l;.;#/..[.q..).vR{.!.m....;8v 2........Opn.Y......T....K.t.%.

C:\Users\user\Downloads\FGAWOVZUJP.mp3

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.832703871923048
Encrypted:	false
SSDEEP:	24:lJCCBDfxNtUKlGkMT4lyX3QkpBooZ360wAXlLM9bNEuutrUl:lJ1DxNmKlGkQ4lyXgkpBfnVL8NGR
MD5:	5B99C707EE277391245920F1CCDB30D3
SHA1:	F53E3A2195F09A805BEB3B7E4ED60A7BC6E100F5
SHA-256:	7531EC1DD17B73B5722BB4BBC2A04B3F63EDE6DA0F9FF27F178764AD4EF7ED51
SHA-512:	0CA1F432FFB8572851FA68EB2ACF91CF704AE285BAA9A4FBAD0A2A0736A13F05CC91C66C0082CD10720D1250CC873094A10FBB5D45E84984B64D9A1058D1BB4F
Malicious:	false
Preview:	......L.n.H....v........~...G.4....y..p?.... .....i...qb 6.ip..z.|{..g.Y.M.'.CKKQ.V..G.n6F.c.#r..T+T.6{&.....W:..D#E..#.dE.....{...4...<k.....FYfv..W.t..........1X'...Q......Dgf...R._...)h.f..}]?4...,..xmzJ2.{...T.Q..d.E!.|....'....K.7..... .T.._$....b..uy.NB.C...}d..dzp..~N]..6.Sdr......x....N.....4....."M.(yl.].7....c%..#..[._Y..6..y.r..W..].M.....3. .+.E..kX..T\|.b.ags...k...S..@.<.}=..].U..q/...A....H$.D}>.../..Ud\..`.....PU<.9tv..Jn{.].........8JU...[.@,....i...% X....}..y..<....J\n.Ax..g.Gn8e....0g..U...IYOP.....+.....[.....:x..l.5..v..0.8.}12.D.g.9.'M.B.GWL....^.....Rw...PHz.}R..s....l....H<..YX.7.z]b.V/p...n......^b`...<....&...j...HO...=..o.......Y...H)...h)M.n^.G.9...XK.t.(>&.....,.p~ .z.....bn...N..D..._...(..Z.q...J.&.=....)...6[...........U7.'C..Q.j..mWE..*E.f....4....uF.u.,....5.i...#st..d.!k...{}K.G.Js6..@...!.F{...m..9K.7.fs..l...mVt}..6'.'MU......O..V.......l.......z........|.W.-.E8L..Y..>..Up. w..*(.-T\.....R/..l ..N..c.

C:\Users\user\Downloads\GJBHWQDROJ.png

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.836846399129623
Encrypted:	false
SSDEEP:	24:hg9g2aXP0F7+u7GLl/7Z/Q1LvUD0ZihL0+nVShnr3P6/3+mw40Zuutrt:lgBXPXBeLgGihL0h9b6/3+x40ft
MD5:	102491D2F3631817EA30386B1B9E6C45
SHA1:	26498CBCB0676BEF95213536B00FCEFA0D49CDC2
SHA-256:	D4702920CA7ACBCA49C16905831565E7F47CA925F7CC7E40C222D25AF2979654
SHA-512:	F865FCF83AAC14A800EFE66C1A6F2CF6CBB9FA95D14321953BE9875249D83CF3B88B931E544D6C25840D1614713A4CF37A44D57ABFC5576358B6FE18F54B74CF
Malicious:	false
Preview:	.|.S.7..6..e....&..<....B.....:...n.H*R.R....Z...;.}....,.K.....p?t..N...D..!..i...'.._?..j.3.....[.{;.....5..>Fo..W...Y.9U...p.8.jt`................h.g.Qe..BWZgU.....Hw.H*..h ....(+.c...........k..K./.....y........2$P..;=..m.........SyY..U i=..t.K....j...^......eo....m...]9J(..^5a.43(z.u.S...5......!........%.%.....l.i&5.~.2.-..D..`.q.it....p......o.=B^.;9.%...&7.N........'-..T..z+..r.....V\.`.W...'M....kL...........?.d.d?/...\.8.....=:E.T...[.P....h.a....++..EL....`.Sg..'.......\s..1.. ....P..i..$,Kq<..4.AV...._:l}..5.l...W.{V..N.t..!..ei....@.w......E..>^b..l.@..g....yt....nJ...._D.9.x..n. ...l.5....2.\.....p.B.b..'...D.....FT..<...SL.........S.}.yKb.N,..R.a+zK...$g.VVZE!.nW.lj\^l.X.Z....T..R..w/A.....5...cR .o.>.G.n..J..i....`....x........!+.....O-.........._.5J....J.5A..f<..Y..P?P..5...y......QWc.).b.....zg.;....N...*..P..?.c..cE....\|.g.....$,..8...../.....p.@..`.vR....w.M..m...}..*j..@..:.P..t*.`..p.......H4?.....H..+.....w..

C:\Users\user\Downloads\GNLQNHOLWB.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.852903831436511
Encrypted:	false
SSDEEP:	24:xiQjJQ5KG0fieTinbjEwpgTxN0OW/eqBVPlFU+SU65uutrjrmqy:gciUrftT23ATxN0OYprlFU+56/XU
MD5:	56F2EEF8B904E473555EF5BC35928BE0
SHA1:	E1B5A353252DC758DC48FC0B8E5F4925F87003A5
SHA-256:	28A48BD8D163EFB56F85B399A70B61D25926F7E330B4D9016E7F52ACFA4B7DCF
SHA-512:	884C50A34738EF13AB0CB10467D2D6026CDA68C81919CD3A70D4DEF063880B3C4455B247474F0E606EA60B30E060D9228CF10535398C56B9CDD37948EFF9DD59
Malicious:	false
Preview:	g....4..B.2.../....E...#3z.`.VG......C..u..c....p..~.._..~C,.g.$..........J.!.\|*.L..6.....{"...]...x.>8UxQu.f.V.i..&.TM..:}.....K(.q...e.....$d..Z9..k...@2p...R.`x......&..%..x[^ye2bk..|X.w.g+D?E..}....<../.2.Ew.>.%.9X..&.(D@..... .\...P..'i..F...`.8..|.<_.@..=v.p.........\w......c........Mx@.n"..o.m..r7.\Z...lAh.b0-Y...9..^-...F..".d..b....J>.:9d.f)...cm..e.b&...Bh.K...v.E_>......e..2..w.n.E...k..q....-:.6..1../H9......lK.........e8.J)S^.W.,.L..@.pc_+...f.q}.P'..K.. e0c.<......9...../.t.}...;..2|.....tq...\.?..rx..!.../s......d.S^G.....S4.u.._...t..r.;\....h..>m.....i.[.L.........S.|....X*#..p..^..6.2/..vT..O....]4#..l.3.u.1. h....DR.^..d#.e..A8.54[...{.f..8..hLS.G}.I..>L18.*..N.1Ab.2-.+.O.."..,...KX.E .1.Q>...k{.=......W..8..}Y...h~.Z..y.c....?w.........N...W7.Fv]7.)2...1...=....l...&.....i.z...g.l..C..]..;_..........d.`...u.*....?v .4...{.f...[.......qK.^^.>.'ppa...Db}:.>};...\&.~..K|..@P....=.j.D.x}.`..7n]5W.]........m.M].]Jea..

File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.841658870782017
Encrypted:	false
SSDEEP:	24:TZNk0PZPHxzhV6q4hCTGWyDRsR3KX7ESQorWoltEa9/s6pl53kuutrF36:TZNpBPZBuCzymR3q7F+ua9k6p28
MD5:	2F139820ED14BB9121F7A4EEC5F0452D
SHA1:	14FAC82BACD0BDEA45DFD8AC091A3B5E7C1133AC
SHA-256:	13813AF1F67E4B55E273FF68A6A34DADA041A175EEC484F3BE8E1846206A7990
SHA-512:	7FBF2CF3A66653A48168C53ED78BBC0A6739ED78FAF0A457B312C4191B9668FC272869F93452BF81949EDD85462368AF9EF1C60DFC5B9594000DA8BA83EFEA50
Malicious:	false
Preview:	/=..1.Ng..<.G.2h%.|./....f.}P2%....;..9.A......)F.e)...v..S..f.....U9..*.". .\..1~#c..G....I.H......?x7B_..S...wSI.H..a.j.Js._....@.2.3..9..A.[..h`$...J.*.....Q....D\|.a.s.f.a..*5..Le....?........I...h.vK'a..*v..t}"".'8..E`.......:TKK.M!.a.. ...wV#..G...U..Z5Q..+.X.jg.#.\|.BE.r.)-d,...v..R.@.._X..A..{YLa.g....P..4,-sW......./.../.IR.P"...p.-..VN]..........m.rc.ODn.j.....\|1.F-{...*KHM.`..,W.*}..S.....?}...:)Y!.F%GgGg.R...%kuQ8b.s....[.\|.....#s....Db.....#..]g. .cm..oH.q...P.9w.X..G#..Pv{.2......p..k%6.....E.#.>y.\.,...<%.....E$.x...M......[...S.tH...X..s o.3]aA.k....+wXu....h.A.2N...V.V.{z.7l..*2...@.s..+Oq..g.M......G.v=1v...z.y|HYgV........^..{.@.A..-..XR^..+l..Qp...A5.....;.. [..b..2.K.BTl.:..uk4.....k.......wtxE{...kY.......h..._...cqH....}.t.K....b.P..U......D......]zA........3....&`...u.)..+`..x7.(..&.....J.....9Y.`.CM]..f=ej....a.=.g.D{H).B.?k...@=dy.d.d..8...Y....xP........N0.@8.9.{e. ....0Fd?........... ....O#..B!.(V.r....U.........W

C:\Users\user\Downloads\IZMFBFKMEB.docx

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.834329925157917
Encrypted:	false
SSDEEP:	24:glfGWPmXvdj5M9msTRcs22aFoVYB1i5Y5cRZKO3DkwZuutrOv.gl+W2CXJHqzi5scPpYwfa
MD5:	287547122D009A443C1CB3EB8BCCCCE1
SHA1:	8F5CF97FAE43C7A4DDD02EDC34311E79596084CB
SHA-256:	1CEB5EA0EE189ECC6EF4C9B71C6B18C2FE3599C8F761495230B66669236B12DF
SHA-512:	59C0D09A12FE05E816DA7A09BE3E317C0EF04CE292BE00BB8CF319B5FBE897A3DBB0A2A1BA76A1CB68CC41FC40ADBDA6549DE036FAEED30D0A75E70B1A292E78
Malicious:	false
Preview:	I......W.'i.......d+2..N..w.7.&.E.c.I...Y.D.8.7kA.|.@.x...H..hg..-X'x50....un.0.....].....BX..ilp...[m..z).E.....4..u......%.82+h5...........@....Q.<.;.....p>!....H3e..@'...._4B........O......R...g.$.1.{.?M...s.zwL....5-v.......r..vn....f.. -............X.).5+...#....0.Cd\|uWM.C.....r..Z4.......q+k.6..rl~L~(k..-.7..}...*.&..1...A4.L..K....v.........o< .8..m.urLRAW..>$S.Z..$........f<.-.lrmt.\|.)..lgt.Y.k*H......v...m7-g.....)......2.v..h.ol..0..JrGE..3...w...(OfL./X ....YD2.... ..+\|..>..T7.u...*'..bkZ...R..4fy.~tqcS....V...._/#..99l..=.......+F=.~z.j.1..Zp(.=.Ca.Qz.k.}y...+#A.."s...q..U....~.!.=R...U5..f_p......S.3YcL7.V<..Y.<..\|f...&..A..t+.p..r../^.n..=..,O \..`..e....wWC]_,&&.z=z;*.O.m..*_\|.:R.....8.. q...L(..r.(.d.}..........!....t6...}M1...._.(j\.A.f.w*[...._...r...P...f.?...!.y...K.w..*9.!m..(....P6..w{L>C..W..^.h..;......y.vN................M..g....'...B.v.......V..._Po..p:....z...V."......VP.>.#t3....H....^.$...4...@L.....LP..0>...{...)i

C:\Users\user\Downloads\MIVTQDBATG.pdf

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.841836264242939
Encrypted:	false
SSDEEP:	24:DC1qgDZNTwhHnuOlzZKWuXUeOgCZlX2GKg0/EzWOsuC6xnXZxuutrtE2:D1gwBTlz0Wu88GdrESOs4x9W2
MD5:	D2F5529FD78105DE7886485E6DBD8C1E
SHA1:	E46591400774DC7898B6507940A2C830C1D4DFB6
SHA-256:	E9D8ED1978136112C9954EB88BA240DB6BA2BAEE21963D55673A8B61FD6156A8
SHA-512:	ED38239E6D825216EDB7FC5609D3CA1E5B6214F7EAEBD6B5B5A7643F89EA3507A8849ADC90C544F5FD675F00AC8783115E48D21027BB461C1BDA854FD7DCE00C
Malicious:	false
Preview:	....8o2...q...2+.*....{.O..~...3$W.P....!N........y.).].e7........ x_}7....&.PG..I.;-.g.gl..,.9.,.H.7U.....7.........W?....`.x.h.uK.DD.@.d-E.2.....N..D.h{..7..O.~.s..>gB.3p.a..a.....i....5.'. +'.._.L......=..*..5`....S. .@..U.9.KY `~..H.Y?.0.Z.3......{........nG...S.X..\|'.5e..N.Y..2......c..E.u../.<R.w.B..6..:...hq.....@....yX.\|.6;e...>......G......Z.....ry...H..L..1Rf+.......Y.a..U/.<.k......z9......uh*A.Y..A..vq.2..0'.@sdC.v?-.. ..9.[.<8.m...L.C.....#.;"I.C...$.... ...?......r.....Ko...K.13x4.,z~...N...&..Ug.....*..f.......@....i.Y......H.I...(....O6...QX+.V...be..tb.Z.).X.>Ug....$b..7.^......CwU..@.S..".W..............JNu.d..m.-. ..JW......zv..,....-..Y.. \/Y|...7 ..z..._..o>......%.K.A.y e.J..@.M...a..C"A....W..3.:.B..%o...........&.......X%..^yV..n..J....{.u....-@.W.....6..Y?....b..w..E.Gq.6..i.z.r.F.;..Z;S.....t.k_)K.,i.-."...0GU....x.%.2..{.F.~J.j.R....7..7..4........j.F.. 6_...0.~eR.qQ).....I.8...J.|E....X.f ..w).......".;...0...g:

C:\Users\user\Downloads\MOCYNWGDZO.jpg

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.849272575794706
Encrypted:	false
SSDEEP:	24:AODCWLJpj73DBGAj1CPz4ZTJ/mhdRrpRJsg+TZ1PxGByZuutrv94:BeSFrNG2CMZTJuzRlRmfTZnsAvu
MD5:	10985D3D60FD7080EE7E3989571F0706
SHA1:	C6EED853B52077E9C4498A63F988DEEA68479863
SHA-256:	06883982ED27C7D7A665A24875D9747DBFCBCCD23FA05EB4CE940BCFAD10DAB2
SHA-512:	30A114877F98086B284A6DA80F2DBEA52F2B3E12F95B002E055F2974563BA82785B1994C298D6CEC2F0914169584798623FD205AD0B124060D4DF79086EE8A3A
Malicious:	false
Preview:	4.7..>....<n.../wy...EM..W....*..h.A.......~..TK.#...3Y..[.../..X.@..3...nU>....r..&E%.q.#bc...F.....f....x...o...._."Y..W]."b^oE.\...,.G=s..!...a.hO.Qt........Hl$R.*..K.=4....6{W..2:.a.....l8...m.jd..>....J....{..7..K...yh...7E.....:.. [..Wn......_..$).O..L..>..U...a./..K...j....+.,..x.CE&.......P$.....).S.*..\|...W...j....t....iH..H...`l.z.Hc....(Ua.O.....>...-.L.M#W..&.`...l=.........h.V!.....c6.....xaj..o5....Y...h....Zs!.JD.:..n../;.P.........2b.._F.7.....tK.L..U.B.K..>.... ....+....+AcViK.F..!..kW..oX]..TM....M.dqUr...v.0~....../..gx..>.@.\|4.;....a^R.].E.......S.w.!5...\|.z.k..-..2...%......S.....h..+f..}...N...q.m.'D.o/("..HD.8b...\......&..W.....&.\|.jL......&t.s).i..t.6.Y...mC.....-...RY..1..m....^..#.m..).: ...Pj.y..Z.......IX<..\.....(...'..k....a.....a'PX..x.Z...c#.cn....!..\|. ..o;..J...x.<.T..V..#....lg..a.. 9T....'......2........j..\8...t...!n..,m."N.G..R/Ka.......K.G f."D./....Fw.1...$.2)......... ..F.....]......s`.2.$o.

C:\Users\user\Downloads\OVWVVIANZH.pdf

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.848130477911951
Encrypted:	false
SSDEEP:	24:MulXXuCwUzxQfOzy8nETiZ7PUy4CH3e1UuqoF3ioIGOuutrDun:eXXBwUiGzRlPFiF4Z0
MD5:	D9FB7DBFDB91127C8677FFF2B06626D3
SHA1:	8DEF364F32FB2166483B7A2C5FCEA9A5B6AEE665
SHA-256:	F30DBD113F24209AB813B7A3E08A9EBEB1BB3DBEBF4C62D5CDA42A83A4D01C75
SHA-512:	B593335930BD3AA33645F94D46BD087025371935775996D5AFEADA539C83444312BD1BF5184B26179CE3A3E9741BA7FE39F525EAD1D9AE33AAEF58A118165245
Malicious:	false
Preview:	.8.P.>a&...K|V..<}~ ..J*#Ltq...(>...\..$..OXo;.....u..?.c....L.....J....c.Y.$...l.:.......[#.2Y.2.Q)Ld...F.(.....d.<}...s.Z....g.;.th../:a..4..(...]..p.6...R7.....2 ....o..`....x.....^...n!.?.Q.%w.5....|.5.3...B..t....U.0...]...o.-.E.65...T

```
[.n../.;..1
```

C:\Users\user\Downloads\OVWVIANZH.xlsx Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.845542869239462
Encrypted:	false
SSDEEP:	24:VzHexFPAvnB+bLaGS3O1pC2sp1g2hG15sTuutr6vTj:tgPAv4bLaGqO1pC3y2h45s9MTj
MD5:	5A628C7229719C42EC5E5D7E27FBC595
SHA1:	DD37A5FFE3F4BCF0EF60F477B3186E57CFAA6FF2
SHA-256:	85C5F910C8AD4C476194A8FB3FDF06AF21E03F2EA78F3367C7962A206662E0EC
SHA-512:	BA428729B6341DF3F90741796DEBDF2EBC04EC3E940002BFF347250BED405B3F9E7C2F9F0BC6D40F7A868B7BA6E080A2A45608DEF6BDD1FB9FCD299BCBC1E9A5
Malicious:	false

Preview:

```
.^.)..``...*.. I$N....m.K8.....V..:.|T...iX.K.....j...".i.s......-.X<.-._.J.....i..qm.$.*..!.*Bc........>.....qW......w*.J3.'......S|A.v....wk..,B}....~5......."4......f.....C...$....$...z*...M.g4....#..*.(.........w....0....`V.....U/ebYB.......GC>..
.TZ.%.n-........_xf(..|...6.1J}Q.G.-.Dv<d...>.I....u.+|..Uv.u..N.I......6.k...Q.d.u..._.8..q..V....'......~i..L.|.-.....y}.7./...g..2.,..d.o...*hG....-..4D.k..u?.}../b.y...X.. ../...EZe.o^...*.P0.T`..\...a.k..I..A;T3.q..x...t.....wj.....J.{.';.....f.
d.G..I.....=.i..*U.O>+.r..\.T[[.)..A.. ..Gh3.f...2.D. +..H..B...~?...h.....n..f[s..8N...iF...j...~".>.,3`..;.A.`~......M/.......D...3...E...."........5...ML{.....k..F.....V....;d...2&i...=.]..:..2M<...b..|."..0..7..(..........eF.......N.P...d.H...3.
Y....I..sX.ut..`.98..wPs.$..w@....C.R2.n}i.?C@1.|G<..14.;.~.....GH..z0GY...!.U...RMd;;..O.NQ.L.d.J.....nt..(....<.....t()L.|.H.B..y..F.%X.Su}]....?Q.<.!..d..,.....Be.f...Ntli..O......0.......!+$].
```

C:\Users\user\Downloads\QEURJOJQOH.mp3 Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.831105134413187
Encrypted:	false
SSDEEP:	24:SwStvDmAm9w/DxNncLP2/uZrU2BXME72E2XyR3nuutrx:S7tv66W2/uZFrv2XQhx
MD5:	C7062017D5771E91438B31E8560D66DE
SHA1:	8C30648294535857669729BD3BA94C6D8AE68C4F
SHA-256:	306904F6FCFF91F3A37C6272C2BAA2146AC8206961E0063C4D747764289B54E0
SHA-512:	D8F0C206E737AE861706B88E34DC5510D7EA3F1B4576CA0E3663D65D15A6903C11C305432CA54A2A95B38924106A0EEB63770A141433610D9DABC2E132422983
Malicious:	false

Preview:

```
.8..mIn.G.0[.."..s..+......Z/.U^..MR.5.uQm...12..<.G..(R....s..v.....,..x=...F..vQ\.>...._.j.T.|{.......j.h.!..u.*7..\....`2h{"t.=...;...]N".....G.I |.Q.c..h.L5phD\..*.".b>....@Br{.9...D<.%n......7E.v. j..~1......h.D.W.e-d..........I.&....
P\}...z2=..^.;B.|/.....].....tp..c..`j....p!./+S.G..(...(....)._.N..&Q..\1.....A>E....T......Ic.|.pL.B.J.96.x.VM+..z..>.x3.N"4..U.9r...*...w..-...U|.'..#...6..DG..Q.H...P..'5T?.$...3f...5...aT5.E.y.If.i.yg..}..b.....y.T.n,dx.Eav.|P..V.).z .
...$..dPm[..M$.Aal5.)~.B.6.q..i.<.].O....}....m\".9.L...K..D[I.(^.1N.Te...rx.....aJ.hi....c.......V..xk..WL...L..u.P.J.(sx.S....I.@..g..\..@.....J...m....9..{...|4...`p\..F.S.,.....Pd...#b...<.zc...21..x0[.yO?..!{....B._..Y....:.....H
.vE8tB..B.m...Q..sl...... .{8....QU..7..<.......7g..d>.J\Y...04..NZ.'s..Mg...1....m+..~y}..q<}..{.T.;.o.{.-v_.2..2.....j..}...F#..!f...p........}.K..].7`...1..L..?....+........J.{,D.!....-.R0...#..f.cOP.R...:,.w...?.h%.....a.L...@..?..=
```

C:\Users\user\Downloads\UBVUNTSCZJ.docx Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.833277913907115
Encrypted:	false
SSDEEP:	24:9JzUWCQIJ4D5vy5oiEOBAGWkfJ0mYK+TSNKYd4aCGFB1HQKnRwCRtuutr5lhTN:9JzUWC2D5vysp/mYtKB/DWIRwATm
MD5:	A9051A5DDD0C0CC652ACF048D9912E7D
SHA1:	48048717BD3CD77C988AB5388E5E2EE2F97893E0
SHA-256:	6B8C18953D1448399D8A02129A7815FBFF3E50D669D9264EFF96A6907CA0CA6D
SHA-512:	72B9C3D067C55C3BA27FCFA92A55631CA7354BD48580972E483F23AACFF47A1E9DB52F7006EDD333686B36CE72A9BC95DAD7DFE8E5E8D2B602A8B6F72985B24F
Malicious:	false

Preview:

```
Q7......uaQ.q1.......;..:.#j.........zBnP..RU.....0.^1...'.,...|+U....^e"~.(.......pSD*4...1O...@.?....a..'s.2z..<.s....j..<..e..+8.1*..I.R..]6b.....\ t..r3i...&2......J....%.T.....7.R6..ZQ.n....|..xER@...d`.q....eh.z..R..A|..........o.h..
......{m...c.Tl|1I..7}..1es.37.]....$:xI..37....{.@..Y.L.^.. ....X.[.....U.K.k..F.0.y.L.C0.y..B^mN.n..)..1.!h...'N.z<....hZ..).)e...E^.+.HJkm+..*.d..z.Lga.....U...Hkh.8m]@..u#j.'..3]..~7.../........@....I.~(..'.....G ...#....;L..q
......5..a.-..hU....8#4w......\......s7..=...d.....D^Z.M..v. ......o.|.$q.[..v?......=w../..M....."o.nj .'.x....SvYg.....0.$..&... f..8bJ..%.c...!{.....B.......K.B..T./......x5.".$.Z..e.8i0...\...WL..<}.....cul.0..ej...a..8.o.1...."..M.P..o.s).0.=..
[....J_.1..v./D.....1. I...~A.U^...V..:%ZB;Pc.....-I...-z7.*...MYw..5.\zwG.r......M.O.uk5.JZ.y.t5...!...v<-I.!.7a.6...}#:G8.[e.O.N.3.qe..:..S.........5-=..ol.d...].N8\..=S..".......>#\a.?..(q..u.......2,{.\...].X.cs.....K..H..I.&...
```

C:\Users\user\Downloads\UBVUNTSCZJ.png Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.850411430642603
Encrypted:	false
SSDEEP:	24:KdI78aGDaSbBfOdRxc5DVOkbwmPAdWx5s2a/Pgguutr7P:KPaVSbBfiXcHt2W3s1gi7P
MD5:	9C31EDE7519B9C30D3933DC8D9264149
SHA1:	C27524E2C3EC5BE6EED9197BEA532B8926DE6742
SHA-256:	DC0EA049724761E08C12FD1DD06BD9636CB518D9FF4E2A51E2A453793657B109
SHA-512:	ECBBFA3599CAF510C9B524037EB574A91102E71D41B83FD0B116E5B77B52B41622F18AE33C2FD87F232F1600E4FEF5A8FCF2CF720C4DA73E2DD49BC5FDB600AC
Malicious:	false

Preview:

```
'7......0.3.;j.<!/;..^.>...8...=O.... .k........Y.y..Q...R.x...h..J............C.....[....G.OCo.B...z........6.[.....f.).t.t..2A.s.Sn2.jC........u.(K.......w.1..D...u.}I...,..0_r.kx] ....<C.i<..r0...M.@...P%.Iczx.Jm.HC.c-...z.G.......v.5L..
.qDY%v.h)...A%........H..[U.rL..T.n...z...v.......o.o>fsz...<.:^f.d4q.G/.u.=.....-..j..|.P<...I....(c..K..m.m..}Z+.hs6X=..<..:...y..dt.v.9....0.f.<..*7x....I....`!.!h!.......y..m..p.[..S.._.ez..a.=.@....-.XYKP[.R.....7b..#.0....']
a..H..W[.... ..%xK.H/...2...'.....L@s.pY....rk...I.R*z..r(Am..*c...L......E.=....?)|...X.U.....?^._..5:......,.t.v.r.&.P.6....-.&F..#"Byb.N../.>.<..K.......|.v4.|...b......zs.*f..pI..9.Hc.....A..@..]x.e.V....9....3.....Z....3..(.|K..95IW..
.h..a..I...}..}.....:.;(.........10...=..<"9cD.$.....(.I...2.....]......)..E..A:'......CT..&..}......C+.\...>(.....*]..)....G}3...../.H#..=..........f,.I..".8.....pt.Ji.10gys. .$..M..o..;9...2x.;.E..].t.M.>-.&...*K.....exr...........
```

C:\Users\user\Downloads\WDBWCPEFJW.jpg Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.84641778720141
Encrypted:	false
SSDEEP:	24:q7j7J+az84ufagU36o8ipbGosyBOqveswLJMCq3zWhk8kuutrUK6X:qLJ+IjU38ebGMBOqmbLJMXDWhk8mU1
MD5:	689089C6A15AB390192965170EF55AAB
SHA1:	D1C5B67C14B243B2FD7B6AC949BD4FB9DB9BE95E
SHA-256:	EA4517B61B478A9CE311F11E36B5D41D3782AF0B91E03506DA36B4B3719CED69
SHA-512:	2D22D997D4F0821192FF4EC7A9FE9F9A6E1CCF647AFE6866674703D6828E3AEC0E4C2380004FCFD1B9E907FAC016933FDDE26721160B53388CC7B7A8A3174DF4

	.)~..y\r........<.t3.... ,..n...G...=...62f.Z{.Y...XM(:._...w.<qp..(..C.\<../?....*.mXj.,."....zc...E.6C..$......&\'.%e...\|........tu...j.tb>2./.".N..e..0[...u...D.F..V..s.ct..e...Q......q....9E....R.T\|..Z....C...1>..RA.xh.s....60....K......? 7'..2T5.3P5......b.BG2.D..H......Bc...d...u.F.yW.t/.f.Ovd.......-@s.{.W..>o.6.#.t4........&h..b......F..Q. [.=0....u,}-.t.$Fn.9b.\.0i.....n...W.V..[.-}.w.[.."...E..k.x..:g...f..*...p.&...K....b..%.ap.........vpr).....PY..t.6....&....\;Oh. -..ZS..$P.......I.A4wY.J...!=.[.#b......n...P.+....)x.vQVIQH.......C...f.Qw2.}~Xd.8N3..3.F.f.;.I[(\|BXQ'..>......E.%$o....6.C...ST...-...=(.!Y..)U.6...Q...G.7.*.OI..g?.p....5T1_.5..ts-......H.2...#I...p..K.%[..A.

C:\Users\user\Downloads\WDBWCPEFJW.mp3	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	7.834610210870247
Encrypted:	false
SSDEEP:	24:3pd3XL65JAco4uzpH0R1qkYFpoUNDFLDoZFMEZzulA4Wj7tqXuutrR1i:jO5KS8aR1qkoWm+Z0lmoR1i
MD5:	F471C4D30355AC89BF49DC56B397302B
SHA1:	1B9371155C96A422F99A139D92A5FDE4DF06B649
SHA-256:	A98940EF6C13A76A949C93F4D657D90695A5CEF99416E9D115508FE4947F8140
SHA-512:	908E2BFA026E9472347851C43C70B9715149902F801F2DF4477F4E9B703BB3EA4E5EA6C267F1555FEDA09738920BF40192BA4759A980BF0AA69C0AAF04428A9D
Malicious:	false
Preview:	9..\;...Y.....;s...F.....8...t{....."..-..;........`.V..v$Z5g..h`...fE...).T..yY...N.....v@....8p.KK......6g..+T&.H.e.)...;f.1...=..q.b.n\......`.F)..?...R..)g.vpw..-.4...k...h9.B~..5.QQ...s....?a..A......e...a_..b...../AioF..#.S.;.h$.O]C.. .....'.MV..B.L.7f..0.......`..t...Xa4Gg .=P....N......h+..\"...f.T..k4..{#.U.T|....\.....jjR....".1.G....f..<.8Nu."A...4......W.H.NLa.K...>K6#.).....VG.....5@..}Fv.....II.>.F. H."...'...X..S...-.H...C....{d.....H.8k.Y.k./>.;...~...U..j.... 0.!..sv..N._k)p....';f....bN..zZl..BN-..V..g../....|..../..`.D).c.k2.w.....6a.Fl...a,.....H..x.:{..A.....E..T..m.J......+..Q..6..b.`!.>..K.UxW*.|..1z|..B...I.I......dE[.<..._.{......T..c.d..6..Uo....e)$#..<=...@.#f....E.......e.g\|..(..j.U.. Z.....]..R..."....F..8.x!=. .....m3=c.....U.@...Eq.(,....>M.1.s...>..i.LX.\|...{....tz.B.WilP...._.3u.+WY3..[$.......*"..i(..O..4f.....U#$>7P.A.....*.X.0.$.9Yh.X..@RV.&..k.1."9......Tg...x.D...Ny.`......;.;....(.....T....H:.:.I....g.s

C:\Users\user\Downloads\z4ra2w5g-readme.txt	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Favorites\Amazon.url	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	343
Entropy (8bit):	7.3732594921357535
Encrypted:	false
SSDEEP:	6:4+b1iyMi6JAF89GadTGGAYy956Cz8Zb0P8wbMvtauOHXj44h3XXHMsMeFX97:4e2AF8XZGXnSSPJMvtaurW3MstXZ
MD5:	DDF45E13434C095ED3E98C34D4AA0715
SHA1:	C42587C8486D66E125AD4260562EC7C4E57D681A
SHA-256:	9711452C64954463198421F548B26E93A1816FDF3BCE44D9F3F22C107BDF5B4F
SHA-512:	3A335A6A9E68D10DF102E31435986DE85AE20DBE15752D94645FF59AC607FE9E9D31D487B49EE912950045421D274E46B5E4F3B71B77E30923C8CB15B68B0D49
Malicious:	false
Preview:	...F..Y....#,.K.=.h...D%.....1..W..G..Xe..q6..A..(.*...7A..!X..?.-.y.K.......V..6.<..v.<.....w.9....}&L.........-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G....... ..?jR.dw......?F.2o.E...x.>.)w2.r.b.......8hS..Z....e.uu..e...Gb."`.[.*.9. ....^

C:\Users\user\Favorites\Bing.url	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	440
Entropy (8bit):	7.5438994103059205
Encrypted:	false
SSDEEP:	6:59GqeagN25Dm/JFNnyWo1+DhXyXLvRCz8Zb0P8wbMvtauOHXj44+NRTWzmr0pWF:e/l8Dm3n9D5GJtSPJMvtaurXPaSr0pWF
MD5:	C9C6ACC5DB7A3BFAA914D032E3E0CC75
SHA1:	15BD6370B195AF47055A4677C5C182A3E9FF15F0
SHA-256:	89A4BF3A8323C194B92C2A9605B1B039DE2BAAC1F0FBFE32F51B491C6C42EF48
SHA-512:	FA5CAAA8E1F583738BDA4947B1B5AB4CD0C91DD89F82C848568465EEBA14948BEE429421B3308FE27FDBC820EAF351E398D0B9A82893B1FDDAD3717B31E5FD84
Malicious:	false
Preview:	?.^y.ok.k..B{.....A..%g+7.QQq..MNR.......K....p...._wX..d.p...24f...5"Yn..g..s.9....)...|.-<..|*.XR.:...6.~.#.\...d%.aA..h......)6^..Q.[..X.....u9.!f........sK.....veT..?.M..Js!L.~..k|.D.i9J.....-...0k....i.........$..~.d.rZ%.f{. ...bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G.........?jR.dw......?F.2o.E...x.>.)w2.r.b..c....."v... 6sl...(.v.<d7.|...;....V.~.........F:.

C:\Users\user\Favorites\Facebook.url	Download File
Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	345
Entropy (8bit):	7.264990375273729
Encrypted:	false
SSDEEP:	6:a9jEGR24ElGeehH1LSlqJCbmz8Zb0P8wbMvtauOHXj444AShpgzns+Xn:aRvR2lGeehVqCtSPJMvtaurnJB+Xn
MD5:	FE50C86D59AC47271ECE0D2FE3F961D6
SHA1:	D5A0FE3F6C191DF3C9F7CA9B43055108D4F64C1F
SHA-256:	67D776BE2E94DC36BA686ED0C0C6450A514F59B467EFBB26A146EDECB714E7AC
SHA-512:	558A4623CBFAA009379FCAD44E8E662F744E7DF06D4CDAE6805F0DD5BD175079B72E6EC174BC7988499BFCBA5999D496BFFBAE36D5465F9D38C692ABED7CBCE6
Malicious:	false

C:\Users\user\Favorites\Google.url

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	343
Entropy (8bit):	7.315823913157121
Encrypted:	false
SSDEEP:	6:wNxmqOJMsrjv0AFtlwPf8iylmz8Zb0P8wbMvtauOHXj44sStlsngEC:wjWdMiylZSPJMvtaurCtlsnc
MD5:	7A346680A41CDA4C3E36D419CCA4FF26
SHA1:	DD94296443C79673006865210FD2F6E3E6E76EB3
SHA-256:	A5610B8E3FE5FC66A6D95E8FCE04EE19AAD82A6E3597F32EE3307E5CC4F48B36
SHA-512:	F3FCB73A9BCBB5BD8D3B02DF254F9E823454BE3C8F66339B52E318B6D245AAC6450BCB12DCCA6D4FA0A7C144BF8A1E42D22CB5B05C605F6D22B5A861F3033E0F
Malicious:	false
Preview:	.....G&...O......5..V.....m..M.1.(...I...\.bE...-...7...*.X]I....).$,......`....`.....d..e*x..s......{.......-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G.........?jR.dw......?F.2o.E...x.>.)w2.r.b..@..o.T..{i...B.Hj..zw.3.?U....V.Te..a=..A..........i.

C:\Users\user\Favorites\Links\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Favorites\Live.url

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	341
Entropy (8bit):	7.426101563818844
Encrypted:	false
SSDEEP:	6:awuTRqq51DOdCtmz8Zb0P8wbMvtauOHXj44Ulffg:aZDOoSPJMvtaurdl
MD5:	2E26E98E3D1B1DDE77F01B28062B1946
SHA1:	87C15A47125B7AEB877634E4960C9D66342461FA
SHA-256:	3C31074D28ADC9009AAD460E13371E38180D04E77D24F0A39E87AB81ABD34A27
SHA-512:	306C5C3314B5C552F4C123CCC9904FF0E631CA08DB2E9F4F45FDC9C34A1AB5DA834C01A591EE3FE54FB51E727F58958F141F4D5E3C0B46DC93F419D505861CA0
Malicious:	false
Preview:	xi.G.+...k..~.U.....tY..y^%.7y`..g..t.9i,*M..5.....w(.......=..}.a.].....O..;.....Pz.g...o.!Vv{+.+..>6......-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G.........?jR.dw......?F.2o.E...x.>.)w2.r.b..#..$...........$q..t..u...L_.}x:...A....P..........1\Y

C:\Users\user\Favorites\NYTimes.url

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	344
Entropy (8bit):	7.363604505160842
Encrypted:	false
SSDEEP:	6:23ZG26f1Q+OMsqEetjQr9Ctmz8Zb0P8wbMvtauOHXj44XwCoEaYe8BQ:2SduqEGCCtZSPJMvtaurGwCoGQ
MD5:	0DB07B3CD01A225EAC306A938E037C7A
SHA1:	FFF8192D8448271592C30F20C0D68093D46D7A19
SHA-256:	A7F0AF956C00EA43B3C38E500D178043C9A14302008EB3AFC604C68AEBE92B46
SHA-512:	361ADA49036ABA6099209E99934BEA09B824367BA7826A55FDDA23C9FBFC5C9E2C1D2637A1010385C05E11B1A38509E9C6CBCED988EE0678E188B72B7B29A1DD
Malicious:	false
Preview:	.,....T...hu......*lB.._..k..+..d....[n.=<.i7.Y.UoC.....\..9....Q......{.9a......M..p.A.E7T.PIJTQ.N.2........-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G.........?jR.dw......?F.2o.E...x.>.)w2.r.b..]T..5b......Po.....D.$SA.4x..+F-....~...9..............

C:\Users\user\Favorites\Reddit.url

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	343
Entropy (8bit):	7.3870468272762775
Encrypted:	false
SSDEEP:	6:sDAnrybXJ7wMS2R4tzL1v5qhVlmz8Zb0P8wbMvtauOHXj442BNxzXTOF:sacJ8uRg5vbZSPJMvtaurjKF
MD5:	72134F264E262FD96C98D0AD9FD78B79
SHA1:	51793DD45CE3883C3C96CC77F2A9652E735A29A7
SHA-256:	ACEF88443CA01BED894CBF3A22581EA47AB053AAF5ABE139303083EA5A3FEAE8
SHA-512:	97CF75DC4927C0CB5AF32C840248998B53DF039815F4754E0D9150D89FD310A09657FC0F8B2B5C631CDC81B96F959F2D5B680F24EA52E4DCE8EBAD368294E14C
Malicious:	false
Preview:	.*.#9..I....=.;....DE..2..?tW.wC.3].E....;...,....,'..c.}...Oz.....:.....[.X[...jm.l8z....F..#A.P._.Z..AI.......-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G.........?jR.dw......?F.2o.E...x.>.)w2.r.b...P...r.+....?...2.1....dh.....T.+|.....M=............GC

C:\Users\user\Favorites\Twitter.url

Download File

Category:	dropped
Size (bytes):	344
Entropy (8bit):	7.3843430611680105
Encrypted:	false
SSDEEP:	6:VxIqbThwJls3Yzb3jelmz8Zb0P8wbMvtauOHXj44dYFxgtd:VeqbThw1qb3bZSPJMvtaurQYXgtd
MD5:	B321483CB00EC77E7B7C2675F2846AFE
SHA1:	5442D884D770EF1129D99582FF9B09C92A1BA081
SHA-256:	2C0BBE9AEA6CBEFFCA2D038DA805D2AEF08572FDE4CDE414235746E44F9EC18B
SHA-512:	1829070E315B138076570333128D08948FFF4D6FF659C9614E684F3414A24BC489506E86C854A7C0708DD3CD8D92C2AA36CA54F751E8D71261FA0744447343E6
Malicious:	false
Preview:	.n..#.....n..b7;....*.......^e%..= ol.J.clO-}......."...t.....W.....I..5....Y].g.....s....f..........e.D}N........-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G.........? jR.dw......?F.2o.E...x.>.)w2.r.b..Z...sN..q.a/.I..%_>e.8./....S..q2[.amb?3j*.........v6..

C:\Users\user\Favorites\Wikipedia.url

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	346
Entropy (8bit):	7.366491198855434
Encrypted:	false
SSDEEP:	6:rKuE9qCFFF76nOVtghFz8Zb0P8wbMvtauOHXj44/QjfDnjLoM:8tdoOVtghKSPJMvtaurjB
MD5:	E29AE3DB0EB08A5CB0580BAECBDC5ADD
SHA1:	A560B06EDCDA583E340806FB85F0A72AC7C35C2D
SHA-256:	CA4B992C649CF7317ACC97EC961458B00DDDB6B1E09E75CA0EC5FD9DC32B95E2
SHA-512:	4B5CBC393A797190C7B810F1181C89537B22522CBF0D51670BBB61FA82D7607C067535836E721F19D1F156B52622A331AC9D179EE451AC9A250DF8DBC7C61461
Malicious:	false
Preview:	...Sa..Y.\0..q(.......qW(....~....;F..Oc=..X..2.........CLX...|.|{.9GH.4..,>r..t...r.....Cl....I,]0Z..d.!.......-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G.........? jR.dw......?F.2o.E...x.>.)w2.r.b....a..b....5 d..a.2..+.[..6.(N<....8....iN............N

C:\Users\user\Favorites\Youtube.url

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	344
Entropy (8bit):	7.387962574243115
Encrypted:	false
SSDEEP:	6:7TzDc4EsVRhRfLBOz8Zb0P8wbMvtauOHXj44L3Dd0tP/q:7TzDPEKhRDLSPJMvtaurS50tnq
MD5:	DF893E8FD51D326AF87EB99323C00251
SHA1:	C727EA0123142F84D55514591AADB6424ABDF07D
SHA-256:	54942C2C01F5436BAD85E4D5F1F53FC20BCA136C32F69A25F1FF50ACA8C8FA9D
SHA-512:	5AB5BBBA1C22EEC73997B58A9BA028952B0B7A680113361CFC2876130B3D3AA50CB221E11013B143445D615B25648E1C9DDD2EBEE28D04305632716FA26DB234
Malicious:	false
Preview:	.7....o.$.s9....X*..N..!..c?4o.D...#0XY9.N../..5!."..c..%....75..zeT..3_s...]m...rB.....b.RY..~.....T. ;e.......-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0 Q`.G.........?jR.dw......?F.2o.E...x.>.)w2.r.b...2m..E.L.SEC.....n@A...F.G....`?=..D.V.H.`>.........n.a

C:\Users\user\Favorites\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Links\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20200930\DatastoreBackup\edb00001.log

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped

Encrypted:	**true**
SSDEEP:	12288:jjpZv3MZBC1cmXD3voNRBzdzcxOhdYj8ws0s6dX:j3MP4LvUzZcuajpds6dX
MD5:	7A076C668D9F1D10F71AA191608E0EC5
SHA1:	0C6445E757291CEDFC06F140A8AC2733A3C96065
SHA-256:	FFF95FEC92200C0B6FD13F6A0204425F149D2533A25EA85A05CBA9F786776E92
SHA-512:	975665DE455707B326B80D3D6DD72F6F87EBAA5AAE338D6C8B4FA9FD51444A196DC9931677E6262537ED42EEBF0A4E983B3D92FB7A2A2CB931B2546F63C962D7
Malicious:	false
Preview:	9.>^A+...i.,7ZK%:....|....7...{.S......&.:.P~....'.bj.<.U,..qDoNA..:0....4...:..Vp..U.....(.....N.....!J.Q...)...sG.........L.`{.hQ.A.7..'.q..{.9...'......$B...@cg.X[W.9@.S.......S...".lS...X,..AL9...".AV=.$..fa..Q.......(J.L,..@+..c....E.a.....<~%....6./g............V..@...a>..(0.$..m.(.0..*.....p....(tE..F.......P.`.\|..,%.f..x.;>.....+`.j..K.bw.hW..z....b. %..i.=../.\|Z....j...........~^.N.....H....-d..R*/.1...v.e...Y..+.X...Vy.P...>.F..I.-..&.K...".)..^.....!)*.*.j......S.@./....\|..,F..#~.r.b....J./t.%...H.1PT...e.....i}]H......43..'..U.B.Y.9iN..#i..3.....xx#..(q~.wr)....?..X...o+..y.Z....>n6....%!..D O..)..+.".m...._.s.n.....*..N.@.Q.m._.A!.......r20^...89*-..K)....!.b.,\3.kV..0..y.oK....J&T...........C..%L......)..:....8.S....^...B.K...........l....$sx..K..n..[...W...)..N...k..Y.....G.|._.A..Y..8....V...'._y.[.-z.+A C....z:._ld4........r.......T.D;(..,...8..l...su.a......[.#Q/.'@..E.f...c........k]...WIU.(....a/...!..29.

C:\Users\user\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20200930\DatastoreBackup\edb00002.log

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	524520
Entropy (8bit):	**7.999673212045116**
Encrypted:	**true**
SSDEEP:	12288:3sNA42WVQ/AS53L8rgrpsiFGoBnsEkpd1MbfPp39NxnmkQ3W:3ZL+Q/AS5bzsiFcHfMhZmV3W
MD5:	552986DD24F6C6C36B4456A4C746614F
SHA1:	7C89ACE9220790937E580C77B109453F522F6056
SHA-256:	3C67B4C4273CCB9E640F88347A2DD3EB0467EE09784AFD60AC8DB2AE571567FD
SHA-512:	7F9A6A212C98C2EDF8DA9B7C97357797461FAF63AFB3018616C434269E91FB7B748E1BCAF034648BA140047FCCAD19400A05B0C4D227AF4CD2C394223CA9EAED
Malicious:	false
Preview:	2.'......t..Vu..h.l).....T.:....N_.<.l.f ...LXLA.g.%....._l....9+....h=...:F.N.}.xfz~..=M/...g.|a.o.T\.pb.W...3...k+C.*.....c..G..3.....&H.W..X.'.F.J._|lr.]k...~#.....i....()..{.....|.s.Y..O n.<?:B-..7.......]...t...../ .:;Rq!Fg.K..._.dB......V.......t2.,.#...V8_=...T..4..K(..V&......=,}aiHh..[g.qt...^p..<.[.}.....bg*faP..$2.RU.....S.y4a.!*..rT...>.5~..@..].~......x..8..".t...W.~.H...k...t........L...*mzG.F._b..BT.r.{....|z.....R.l.*....w..Fon....K.....j+.P....#l..r.1.rvD.."....el. ,&`-U9e....~].S....9..S.>a1..w..X.LK.D...T.<./.X.k...Q....).;.'.P=.{..0........{yX.=y.....y..3."..l...0.1l..2.\..Y..........y.!......H...c..t....^.H.......[O#P.Y........0.7..B...jlM.....J.Nk..f...:......#..P;....YKP..rD._..h.)[..?.RX.&...@_8..U8.....q9...y...Dh..b.w....SF.........M.v.E.H..;.'b..W..?h{/..n.7...e..#N>...H..NN...0C...;S..(G!f..sz...a.A..7.......'s......%...|.O..(..#.t.7.c.L.X..V...4y6N../.H..v.....'..j.\H!Yrp.o:U..e..Ftxg.6.%.T .By..

C:\Users\user\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20200930\DatastoreBackup\schema.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	253
Entropy (8bit):	7.148615116025246
Encrypted:	false
SSDEEP:	6:Wtmz8Zb0P8wbMvtauOHXj44B+fOvyafllj:WSPJMvtaurfftaT
MD5:	DBE4E0679D189C8E9C63AE98A10CE6C5
SHA1:	B326393C624922CB3FAB5441B72BEC68CAC2FD2E
SHA-256:	FCFD478C010C0E4884A00BBE9154EFFB754026BF52054411294130FFD08EE03F
SHA-512:	8CBAB11B15FBFDBB557F68D7C89B377BD44E465E93510463BB783CFC67F5582DE1D8DEDC39239478A7366A4A7D9C39983B5C359E397DBBD04FFBC92455447863
Malicious:	false
Preview:	t.;t....i:J...F.&.......-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G.........?jR.dw......?F.2o.E...x.>.)w2.r.b...'.M._..Vz..Sj...<{......U..J.YS...J..f.N............o

C:\Users\user\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20200930\DatastoreBackup\spartan.edb

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	2105576
Entropy (8bit):	**7.9999136618737134**
Encrypted:	**true**
SSDEEP:	49152:2dEweo934S7zrmpJxKccfOJNvx9zelyKPT14qpL6loL:2dEweVS7Pccf8N7elBtmuL
MD5:	4FF041D7395B12B09C1AC41E675CB98C
SHA1:	EF4A57E0046B0710F9ED4A713741441063F35592
SHA-256:	53FC8A45978F40D8C8F332868870115D53A23E8049C4CE569D3129F28C141623
SHA-512:	49C438EC2BB50BB1566BD9DC319C139916CA74B00160C74665B4817A1A152B036DDE8FFA265BDE8E6457C94390D3CC1423923789A4770B72CDBC1B763A42823B
Malicious:	false
Preview:	B.C..l..".*3..HZ.,.N@.8(.Z.p.Z..].e.g..z.Y.3u.1R..?.W~:..+./.].......x...[|...X...E.k.X7..H...}......f.V.D.i2..X2...gP.n !F.+.MM.........#h.Z....~..z...z.+e...1....b5is.Z....-..).B........4...F.........,g.sF..]....G....s(.m.6..S..=..O.1(Y.I.J.s.L{...P.q..z9.Oa...6.b....s=$....l...F../..u.....:....\|0..'K.m.....`r....l.D..8..v...6.i.x\..1N...W.x.V.....2..=.K.'........C..FD.g..K/..JA+.](.....%....T...Hm.....'..N>.?bA].K.fbC....9DO..R8Y.d.g7c..'.5;.....V..g....'B....'V.Im......u9.O..+.JcQ...`48...wR.kN'..A.%..u....p./.N.$".~w1~.m.'..l8M@V[W..%.b.L{..[.4.7~. ......Y...K....A.!-.R<....`.m0.&..*(..n..W_..E..i.D.o......$..dg.............x.W..`S..J0'O?..u....H..*.........g...*P.Rs..s...T.y../od..h.....(.(.....bP..4T&(...8&.......|H....X.^'..m. ....(.s.|.i.;...OW.F0tP|.\...J.. `7@..7.......!]/..H...jo.R7.>=3.......*.)fa....*.W..H.........3..}....YH8..r...........:..S.u..6....D........ 0U......@4L.......n!.{.e..E.J.gOC..^.........8..w..Ad.8EJ..

C:\Users\user\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20200930\DatastoreBackup\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.]........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.]........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20200930\MicrosoftEdgeCookiesBackup.dat

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped

Encrypted:	false
SSDEEP:	6:UqF9bDZkFY3HyvOptsODsRa4qxLdkHW/04aaVTlXz8Zb0P8wbMvtauOHXj44jzzf:UQ9bSsSvOpKfM4lHyYSPJMvtaurKlZ
MD5:	9FE6FF90882A32079F8815A5F63DD896
SHA1:	3321E9CDD6B91CC33B43B6EA4520D8E95938A524
SHA-256:	148FDA545DBF09BEB5E674A48A7D0AD36AF44225EE872271D0BCD59CBDF9DD5E
SHA-512:	7C47D8A37830EFCA4864B1A1CBF64551E151CCD246D8030381DC16CAEF145388D9A14F658029A29C9535418C008CE09CC4879CA080EBFFAB339C5B6B1FEA1257
Malicious:	false
Preview:	.X.g.?..b.^...]......*..0..A.%^eB~J.....Q...*.k..s...,..:}.&..Q....M..)*A9...X.&+...=.v.........}mV....ILFuh...W.5.5{j..).Il...4\.Vuv..x....+...,3.F.^...7.6(...oR.~.d.9.G..M../...%3g|S}....e.(]...s...A......a.m.n...$..s.w<.3........-...0k ....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G.........?jR.dw......?F.2o.E...x.>.)w2.r.b...2...b.....>.m#......,.V...yM..\.PW.U..........3..

C:\Users\user\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20200930\Protected - It is a violation of Windows Policy to modify\Backup.dat

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	770
Entropy (8bit):	7.765136641417782
Encrypted:	false
SSDEEP:	24:FQEPduMIUPF4kwMUUC1L/01nZVv0uutrJ8aM:acvlUpwMUUC1L/01nZlJ8R
MD5:	1925B33ED01CDC74A41CCA49FF308DED
SHA1:	61252A51C758B43D213E305899930295135C7EA8
SHA-256:	B3402A1DAB0E7BFD2BC3A22F9D852957545001C5340421C64F635C7DF8D52CEE
SHA-512:	D6C11DD82CEDE760209C54532B33DB0AA7FC4FF17027151AA551B250B2503D024256BDD992D2E58BC4C8EAF0326C6D7DC1C7F60F1D6F1E1EAF78EB97C2FCF69E
Malicious:	false
Preview:	.:..V.J.7...[...D.9....UH.S.&..v.\..NR.....>0t$.......a\|....)....i.r.<.{...+.{.>..#Y}0]Y./F".._.&..y.1.......M.+8..$...,.K........|(ju../..{...K.dljy....oF......T2....h|@..X....!t4.n...JS............R....q.4.a.3.m...T+.{......Ez0.......`./.....bN.. =#(1.=$.....cs...H..O......ilj.....``GV?.K...Br.R.)...=s6.^.W.B.wl>+.]{^+!.....l{h1...?.)..v..o....'0..8..^..q../.\.d.4...} >....a=.\|..>l....*.[..'u.].0hz.PEdo6.w.../.....J5k.h..i..@..+...f....3l..~...ka....ui..M...e}.g ..][Xa..;.....n.b.e.X. ...._..r{!F.Y............-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G.........?jR.dw......?F.2o.E...x.>.)w2.r.b..6?.:..^.....eGg}..)..t...w.(PN...!i.A.#OfU.......... <

C:\Users\user\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20200930\Protected - It is a violation of Windows Policy to modify\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20200930\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\MicrosoftEdgeBackups\backups\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\MicrosoftEdgeBackups\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped

Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Music\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\OneDrive\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Pictures\Camera Roll\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Pictures\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Recent\z4ra2w5g-readme.txt Download File

Process:	C:\Windows\MsMpEng.exe

Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.]........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.]........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Saved Games\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.]........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.]........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Searches\Everywhere.search-ms

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	480
Entropy (8bit):	7.596813007535851
Encrypted:	false
SSDEEP:	6:pQaCSmpnJV8l0OaLCPwOLDglkw6G0d3nk4TqACrGJJzz8Zb0P8wbMvtauOHXj44z:pKrPRLywt0d3k4DC4OSPJMvtaur/D5o
MD5:	7C9237586BAD8A82927B3A14B6BAC4F7
SHA1:	0198592D7BA5A76D41CDE78CD3C4A1D5758FBD0B
SHA-256:	D10BFF4DD649DE0515DBF20E8F23E5AD68FD4029555906A8523C34A654F51767
SHA-512:	DA6375292160D44115DA715393797422FEF271C3DE79693686F5CBD07E8ABCF257A97F60D90F8743445691A9952EF6946F17F063F84B1E888E8C1A367A813859
Malicious:	false
Preview:	.C...Y;..........{...K"....Fz.'..6....cYbr]".# S..++H)F.....F...>D8@ jg*Q..h.P[..*.pX.Y...+K..H..c.|.A.w .x.....{c.\v.B...B+N..N.-..}n+./...zHFV.eL....s/..K.......M.a.i....B>.:..{...0.].P...B.&.U_.8..y.....kS..H..7....\.W..Z..... ...-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..|...J. ..0Q`.G.........?jR.dw......?F.2o.E...x.>.)w2.r.b..U.Yt..=..Q......m.X.........@.6.'''...w.h.............*.

C:\Users\user\Searches\Indexed Locations.search-ms

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	480
Entropy (8bit):	7.541905870823924
Encrypted:	false
SSDEEP:	12:Bdt9vlpX/B15Giotf+qvSPJMvtaur5gZgv:Bd09B1ytxvuutr6y
MD5:	896FCC58A48A3A83EB7116C89981CE75
SHA1:	809AC18D797B3657A82DA4E4F37AC8AC1C52880A
SHA-256:	D8115B8F6354A5099F222D1FD9BBE861D0E4E78DE1CC57289B3A736B607D1AF3
SHA-512:	2D0C48D163AFCBC0D1DA464821F2CA810941BDD65C77DF8E92808FA51BFF2346B8A622051A172EB145632FA4A0B7FD866887AE7CCE71C9E15DBD9C3D78974392
Malicious:	false
Preview:	...`.g@..Y.....V..r............a.......f...m.wz..dm*.r.l{..%N.+.k........b9S.U......j...F.)..<.tlyr.U..l.eB/...(.m.!r.......N. >.P.....'.....v.m#q......Z..aJ]'D.........+..8.`.'.g.[$........t.....)k,3_..wP....(C[.J._G[.Ui.N....T.....-...0k....i...... ...$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw.\..\|...J. ..0Q`.G.........?jR.dw......?F.2o.E...x.>.)w2.r.b...z..p$-...>.Z..b.).s.?}.w7|.........8n.w.............

C:\Users\user\Searches\winrt--{S-1-5-21-3853321935-2125563209-4053062332-1002}-.searchconnector-ms

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	1091
Entropy (8bit):	7.821896515314162
Encrypted:	false
SSDEEP:	24:kDJSxDRm94edYmQHaABABq4sbfou969b8uutrbSqf:cKk4sYmQ49s/6Abpf
MD5:	98B182BF01B2D38D0EEF2B51A535CE4B
SHA1:	035BB21594421C96CBF4456E917B2D24E0AF32AB
SHA-256:	7AC3CB181E8EDC0D1BC784B4DE0C4ACB84E89A32B403D998443F6CEF2F7C347A
SHA-512:	9B0ADA2E8A02EFA0C580FCB57CD26EF9F43F6C2DF710DD0694A99F999D8C3FCFFC591C8B32346B55E442239D7248AABC5256EBFF79151509F78A63FFBC035F53
Malicious:	false
Preview:	..*.)...0a.....aM...L.3}.W..].k..*.0LZ..W.Z.;.z..".)Z....;/.0....38.F.....I...P/..E./..._7Ehs../...OsU<&.ZZ.....o.x..s....{C.H.G......)].)l..N......<.........V......_.DV..C:...O.g.k...:.u<.=.jC \\|..6.>.......~..yl..Y. .c.?U..-Y.v....8:..,=. ....8..|Uh.d...<...=.2..R....57.._......Lw.).9.k.x..U...+..O.{9Z...e.J..e.y.........6.B..^......8,~ipx.l}..cb.._.o.i0..p..k..~....I.O.........6.l@.%r..T...\+c.P.....;Ug(.0...r.,..U.Z..D..[.\..J.<~1r.x..R...;.J...!.o@.tB...'.)...J..4l.I.C/.. =o....V....yw.....4.bo.;$...$.u....E.....8>..Y.R....O...y.....Z...Ry".{....P>.<....`g.K.O}...]O.....y.Ox.=g.".*c(..Ca..O.o...]*P..Bj..G.Q.5.[.W.?..6......o...O..r.A.#0.W\"..w=V.Zc.._H.._...q..P.^.[....h....?.B...=...A.....[..t$q.9 n..4.D...g._...V.8.W3..GW...aKT!.SJ.D..}.C...<.8_.{X.;).4l.......eA.=k.....O.S3N..b.#.=.'.(tX#...m...;......X.)9.S......!.....-...0k....i.........$..~.d.rZ%.f{....bp.k..#...j....1.1U.2.E0AF;W,..R'gPa.$...ym.A....V......q..D ...pw. \..|...J. ..0Q`.G.........?jR.d

C:\Users\user\Searches\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data

Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\Videos\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\user\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Users\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	false
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. .i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)...........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

C:\Windows\MsMpEng.exe

Download File

Process:	C:\Users\user\Desktop\revil.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22224
Entropy (8bit):	6.802966536066802
Encrypted:	false
SSDEEP:	384:NDr3WIqWJ1q//0GftpBjRwtxO4HRN7uJlYaibn6:FLe8ifJkuUaY6
MD5:	8CC83221870DD07144E63DF594C391D9
SHA1:	3D409B39B8502FCD23335A878F2CBDAF6D721995
SHA-256:	33BC14D231A4AFAA18F06513766D5F69D8B88F1E697CD127D24FB4B72AD44C7A
SHA-512:	E7F964A10A8799310A519FA569D264F652E13CC7EA199792DC6A5C0507DEC4A12844A87BF8BAB714255DCE717839908ED5D967CE8F65F5520FE4E7F9D25A622C
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

	• Filename: srnmp.exe, Detection: malicious, Browse • Filename: BORANG MAKLUMBALAS - SESI WORKSHOP DIREKTORAT.doc, Detection: malicious, Browse • Filename: BRIEF WRITE ON EVENT IDE 18 JAN.docx, Detection: malicious, Browse
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........K.*..*..*..R.H.*..*..*..R.M.*..R.Q.*..R.J.*..R.O.*..Rich.*.................PE..L....w,S................................. ....@..........................`......9............`..........................$0..<....@..................@...P..$...................................H...@............0..$............................text................................ ..`.data...$.... ....@ ....idata..,.....0.......................@..@.rsrc........@.......................@..@.reloc.......P......................@..B.. ....

C:\Windows\mpsvc.dll

Download File

Process:	C:\Users\user\Desktop\revil.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	808328
Entropy (8bit):	6.978893799604197
Encrypted:	false
SSDEEP:	12288:KXnKcEqGM00LJdqoHuDWeij0XukcWI9e56+5gD6QRqb/kYxFNFsX3ArTjvJjx0uA:YETDWX4XukZeVL/kYx9P/JY6gfjcs
MD5:	A47CF00AEDF769D60D58BFE00C0B5421
SHA1:	656C4D285EA518D90C1B669B79AF475DB31E30B1
SHA-256:	8DD620D9AEB35960BB766458C8890EDE987C33D239CF730F93FE49D90AE759DD
SHA-512:	4C2DCAD3BD478FA70D086B7426D55976CAA7FFC3D120C9C805CBB49EAE910123C496BF2356066AFCACBA12BA05C963BBB8D95ED7F548479C90FEC57AA16E4637
Malicious:	**true**
Yara Hits:	• Rule: APT_MAL_REvil_Kaseya_Jul21_2, Description: Detects malware used in the Kaseya supply chain attack, Source: C:\Windows\mpsvc.dll, Author: Florian Roth
Antivirus:	• Antivirus: Metadefender, Detection: 17%, Browse • Antivirus: ReversingLabs, Detection: 30%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........x.............HU.....Hk.....HT.|...T.T.....a'.............KU......Kh......Kj.....Rich............PE..L...j..`...........! .........h............... ........................................[....@.....................................P....................>.......0...a..................................P...@............ ..h............................text...B............................ ..`.rdata..d.... ....@..@.data....\....... ....@....reloc...a...0...b..................@..B.. ....

C:\z4ra2w5g-readme.txt

Download File

Process:	C:\Windows\MsMpEng.exe
File Type:	data
Category:	dropped
Size (bytes):	6928
Entropy (8bit):	3.8723818356503363
Encrypted:	false
SSDEEP:	192:oHLyQ3jjZUu5jGN42sTKthBLvJbyDycD8hc:iSuau2sTEhBrJb+ycD8hc
MD5:	F8E45B4CB92153FBFB52B8DA885CA1DE
SHA1:	8F741D58CFB91E43D7E9F156D1008593DE73C6E3
SHA-256:	D15544EB68334A39D904CFB0C020E848FD38D2F49DDDB9E172EF26F59DDD998E
SHA-512:	4B1819E4E67535BE656905CF1BD0E90108352FFE27D32F0591E58FD8DE92F211C52FC631FF1A8DD04B035C104448A8D31C43821E91F21D3F2615FEE1D0934EC7
Malicious:	**true**
Preview:	-.-.-.=.=.=. .W.e.l.c.o.m.e... .A.g.a.i.n... .=.=.=.-.-.-.........[.-.]. .W.h.a.t.s. .H.a.p.P.e.n.?. .[.-.].........Y.o.u.r. .f.i.l.e.s. .a.r.e. .e.n.c.r.y.p.t.e.d.,. .a.n.d. .c.u.r.r.e.n.t.l.y. .u.n.a.v.a.i.l.a.b.l.e... .Y.o.u. .c.a.n. .c.h.e.c.k. . i.t.:. .a.l.l. .f.i.l.e.s. .o.n. .y.o.u.r. .s.y.s.t.e.m. .h.a.s. .e.x.t.e.n.s.i.o.n. .z.4.r.a.2.w.5.g.......B.y. .t.h.e. .w.a.y.,. .e.v.e.r.y.t.h.i.n.g. .i.s. .p.o.s.s.i.b.l.e. .t.o. .r.e.c.o.v.e.r. .(.r.e.s.t.o.r.e.).,. .b.u.t. .y.o.u. .n.e.e.d. .t.o. .f.o.l.l.o.w. .o.u.r. .i.n.s.t.r.u.c.t.i.o.n.s... .O.t.h.e.r.w.i.s.e.,. .y.o.u. .c.a.n.t. .r.e.t.u.r.n. .y.o.u.r. .d.a.t.a. .(.N.E.V.E.R.)..........[.+.]. .W.h.a.t. .g.u.a.r.a.n.t.e.e.s.?. .[.+.].........I.t.s. .j.u.s.t. .a. .b.u.s.i.n.e.s.s... .W.e. .a.b.s.o.l.u.t.e.l.y. .d.o. .n.o.t. .c.a.r.e. .a.b.o.u.t. .y.o.u. .a.n.d. .y.o.u.r. .d.e.a.l.s.,. .e.x.c.e.p.t. .g.e.t.t.i.n.g. .b.e.n.e.f.i.t.s... .I.f. .w.e. .d.o. .n.o.t. .d.o. .o.u.r. .w.o.r.k. .a.n.d. .l.i.a.b.i.l.i.t.i.e.s. .-. .n.o.b.o.d.

\Device\ConDrv

Download File

Process:	C:\Windows\SysWOW64\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	4.106890595608519
Encrypted:	false
SSDEEP:	3:jMs/yha:jMUma
MD5:	78890DD69B4AB45F912760EC5EA2AED1
SHA1:	050994B6DB3BC0103A5320BAE25F21DAEF677A5E
SHA-256:	803AF0F87EF5899F1FA217B97B50BCC360E5DA596B24F5449779945BAEF35285
SHA-512:	45B2FCA2AB032F03F40C4ED30F25AB0606A86AB06BE0161122453E74B623D40254E7697E13F29FCCC658588AF4C25C9388DFBC2293D25678B712341582D170D0
Malicious:	false
Preview:	..Updated 52 rule(s)...Ok.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.952255719094324
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	revil.exe
File size:	912264
MD5:	561cffbaba71a6e8cc1cdceda990ead4
SHA1:	5162f14d75e96edb914d1756349d6e11583db0b0
SHA256:	d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e
SHA512:	09149b9825db2c9e6d2ec6665abc64b0b7aaafaa47c921c5bf0062cd7bedd1fc64cf54646a098f45fc4b930f5fbecee586fe839950c9135f64ea722b00baa50e
SSDEEP:	24576:vMz7ETDWX4XukZeVL/kYx9P/JY6gfjcsAE:kfF7k4pB/JYPIsAE
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..............G...G...G...F...G...F...G...F...G... F...G...F...G...F...G...F...G...G...GE..F...GE.~G...GE..F...GRich...G...............

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4013ef
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60DDB7BD [Thu Jul 1 12:40:29 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	59349b1648eddf021c01f05a17a0e870

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file**
Error Number:	-2146762495
Not Before, Not After	• 4/29/2021 2:00:00 AM 4/30/2022 1:59:59 AM
Subject Chain	• CN=PB03 TRANSPORT LTD., O=PB03 TRANSPORT LTD., L=Brampton, S=Ontario, C=CA
Version:	3
Thumbprint MD5:	786FE71031A7CE560DCE51D45EEAF576
Thumbprint SHA-1:	11FF68DA43F0931E22002F1461136C662E623366
Thumbprint SHA-256:	6A937953F7F2527D40C5264D24E3AADBC39348577FABCE82AC71D7D3EF01EF16
Serial:	119ACEAD668BAD57A48B4F42F294F8F0

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb072	0xb200	False	0.590919066011	data	6.62319495618	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x59f0	0x5a00	False	0.419921875	data	4.86045729034	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x13000	0x1410	0xa00	False	0.1390625	DOS executable (block device driver \277DN)	1.81174628065	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x15000	0xcab18	0xcac00	False	0.594584473258	data	6.98948797117	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe0000	0xe04	0x1000	False	0.692626953125	data	6.12011193404	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

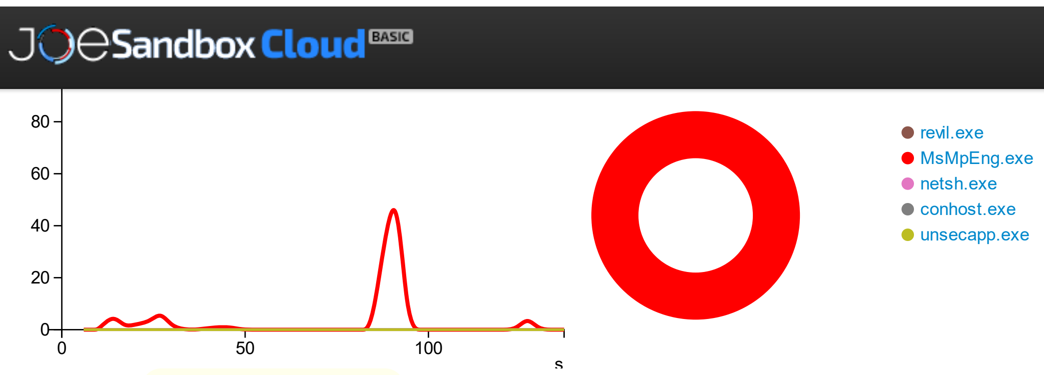
Network Behavior

No network behavior found

Code Manipulations

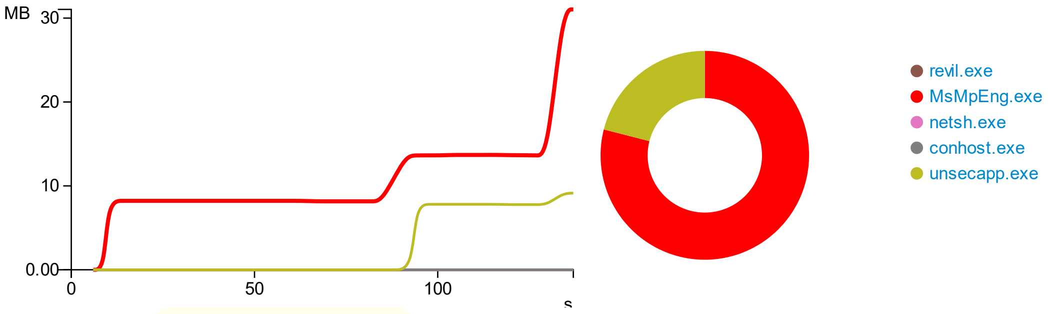
Statistics

CPU Usage



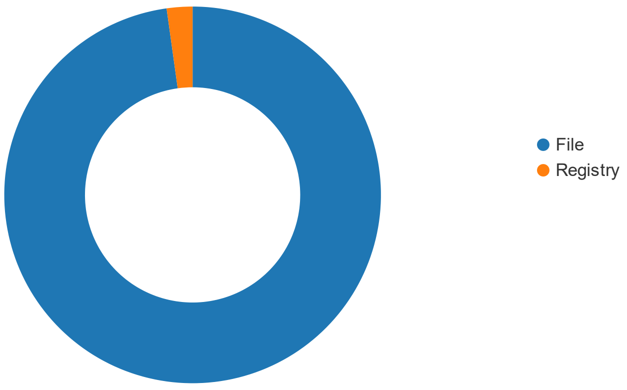
Click to jump to process

Memory Usage



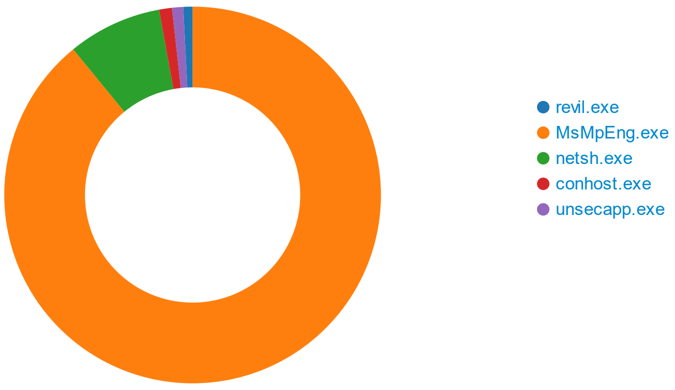
Click to jump to process

High Level Behavior Distribution



Click to dive into process behavior distribution

Behavior



Click to jump to process

System Behavior

Analysis Process: revil.exe PID: 6960 Parent PID: 5904

Function Logs

General

Start time:	07:48:09
Start date:	03/07/2021
Path:	C:\Users\user\Desktop\revil.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\revil.exe'
Imagebase:	0x160000
File size:	912264 bytes
MD5 hash:	561CFFBABA71A6E8CC1CDCEDA990EAD4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Created

File Written

Section Activities Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities Show Windows behavior

Process Activities Show Windows behavior

Process Created

Process Terminated

Thread Activities Show Windows behavior

Memory Activities Show Windows behavior

Memory Allocated

System Activities Show Windows behavior

LPC Port Activities Show Windows behavior

Chronological Activities

Analysis Process: MsMpEng.exe PID: 6972 Parent PID: 6960

Function Logs

General

Start time:	07:48:10
Start date:	03/07/2021
Path:	C:\Windows\MsMpEng.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\MsMpEng.exe
Imagebase:	0xb20000
File size:	22224 bytes
MD5 hash:	8CC83221870DD07144E63DF594C391D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MAL_RANSOM_REvil_Oct20_1, Description: Detects REvil ransomware, Source: 00000001.00000002.917270010.0000000000F60000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_RANSOM_REvil_Oct20_1, Description: Detects REvil ransomware, Source: 00000001.00000002.917636237.00000000029A0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Sodinokibi, Description: Yara detected Sodinokibi Ransomware, Source: 00000001.00000003.649759193.00000000033F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Sodinokibi, Description: Yara detected Sodinokibi Ransomware, Source: 00000001.00000003.650121407.00000000033F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Sodinokibi, Description: Yara detected Sodinokibi Ransomware, Source: 00000001.00000003.649936181.00000000033F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Sodinokibi, Description: Yara detected Sodinokibi Ransomware, Source: 00000001.00000003.649851083.00000000033F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Sodinokibi, Description: Yara detected Sodinokibi Ransomware, Source: 00000001.00000003.649708286.00000000033F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Sodinokibi, Description: Yara detected Sodinokibi Ransomware, Source: 00000001.00000003.650242625.00000000033F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Sodinokibi, Description: Yara detected Sodinokibi Ransomware, Source: 00000001.00000003.650215316.00000000033F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Sodinokibi, Description: Yara detected Sodinokibi Ransomware, Source: 00000001.00000003.823910328.00000000033F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Sodinokibi, Description: Yara detected Sodinokibi Ransomware, Source: 00000001.00000003.649804113.00000000033F8000.00000004.00000040.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Opened

File Created

File Moved

File Written

File Read

File Attributes Queried

Other File Operations

Volume Information Queried

Section Activities

Sections loaded by Program

Registry Activities — Show Windows behavior

Key Opened

Key Created

Key Value Created

Key Value Queried

COM Activities — Show Windows behavior

WMI Operations

Mutex Activities — Show Windows behavior

Mutex Created

Process Activities — Show Windows behavior

Process Created

Process Information Set

Thread Activities — Show Windows behavior

Thread Created

Thread Delayed

Thread Information Set

Memory Activities — Show Windows behavior

Memory Allocated

Memory Usage Statistics

System Activities — Show Windows behavior

System Information Queried

Timing Activities — Show Windows behavior

Windows UI Activities — Show Windows behavior

Process Token Activities — Show Windows behavior

Object Security Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: netsh.exe PID: 5964 Parent PID: 6972

Function Logs

General

Start time:	07:49:32
Start date:	03/07/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh advfirewall firewall set rule group='Network Discovery' new enable=Yes
Imagebase:	0x9f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Written

Sections loaded by Windows

Sections loaded by Program

Registry Activities Show Windows behavior

Mutex Activities Show Windows behavior

Process Activities Show Windows behavior

Thread Activities Show Windows behavior

Thread Information Set

Memory Activities Show Windows behavior

Memory Usage Statistics

System Activities Show Windows behavior

Windows UI Activities Show Windows behavior

LPC Port Activities Show Windows behavior

Chronological Activities

Analysis Process: conhost.exe PID: 1424 Parent PID: 5964

Function Logs

General

Start time:	07:49:33
Start date:	03/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Attributes Queried

Volume Information Queried

Section Activities Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities Show Windows behavior

Mutex Activities Show Windows behavior

Mutex Created

Process Activities Show Windows behavior

Thread Activities Show Windows behavior

Thread Created

Thread Delayed

Memory Activities Show Windows behavior

Memory Usage Statistics

System Activities Show Windows behavior

Windows UI Activities Show Windows behavior

Window UI Enumerated

Message Posted to Windows UI

Window UIs Event Hook Set

LPC Port Activities Show Windows behavior

Chronological Activities

Analysis Process: unsecapp.exe PID: 5948 Parent PID: 800

Function Logs

General

Start time:	07:49:33
Start date:	03/07/2021
Path:	C:\Windows\System32\wbem\unsecapp.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\unsecapp.exe -Embedding
Imagebase:	0x7ff6809a0000
File size:	48640 bytes
MD5 hash:	9CBD3EC8D9E4F8CE54258B0573C66BEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Section Activities Show Windows behavior

Sections loaded by Windows

Registry Activities Show Windows behavior

Mutex Activities Show Windows behavior

Process Activities Show Windows behavior

Thread Activities Show Windows behavior

Thread Information Set

Memory Activities Show Windows behavior

Memory Usage Statistics

System Activities Show Windows behavior

Timing Activities Show Windows behavior

Windows UI Activities Show Windows behavior

LPC Port Activities Show Windows behavior

Chronological Activities

Disassembly

Code Analysis

Analysis Process: revil.exe PID: 6960 Parent PID: 5904 revil.exe COMMON

Executed Functions

Function 001610F2, Relevance: 19.3, APIs: 7, Strings: 4, Instructions: 57 HDC PROCESS COMMON Download Yara Rule

Function 00163CFC, Relevance: 4.5, APIs: 3, Instructions: 20 HDC COMMON Download Yara Rule

Function 001618F4, Relevance: 1.5, APIs: 1, Instructions: 3 HDC COMMON Download Yara Rule

Function 00165FD1, Relevance: .0, Instructions: 22 HDC COMMON Download Yara Rule

Function 00166CBB, Relevance: 10.6, APIs: 4, Strings: 2, Instructions: 77 HDC COMMON Download Yara Rule

Function 00168410, Relevance: 4.7, APIs: 3, Instructions: 199 HDC COMMON Download Yara Rule

Function 00165EE1, Relevance: 4.5, APIs: 3, Instructions: 37 HDC COMMON Download Yara Rule

Function 0016575F, Relevance: 3.6, APIs: 1, Strings: 1, Instructions: 127 HDC COMMON Download Yara Rule

Function 00165AF4, Relevance: 3.2, APIs: 2, Instructions: 166 HDC COMMON Download Yara Rule

Function 001658E0, Relevance: 3.1, APIs: 2, Instructions: 100 HDC COMMON Download Yara Rule

Function 00166F8F, Relevance: 3.0, APIs: 2, Instructions: 34 HDC COMMON Download Yara Rule

Function 00166D82, Relevance: 1.6, APIs: 1, Instructions: 57 HDC COMMON Download Yara Rule

Function 00166002, Relevance: 1.6, APIs: 1, Instructions: 52 HDC COMMON Download Yara Rule

Function 00164FC8, Relevance: 1.5, APIs: 1, Instructions: 39 HDC MEMORY COMMON Download Yara Rule

Function 0016672E, Relevance: 1.5, APIs: 1, Instructions: 32 HDC MEMORY COMMON Download Yara Rule

Non-executed Functions

Function 00164C12, Relevance: 4.6, APIs: 3, Instructions: 77 HDC COMMON Download Yara Rule

Function 0016B16D, Relevance: 1.8, APIs: 1, Instructions: 274 HDC COMMON CRYPTO Download Yara Rule

Function 00161A1B, Relevance: 1.6, APIs: 1, Instructions: 139 HDC COMMON Download Yara Rule

Function 0016529F, Relevance: 1.6, APIs: 1, Instructions: 108 HDC COMMON Download Yara Rule

Function 001670EB, Relevance: 1.3, APIs: 1, Instructions: 5 HDC MEMORY COMMON Download Yara Rule

Function 0016696A, Relevance: 19.6, APIs: 13, Instructions: 113 HDC COMMON Download Yara Rule

Function 001648A8, Relevance: 15.1, APIs: 10, Instructions: 69 HDC COMMON Download Yara Rule

Function 00161D60, Relevance: 10.6, APIs: 5, Strings: 1, Instructions: 120 HDC COMMON Download Yara Rule

Function 00166626, Relevance: 10.6, APIs: 7, Instructions: 65 HDC COMMON Download Yara Rule

Function 001688D8, Relevance: 9.3, APIs: 6, Instructions: 318 HDC FILE COMMON Download Yara Rule

Function 0016235E, Relevance: 9.1, APIs: 6, Instructions: 60 HDC COMMON Download Yara Rule

Function 001625EE, Relevance: 8.8, APIs: 4, Strings: 1, Instructions: 68 HDC COMMON Download Yara Rule

Function 00163D3E, Relevance: 8.8, APIs: 3, Strings: 2, Instructions: 30 HDC LIBRARY LOADER COMMON Download Yara Rule

Function 00166585, Relevance: 7.5, APIs: 5, Instructions: 40 HDC COMMON Download Yara Rule

Function 0016355E, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 121 HDC COMMON Download Yara Rule

Function 001649C0, Relevance: 6.1, APIs: 4, Instructions: 72 HDC COMMON Download Yara Rule

Function 00164B17, Relevance: 6.1, APIs: 4, Instructions: 69 HDC COMMON Download Yara Rule

Function 00169DC6, Relevance: 6.0, APIs: 4, Instructions: 29 HDC COMMON Download Yara Rule

Function 00164382, Relevance: 6.0, APIs: 4, Instructions: 19 HDC COMMON Download Yara Rule

Analysis Process: MsMpEng.exe PID: 6972 Parent PID: 6960 MsMpEng.exe COMMON

Executed Functions

Function 029A7FC1, Relevance: 10.6, APIs: 7, Instructions: 59 THREAD PROCESS COMMON Download Yara Rule

Function 029A8122, Relevance: 6.2, APIs: 4, Instructions: 193 COMMON Download Yara Rule

Function 029A61C8, Relevance: 6.0, APIs: 4, Instructions: 12 TIME SLEEP COMMON Download Yara Rule

Function 029A5508, Relevance: 5.3, APIs: 2, Strings: 1, Instructions: 90 COMMON Download Yara Rule

Function 029A423B, Relevance: 4.6, APIs: 3, Instructions: 92 SERVICE COMMON Download Yara Rule

Function 029A79F8, Relevance: 4.6, APIs: 3, Instructions: 71 MEMORY COMMON Download Yara Rule

Function 029A5B96, Relevance: 3.0, APIs: 2, Instructions: 46 ENCRYPTION COMMON Download Yara Rule

Function 029A58B4, Relevance: 1.5, APIs: 1, Instructions: 26 COMMON Download Yara Rule

Function 029A5AEB, Relevance: 1.5, APIs: 1, Instructions: 10 COMMON Download Yara Rule

Function 6D4C10E0, Relevance: .0, Instructions: 16 COMMON Download Yara Rule

Function 029A2809, Relevance: 44.1, APIs: 19, Strings: 6, Instructions: 344 STRING COMMON Download Yara Rule

Function 029A2BB5, Relevance: 19.5, APIs: 10, Strings: 1, Instructions: 246 COMMON Download Yara Rule

Function 029A3FAE, Relevance: 15.2, APIs: 10, Instructions: 243 COMMON Download Yara Rule

Function 029A3DB7, Relevance: 13.6, APIs: 9, Instructions: 103 THREAD PROCESS COMMON Download Yara Rule

Function 029A38F7, Relevance: 10.7, APIs: 7, Instructions: 211 COMMON Download Yara Rule

Function 029A86E6, Relevance: 7.6, APIs: 5, Instructions: 139 COMMON Download Yara Rule

Function 6D4C11B0, Relevance: 7.6, APIs: 5, Instructions: 70 HDC THREAD COMMON Download Yara Rule

Function 029A47D8, Relevance: 7.0, APIs: 2, Strings: 2, Instructions: 48 WINDOW COMMON Download Yara Rule

Function 029A351E, Relevance: 6.2, APIs: 4, Instructions: 160 COMMON Download Yara Rule

Function 029A8584, Relevance: 6.1, APIs: 4, Instructions: 127 SHARE COMMON Download Yara Rule

Function 029A5CB3, Relevance: 6.1, APIs: 4, Instructions: 57 REGISTRY COMMON Download Yara Rule

Function 029A5DCD, Relevance: 6.1, APIs: 4, Instructions: 54 SERVICE COMMON Download Yara Rule

Function 029A7CB3, Relevance: 6.0, APIs: 4, Instructions: 48 COMMON Download Yara Rule

Function 029A8441, Relevance: 6.0, APIs: 4, Instructions: 24 FILE COMMON Download Yara Rule

Function 029A7B9D, Relevance: 4.6, APIs: 3, Instructions: 50 COMMON Download Yara Rule

Function 029A5B1F, Relevance: 4.5, APIs: 3, Instructions: 46 PROCESS COMMON Download Yara Rule

Function 029A5D32, Relevance: 4.5, APIs: 3, Instructions: 36 REGISTRY COMMON Download Yara Rule

Function 00B210E1, Relevance: 4.5, APIs: 3, Instructions: 9 HDC COMMON Download Yara Rule

Function 029A8482, Relevance: 3.6, APIs: 1, Strings: 1, Instructions: 90 COMMON Download Yara Rule

Function 029A5DBD, Relevance: 3.5, APIs: 1, Strings: 1, Instructions: 5 COMMON Download Yara Rule

Function 6D4C1000, Relevance: 3.1, APIs: 2, Instructions: 69 HDC MEMORY COMMON Download Yara Rule

Function 029A32A5, Relevance: 3.1, APIs: 2, Instructions: 57 FILE COMMON Download Yara Rule

Function 029A7EA3, Relevance: 3.0, APIs: 2, Instructions: 45 THREAD COMMON Download Yara Rule

Function 029A59CE, Relevance: 3.0, APIs: 2, Instructions: 32 SYNCHRONIZATION COMMON Download Yara Rule

Function 029A59CD, Relevance: 3.0, APIs: 2, Instructions: 32 SYNCHRONIZATION COMMON Download Yara Rule

Function 029A7C36, Relevance: 3.0, APIs: 2, Instructions: 29 COMMON Download Yara Rule

Function 6D4C1290, Relevance: 3.0, APIs: 2, Instructions: 23 SLEEP THREAD COMMON Download Yara Rule

Function 029A5174, Relevance: 3.0, APIs: 2, Instructions: 23 MEMORY COMMON Download Yara Rule

Function 029A510A, Relevance: 3.0, APIs: 2, Instructions: 17 MEMORY COMMON Download Yara Rule

Function 029A1E18, Relevance: 1.6, APIs: 1, Instructions: 139 COMMON Download Yara Rule

Function 029A3B70, Relevance: 1.6, APIs: 1, Instructions: 120 COMMON Download Yara Rule

Function 029A5777, Relevance: 1.6, APIs: 1, Instructions: 59 COMMON Download Yara Rule

Function 029A3D31, Relevance: 1.6, APIs: 1, Instructions: 51 COMMON Download Yara Rule

Function 029A3CBA, Relevance: 1.5, APIs: 1, Instructions: 44 COMMON Download Yara Rule

Function 029A7F01, Relevance: 1.5, APIs: 1, Instructions: 42 COMMON Download Yara Rule

Function 029A3887, Relevance: 1.5, APIs: 1, Instructions: 39 COMMON Download Yara Rule

Function 029A5FD5, Relevance: 1.5, APIs: 1, Instructions: 32 COMMON Download Yara Rule

Function 029A7E1F, Relevance: 1.5, APIs: 1, Instructions: 16 COMMON Download Yara Rule

Function 029A834D, Relevance: 1.5, APIs: 1, Instructions: 15 FILE COMMON Download Yara Rule

Function 029A5A21, Relevance: 1.5, APIs: 1, Instructions: 12 COMMON Download Yara Rule

Function 029A80D4, Relevance: 1.5, APIs: 1, Instructions: 11 FILE COMMON Download Yara Rule

Function 029A8108, Relevance: 1.5, APIs: 1, Instructions: 11 FILE COMMON Download Yara Rule

Function 029A5133, Relevance: 1.5, APIs: 1, Instructions: 11 MEMORY COMMON Download Yara Rule

Function 029A838C, Relevance: 1.5, APIs: 1, Instructions: 10 COMMON Download Yara Rule

Function 029A83A5, Relevance: 1.5, APIs: 1, Instructions: 10 FILE COMMON Download Yara Rule

Function 029A8373, Relevance: 1.5, APIs: 1, Instructions: 10 FILE COMMON Download Yara Rule

Function 029A79B0, Relevance: 1.5, APIs: 1, Instructions: 9 LIBRARY COMMON Download Yara Rule

Function 029A515E, Relevance: 1.5, APIs: 1, Instructions: 9 MEMORY COMMON Download Yara Rule

Function 029A73E6, Relevance: 1.3, APIs: 1, Instructions: 86 COMMON Download Yara Rule

Non-executed Functions

Function 029A4EFA, Relevance: 31.7, APIs: 21, Instructions: 202 WINDOW COMMON Download Yara Rule

Function 029A532D, Relevance: 12.3, APIs: 3, Strings: 4, Instructions: 73 COMMON Download Yara Rule

Function 6D4E1810, Relevance: 7.3, APIs: 3, Strings: 1, Instructions: 345 HDC COMMON CRYPTO Download Yara Rule

Function 6D4E1440, Relevance: 5.6, APIs: 2, Strings: 1, Instructions: 306 HDC COMMON CRYPTO Download Yara Rule

Function 029A64F2, Relevance: 3.0, APIs: 2, Instructions: 44 ENCRYPTION COMMON Download Yara Rule

Function 029A5C85, Relevance: 3.0, APIs: 2, Instructions: 18 SHUTDOWN NATIVE COMMON Download Yara Rule

Function 029A5DA9, Relevance: 1.5, APIs: 1, Instructions: 9 SERVICE COMMON Download Yara Rule

Function 029A611E, Relevance: .1, Instructions: 75 COMMON Download Yara Rule

Function 6D52017C, Relevance: 22.8, APIs: 12, Strings: 1, Instructions: 84 HDC COMMON Download Yara Rule

Function 6D4C2A20, Relevance: 19.3, APIs: 9, Strings: 2, Instructions: 91 HDC REGISTRY FILE WINDOW COMMON Download Yara Rule

Function 6D4CD959, Relevance: 16.7, APIs: 11, Instructions: 186 HDC COMMON Download Yara Rule

Function 029A5E46, Relevance: 16.6, APIs: 11, Instructions: 121 COMMON Download Yara Rule

Function 6D4CA6A0, Relevance: 16.0, APIs: 5, Strings: 4, Instructions: 247 HDC COMMON Download Yara Rule

Function 029A2F04, Relevance: 15.9, APIs: 8, Strings: 1, Instructions: 189 MEMORY COMMON Download Yara Rule

Function 6D4C28E0, Relevance: 15.9, APIs: 7, Strings: 2, Instructions: 106 HDC LIBRARY LOADER COMMON Download Yara Rule

Function 6D4CD9D5, Relevance: 15.2, APIs: 10, Instructions: 165 HDC COMMON Download Yara Rule

Function 029A4C40, Relevance: 13.7, APIs: 9, Instructions: 170 FILE MEMORY COMMON Download Yara Rule

Function 6D4C69E0, Relevance: 10.7, APIs: 1, Strings: 5, Instructions: 244 HDC COMMON Download Yara Rule

Function 6D524F90, Relevance: 10.5, APIs: 7, Instructions: 45 HDC THREAD COMMON Download Yara Rule

Function 6D4CDAE9, Relevance: 9.1, APIs: 6, Instructions: 99 HDC COMMON Download Yara Rule

Function 029A4893, Relevance: 9.0, APIs: 4, Strings: 1, Instructions: 264 PROCESS COMMON Download Yara Rule

Function 6D4C16B0, Relevance: 9.0, APIs: 2, Strings: 3, Instructions: 246 HDC COMMON Download Yara Rule

Function 6D4C1D80, Relevance: 8.9, APIs: 3, Strings: 2, Instructions: 168 HDC COMMON Download Yara Rule

Function 6D52229B, Relevance: 7.7, APIs: 5, Instructions: 163 HDC COMMON Download Yara Rule

Function 6D4CAB50, Relevance: 7.6, APIs: 6, Instructions: 148 HDC COMMON Download Yara Rule

Function 6D51FFD5, Relevance: 7.6, APIs: 5, Instructions: 67 HDC COMMON Download Yara Rule

- Function 6D4CB8E0, Relevance: 7.2, APIs: 3, Strings: 1, Instructions: 161 HDC COMMON Download Yara Rule
- Function 6D4C4110, Relevance: 7.1, APIs: 1, Strings: 3, Instructions: 122 HDC COMMON Download Yara Rule
- Function 6D4C1B30, Relevance: 7.1, APIs: 2, Strings: 2, Instructions: 115 HDC COMMON Download Yara Rule
- Function 6D4D1A20, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 105 HDC COMMON Download Yara Rule
- Function 029A7D2B, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 83 COMMON Download Yara Rule
- Function 6D4C2B60, Relevance: 7.1, APIs: 1, Strings: 3, Instructions: 55 HDC COMMON Download Yara Rule
- Function 6D5268E6, Relevance: 7.0, APIs: 3, Strings: 1, Instructions: 49 HDC COMMON Download Yara Rule
- Function 6D522A1A, Relevance: 6.1, APIs: 4, Instructions: 136 HDC COMMON Download Yara Rule
- Function 6D52E403, Relevance: 6.1, APIs: 4, Instructions: 97 HDC COMMON Download Yara Rule
- Function 6D4D3FD0, Relevance: 6.1, APIs: 4, Instructions: 88 HDC COMMON Download Yara Rule
- Function 6D4D5980, Relevance: 6.1, APIs: 4, Instructions: 88 HDC COMMON Download Yara Rule
- Function 6D4CAA60, Relevance: 6.1, APIs: 1, Strings: 3, Instructions: 79 HDC COMMON Download Yara Rule
- Function 029A2E57, Relevance: 6.1, APIs: 4, Instructions: 76 MEMORY COMMON Download Yara Rule
- Function 6D527C6F, Relevance: 6.0, APIs: 4, Instructions: 48 HDC COMMON Download Yara Rule
- Function 029A52E0, Relevance: 6.0, APIs: 4, Instructions: 28 SLEEP COMMON Download Yara Rule
- Function 6D4CF260, Relevance: 5.5, APIs: 2, Strings: 1, Instructions: 201 HDC COMMON Download Yara Rule
- Function 6D4D13A0, Relevance: 5.4, APIs: 1, Strings: 2, Instructions: 177 HDC COMMON Download Yara Rule
- Function 029A337C, Relevance: 5.4, APIs: 2, Strings: 1, Instructions: 125 COMMON Download Yara Rule
- Function 6D4D1940, Relevance: 5.3, APIs: 2, Strings: 1, Instructions: 91 HDC COMMON Download Yara Rule
- Function 6D4C3820, Relevance: 5.3, APIs: 1, Strings: 2, Instructions: 69 HDC COMMON Download Yara Rule
- Function 6D4CA590, Relevance: 5.3, APIs: 2, Strings: 1, Instructions: 44 HDC COMMON Download Yara Rule

Joe Sandbox Cloud Basic 32.0.0 Black Diamond