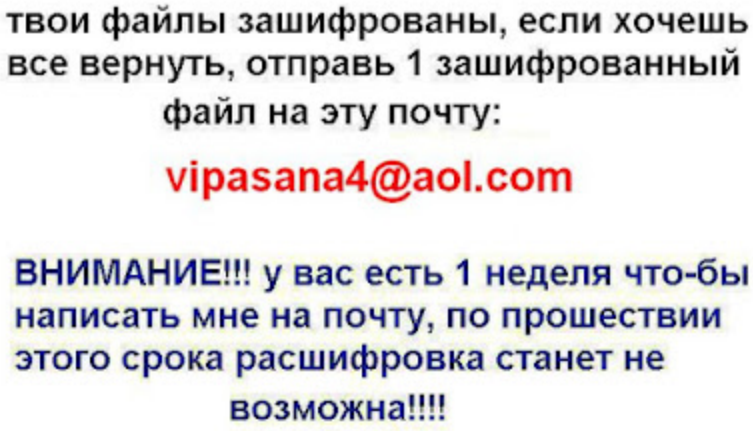
Vipasana ransomware new ransom on the block

bartblaze.blogspot.com/2016/02/vipasana-ransomware-new-ransom-on-block.html

Yet another ransomware is going around (since at least the 20th of December), which I've dubbed **Vipasana ransomware** due to where you need to send your encrypted files to:



Message in Russian, you need to mail vipasana4@aol.com to get your files back

The name may be derived from Vipassanā or 'insight meditation'.

The message in Russian reads:

> твои файлы зашифрованы, если хочешь
> все вернуть, отправь 1 зашифрованный файл на эту почту:
>
> vipasana4@aol.com
>
> ВНИМАНИЕ!!! у вас есть 1 неделя что-бы написать мне на почту, по прошествии этого срока расшифровка станет не возможна!!!!

Translated:

> *Your files are encrypted, if you want them all returned,*
> *send 1 encrypted file to this email:*
>
> *vipasana4@aol.com*
>
> *ATTENTION!!! you have 1 week to send the email, after*
> *this deadline decryption will not be possible !!!!*

It seems these ransomware authors first want you to send an email before requiring any other action, rather than immediately (or in a certain timeframe) paying Bitcoins to get your files back. In this sense, their technique is novel. Instead of the usual 24/48/72h to pay up, they give you a week.

Do not be fooled: this does **not** make them 'good guys' in any way, they encrypted your files and as such are criminals.

Search results for vipasana4@aol.com are non-existent, with the exception of one victim hit by this ransomware:

Email addresses used in this specific ransomware campaign:
johnmen.24@aol.com
vipasana4@aol.com

Files will be encrypted and renamed following below naming convention:
email-vipasana4@aol.com.ver-CL 1.2.0.0.id-[ID]-[DATE-TIME].randomname-[RANDOM].[XYZ].CBF

Where [XYZ] is also a random 'extension', the real extension is **.cbf**

ver-CL 1.2.0.0 may refer to the version number of the ransomware, indicating there are older versions as well.

Targeted file extensions:

> *.r3d, .rwl, .rx2, .p12, .sbs, .sldasm, .wps, .sldprt, .odc, .odb, .old, .nbd, .nx1, .nrw, .orf, .ppt, .mov, .mpeg, .csv, .mdb, .cer, .arj, .ods, .mkv, .avi, .odt, .pdf, .docx, .gzip, .m2v, .cpt, .raw, .cdr, .cdx, .1cd, .3gp, .7z, .rar, .db3, .zip, .xlsx, .xls, .rtf, .doc, .jpeg, .jpg, .psd, .zip, .ert, .bak, .xml, .cf, .mdf, .fil, .spr, .accdb, .abf, .a3d, .asm, .fbx, .fbw, .fbk, .fdb, .fbf, .max, .m3d, .dbf, .ldf, .keystore, .iv2i, .gbk, .gho, .sn1, .sna, .spf, .sr2, .srf, .srw, .tis, .tbl, .x3f, .ods, .pef, .pptm, .txt, .pst, .ptx, .pz3, .mp3, .odp, .qic, .wps*

I have sent over all necessary files to the good people over at Bleeping Computer, as there may be a way to recover files. If so, I will update this post.

Update - 12/02: thanks to a tweet from Catalin this appears to be another version of so called "offline" ransomware, discovered by Check Point:
“Offline” Ransomware Encrypts Your Data without C&C Communication

Note this is in fact a Cryakl variant.

Unfortunately, there doesn't appear to be a way to recover your files once encrypted. Your best best in trying to recover files is using a tool like Shadow Explorer, which will check if you can restore files using 'shadow copies' or 'shadow volume copies'.

If that doesn't work, you may try using a data recovery program such as PhotoRec or Recuva

Conclusion

Ransomware is, unfortunately, long from gone. Almost each week or month, new variants or totally new strains of ransomware are popping up. In this way, the first and foremost rule is:

Create (regular) backups!

For more prevention advise, see here.

You may also find a list of Indicators of Compromise (IOCs; hashes, domains, ...) over at AlienVault:
Vipasana ransomware