in: *Ransomware, Win32 ransomware, Win32, and 3 more*

Hermes

Hermes is a ransomware that runs on Microsoft Windows. It was discovered by Michael Gillespie. It is aimed at English-speaking users. It is reported that this does not work for Russia, Ukraine and Belarus.

Payload

Transmission

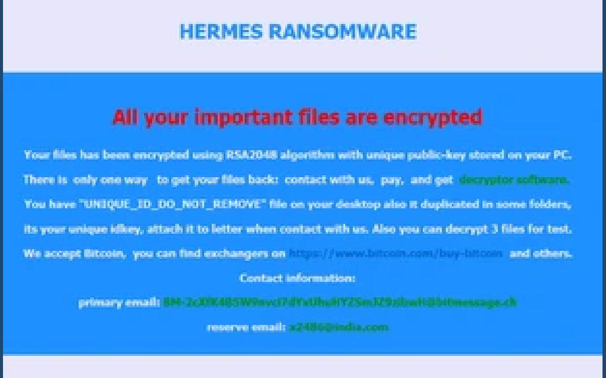
Hermes is distributed through email spam and malicious attachments, exploits, fake updates, repackaged and infected installers.

Infection

When Hermes is executed, it will also use a User Account Control, or UAC, bypass called Eleven, or Elevation by environment variable expansion, to delete a victim's Shadow Volume Copies and backup files. This bypass will allow a VBS file called Shade.vbs file to bypass User Account Control and launch with elevated privileges. This VBS file then launches a batch file called Shade.bat that is used to clear all of the

The backup images that are deleted are ones that match the following filenames:

Hermes



HERMES RANSOMWARE

All your important files are encrypted

Your files has been encrypted using RSA2048 algorithm with unique public-key stored on your PC.
There is only one way to get your files back: contact with us, pay, and get decryptor software.
You have "UNIQUE_ID_DO_NOT_REMOVE" file on your desktop also it duplicated in some folders,
its your unique idkey, attach it to letter when contact with us. Also you can decrypt 3 files for test.
We accept Bitcoin, you can find exchangers on https://www.bitcoin.com/buy-bitcoin and others.
Contact information:
primary email: BM-2cXfK4B5W9nvcl7dYxUhuHYZSmJZ9zbwH@bitmessage.ch
reserve email: x2486@india.com

Type

Ransomware, Trojan

Creator(s)

CryptoTech

Date

February 10th, 2017

Place of Origin

Russia

Microsoft Wind

File Type

```
.VHD, .bac, .bak, .wbcat, .bkf, .Backup,
.backup, .set, .win, .dsk
```

It will copy itself to C:\Users\Public\Reload.exe and execute itself. It will then launch a batch file called system_.bat, which is used to delete the original installer.

Hermes will then begin to scan a victim's computer and unmapped network shares for files that contain certain extensions and encrypt them using AES encryption. It will encrypt the following extensions:

```
.tif, .php, .accdb, .dbf, .arw, .txt, .doc,
.docm, .docx, .zip, .rar, .xlsx, .xls,
.xlsb, .xlsm, .jpg, .jpe, .jpeg, .bmp, .eql,
.sql, .adp, .mdf, .frm, .mdb, .odb, .odm,
.odp, .ods, .dbc, .frx, .dbs, .pds, .pdt,
.pdf, .cfu, .mxl, .epf, .kdbx, .erf, .vrp,
.grs, .geo, .pff, .mft, .efd, .rib, .max,
.lwo, .lws, .obj, .fbx, .dgn, .dwg, .abs,
.adn, .aft, .ahd, .alf, .ask, .awdb, .azz,
.bdb, .bib, .bnd, .bok, .btr, .bak, .cdb,
.ckp, .clkw, .cma, .crd, .dad, .daf, .dbk,
.dbt, .dbv, .dbx, .dcb, .dct, .dcx, .ddl,
.dmo, .dnc, .dqy, .dsk, .dsn, .dta, .dtsx,
.dxl, .eco, .ecx, .edb, .emd, .fcd, .fic,
.fid, .fil, .fol, .fpt, .fzb, .fzv, .gdb,
.gwi, .hdb, .his, .idc, .ihx, .itdb, .itw,
.jtx, .kdb, .lgc, .maq, .mdn, .mdt, .mrg,
.mud, .mwb, .myd, .ndf, .nsf, .nyf, .oce,
.oqy, .ora, .orx, .owc, .owg, .oyx, .pan,
.pdb, .pdm, .phm, .pnz, .pth, .pwa, .qpx,
.qry, .qvd, .rctd, .rdb, .rpd, .rsd, .sbf,
.sdb, .sdf, .spq, .sqb, .stp, .str, .tcx,
.tdt, .tmd, .trm, .udb, .usr, .vdb, .vpd,
.wdb, .wmdb, .xdb, .xld, .xlgc, .zdb, .zdc,
.cdr, .cdr3, .ppt, .pptx, .abw, .act, .aim,
.ans, .apt, .asc, .ase, .aty, .awp, .awt,
.aww, .bad, .bbs, .bdp, .bdr, .bean, .bna,
.boc, .btd, .cnm, .crwl, .cyi, .dca, .dgs,
.diz, .dne, .docz, .dot, .dotm, .dotx, .dsv,
.dvi, .eio, .eit, .emlx, .epp, .err, .etf,
.etx, .euc, .faq, .fbl, .fcf, .fdf, .fdr,
.fds, .fdt, .fdx, .fdxt, .fes, .fft, .flr,
.fodt, .gtp, .frt, .fwdn, .fxc, .gdoc, .gio,
.gpn, .gsd, .gthr, .hbk, .hht, .htc, .hwp,
.idx, .iil, .ipf, .jis, .joe, .jrtf, .kes,
.klg, .knt, .kon, .kwd, .lbt, .lis, .lit,
.lnt, .lrc, .lst, .ltr, .ltx, .lue, .luf,
.lwp, .lyt, .lyx, .man, .map, .mbox, .mell,
.min, .mnt, .msg, .mwp, .nfo, .njx, .now,
.nzb, .ocr, .odo, .odt, .ofl, .oft, .ort,
.ott, .pfs, .pfx, .pjt, .prt, .psw, .pvj,
.pvm, .pwi, .pwr, .qdl, .rad, .rft, .ris,
.rng, .rpt, .rst, .rtd, .rtf, .rtx, .run,
.rzk, .rzn, .saf, .sam, .scc, .scm, .sct,
.scw, .sdm, .sdoc, .sdw, .sgm, .sig, .sla,
.sls, .smf, .sms, .ssa, .stw, .sty, .sub,
.sxg, .sxw, .tab, .tdf, .tex, .text, .thp,
.tlb, .tmv, .tmx, .tpc, .tvj, .unx, .uof,
.uot, .upd, .utf8, .utxt, .vct, .vnt, .wbk,
.wcf, .wgz, .wpa, .wpd, .wpl, .wps, .wpt,
.wpw, .wri, .wsc, .wsd, .wsh, .wtx, .xdl,
.xlf, .xps, .xwp, .xyp, .xyw, .ybk, .yml,
.zabw, .abm, .afx, .agif, .agp, .aic, .albm,
.apd, .apm, .apng, .aps, .apx, .art, .asw,
```

Win32 PE executable (.EXE)

Aliases

Trojan-Ransom.Win32.Hermez.a(Kaspersky)

File Size

109.27 KB (111,896 Bytes)

MD5 Hash

61075faba222f97d3367866793f0907b

SHA1 Hash

cc033c3bf41550563a180444b6166515faa53c3a

SHA256 Hash

059aab1a6ac0764ff8024c8be37981d0506337909664c7b3862fc056d8c405b0

Authentihash

2504f77bf5514730023a60626445ee71d8ee4e60c18ad92ea5c8f33efc5ed43d

Imphash

ff847787dd14576ae2758ab87598c496

SSDEEP Hash

1536:9+Gy5E9sg99CxI4dqFhTfLZ8Lb1WyHVviF9k6zeEkA5YaH88C5Wa/HR:D2E9R9sxfdiqLP1a9keeEkA5YA9afR

Vhash

015046651d155az44!z

```
.bay, .bmx, .brk, .brn, .brt, .bss, .bti,
.cal, .cals, .can, .cdc, .cdg, .cimg, .cin,
.cit, .colz, .cpc, .cpd, .cpg, .cps, .cpx,
.dcr, .dds, .dgt, .dib, .djv, .djvu, .dmi,
.vue, .dpx, .wire, .drz, .dtw, .dvl, .ecw,
.eip, .exr, .fal, .fax, .fpos, .fpx, .gcdp,
.gfb, .gfie, .ggr, .gif, .gih, .gim, .spr,
.scad, .gpd, .gro, .grob, .hdp, .hdr, .hpi,
.icn, .icon, .icpr, .iiq, .info, .ipx,
.itc2, .iwi, .jas, .jbig, .jbmp, .jbr,
.jfif, .jia, .jng, .jpg2, .jps, .jpx, .jtf,
.jwl, .jxr, .kdc, .kdi, .kdk, .kic, .kpg,
.lbm, .ljp, .mac, .mbm, .mef, .mnr, .mos,
.mpf, .mpo, .mrxs, .myl, .ncr, .nct, .nlm,
.nrw, .oci, .omf, .oplc, .asy, .cdmm, .cdmt,
.cdmz, .cdt, .cgm, .cmx, .cnv, .csy, .cvg,
.cvi, .cvs, .cvx, .cwt, .cxf, .dcs, .ded,
.dhs, .dpp, .drw, .dxb, .dxf, .egc, .emf,
.eps, .epsf, .fif, .fig, .fmv, .ftn, .fxg,
.gem, .glox, .hpg, .hpgl, .hpl, .idea, .igt,
.igx, .imd, .ink, .lmk, .mgcb, .mgmf, .mgmt,
.mgmx, .mgtx, .mmat, .mat, .otg, .ovp, .ovr,
.pcs, .pfv, .plt, .vrml, .pobj, .psid, .rdl,
.scv, .ssk, .stn, .svf, .svgz, .sxd, .tlc,
.tne, .ufr, .vbr, .vec, .vml, .vsd, .vsdm,
.vsdx, .vstm, .stm, .vstx, .wpg, .vsm, .xar,
.yal, .orf, .ota, .oti, .ozb, .ozj, .ozt,
.pal, .pano, .pap, .pbm, .pcd, .pdd, .pef,
.pfi, .pgf, .pgm, .pic, .pict, .pix, .pjpg,
.pmg, .pni, .pnm, .pntg, .pop, .ppm, .prw,
.psdx, .pse, .psp, .ptg, .ptx, .pvr, .pxr,
.pza, .pzp, .pzs, .qmg, .ras, .rcu, .rgb,
.rgf, .ric, .riff, .rix, .rle, .rli, .rpf,
.rri, .rsb, .rsr, .rwl, .s2mv, .sci, .sep,
.sfc, .sfw, .skm, .sld, .sob, .spa, .spe,
.sph, .spj, .spp, .srw, .ste, .sumo, .sva,
.save, .ssfn, .tbn, .tfc, .thm, .tjp, .tpi,
.ufo, .uga, .vda, .vff, .vpe, .vst, .wbc,
.wbd, .wbm, .wbmp, .wbz, .wdp, .webp, .wpb,
.wpe, .wvl, .ysp, .zif, .cdr4, .cdr6, .cdrw,
.ddoc, .css, .pptm, .raw, .cpt, .pcx, .pdn,
.png, .psd, .tga, .tiff, .xpm, .sai, .wmf,
.ani, .flc, .fli, .mng, .smil, .svg, .mobi,
.swf, .html, .csv, .xhtm, .dat,
```

It should be noted that when Hermes encrypts a file, it does not append a new extension to the encrypted file. It will, though, add a file marker at the end of the encrypted file's contents called HERMES

While encrypting files it will create a ransom note named DECRYPT_INFORMATION.html and a file called UNIQUE_ID_DO_NOT_REMOVE in each folder that a file was encrypted. It is suspected that UNIQUE_ID_DO_NOT_REMOVE file contains the AES encryption key used to encrypt the files, which is further encrypted by a bundled RSA key. .This makes it so only the ransomware developer can decrypt this file and retrieve a victim's decryption key. The ransom note saids the following:

```
HERMES RANSOMWARE

All your important files are encrypted


Your files has been encrypted using RSA2048 algorithm with unique public-
key stored on your PC.

There is  only one way   to get your files back:  contact with us,  pay,
and get  decryptor software.

You have "UNIQUE_ID_DO_NOT_REMOVE" file on your desktop also it
```

```
duplicated in some folders,

its your unique idkey, attach it to letter when contact with us. Also you
can decrypt 3 files for test.

We accept Bitcoin,  you can find exchangers on
https://www.bitcoin.com/buy-bitcoin  and others.


Contact information:

primary email: BM-2cXfK4B5W9nvci7dYxUhuHYZSmJZ9zibwH@bitmessage.ch

reserve email: x2486@india.com
```

Removal

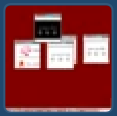
While analyzing the Hermes sample, Fabian found that the seed used to generate the encryption key could be attacked in order to create a decryptor. Once this was determined, Fabian displayed how this knowledge could be used to generate a key and a subsequent decryptor for encrypted files.

Categories: Ransomware | Win32 ransomware | Win32 | Win32 trojan | Microsoft Windows | Trojan

Popular Pages

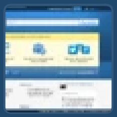
The Journey of Ahsoka Tano So Far

Fandom



You Are An Idiot

Goggle



Adf.ly

MEMZ

Recent Wiki Activity

Maestro MP3
RojasGorePlex7770 • 9 hours ago

616
RojasGorePlex7770 • 13 hours ago

Earthquake
RojasGorePlex7770 • 13 hours ago

Softonic
RojasGorePlex7770 • 13 hours ago

Help us grow Malware Wiki! GET STARTED

wikia.org