Chaos ransomware v4

brianstadnicki.github.io/posts/malware-chaos-ransomware-v4/

Brian Stadnicki February 14, 2022

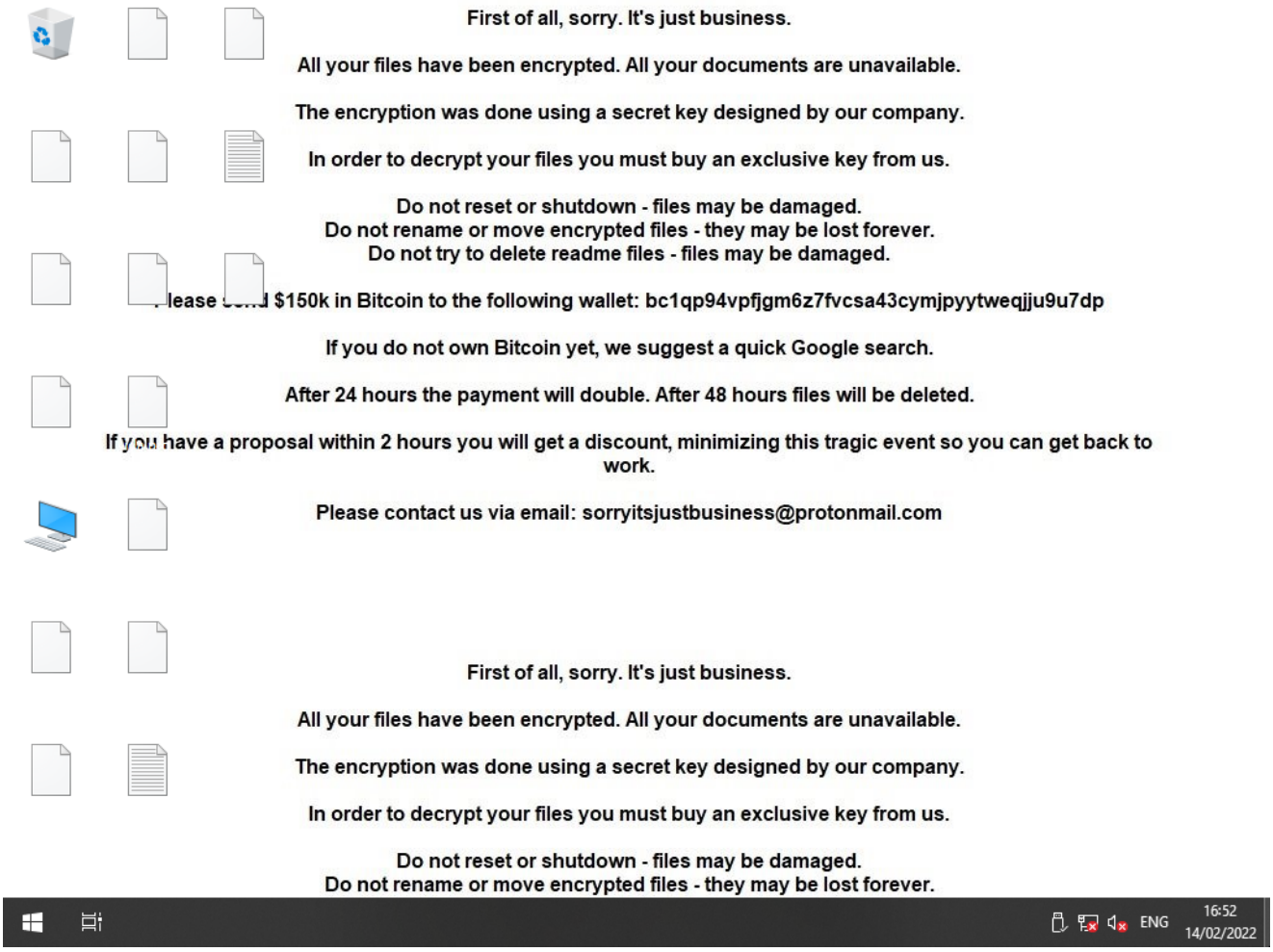
Contents

Brian Stadnicki included in malware analysis
2022-02-14 618 words 3 minutes

Contents

The chaos ransomware is fairly new, first appearing in June 2021 as a builder, offered on multiple darknet forums and marketplaces. It doesn't appear to have been involved in any significant incidents yet, a few minecraft players don't count. Unsurprisingly therefore, the sample has not had a single transaction to the wallet.

It isn't very complicated, as likely a simple proof-of-concept ransomware. Simply a 32bit .NET executable, with the ransom wallpaper base64 encoded in and completely unobfuscated with names.



Analysis

The execution process is as follows:

- Make sure only copy running
- If not running from the temp folder, wait 10 seconds (anti-virus evasion)
- If not running as admin, copy itself to the roaming folder and run
- Add itself to the startup folder
- Delete itself, copy itself to the roaming folder and run
- Look for directories to encrypt (drives other than C:\ and common user directories)
- Recursively encrypt the files with the correct file extension and add a random file extension
    - 2.2mb are AES encrypted
    - Over 200mb are partly overwritten with random bytes
    - Inbetween are randomly overwritten
    - Write a ransom note read_it.txt to the directory

- If running as admin
  - Delete backups
  - Disable recovery modes
  - Delete backup catalog (record of where backups are)
- Spread to external drives by copying itself to drives which aren't C:\
- Drop the ransom message and open in notepad
- Set the wallpaper
- Change any bitcoin addresses in the clipboard

IOC

Sample: d9771a04128e50870a96bc7ac8605982205011b723810a04a3411a1ac7eba05d

Names:

- surprise.exe
- svchost.exe
- read_it.txt

Ransom message:

```
First of all, sorry. It's just business.

All your files have been encrypted. All your documents are unavailable.

The encryption was done using a secret key designed by our company.

In order to decrypt your files you must buy an exclusive key from us.

Do not reset or shutdown - files may be damaged.
Do not rename or move encrypted files - they may be lost forever.
Do not try to delete readme files - files may be damaged.

Please send $150k in Bitcoin to the following wallet:
bc1qp94vpfjgm6z7fvcsa43cymjpyytweqjju9u7dp

If you do not own Bitcoin yet, we suggest a quick Google search.

After 24 hours the payment will double. After 48 hours files will be deleted.

If you have a proposal within 2 hours you will get a discount, minimizing this tragic
event so you can get back to work.

Please contact us via email: sorryitsjustbusiness@protonmail.com
```

File extensions infected:

.txt, .jar, .dat, .contact, .settings, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .mka, .mhtml, .oqy, .png, .csv, .py, .sql, .mdb, .php, .asp, .aspx, .html, .htm, .xml, .psd, .pdf, .xla, .cub, .dae, .indd, .cs, .mp3, .mp4, .dwg, .zip, .rar, .mov, .rtf, .bmp, .mkv, .avi, .apk, .lnk, .dib, .dic, .dif, .divx, .iso, .7zip, .ace, .arj, .bz2, .cab, .gzip, .lzh, .tar, .jpeg, .xz, .mpeg, .torrent, .mpg, .core, .pdb, .ico, .pas, .db, .wmv, .swf, .cer, .bak, .backup, .accdb, .bay, .p7c, .exif, .vss, .raw, .m4a, .wma, .flv, .sie, .sum, .ibank, .wallet, .css, .js, .rb, .crt, .xlsm, .xlsb, .7z, .cpp, .java, .jpe, .ini, .blob, .wps, .docm, .wav, .3gp, .webm, .m4v, .amv, .m4p, .svg, .ods, .bk, .vdi, .vmdk, .onepkg, .accde, .jsp, .json, .gif, .log, .gz, .config, .vb, .m1v, .sln, .pst, .obj, .xlam, .djvu, .inc, .cvs, .dbf, .tbi, .wpd, .dot, .dotx, .xltx, .pptm, .potx, .potm, .pot, .xlw, .xps, .xsd, .xsf, .xsl, .kmz, .accdr, .stm, .accdt, .ppam, .pps, .ppsm, .1cd, .3ds, .3fr, .3g2, .accda, .accdc, .accdw, .adp, .ai, .ai3, .ai4, .ai5, .ai6, .ai7, .ai8, .arw, .ascx, .asm, .asmx, .avs, .bin, .cfm, .dbx, .dcm, .dcr, .pict, .rgbe, .dwt, .f4v, .exr, .kwm, .max, .mda, .mde, .mdf, .mdw, .mht, .mpv, .msg, .myi, .nef, .odc, .geo, .swift, .odm, .odp, .oft, .orf, .pfx, .p12, .pl, .pls, .safe, .tab, .vbs, .xlk, .xlm, .xlt, .xltm, .svgz, .slk, .tar.gz, .dmg, .ps, .psb, .tif, .rss, .key, .vob, .epsp, .dc3, .iff, .onepkg, .onetoc2, .opt, .p7b, .pam, .r3d