CryptoLocker

–

Retour d'expérience …

(20/05/2014)

Kesako

- Rançongiciel
- Windows
- Via mail / PJ
- Chiffre les fichiers, locaux & réseau

Exec. – 1/4

- Email + Trojan.Zbot ⇒ download Trojan.Cryptolocker
  - file: Jcgnbunudberrr.zip (⇒ Jcgnbunudberrr.exe), Lmpjxmvheortt, Icmcobxksjghdlnnt, …
  - site: xeogrhxquuubt.com, qaaepodedahnslq.org, ovenbdjnihhdlb.net, ...
- .EXE ⋯ « Mes Documents »
  - nom de fichier « random »
- HKEY_CURRENT_USER\…\Run
  CryptoLocker = %appdata%\{CLSID}.exe
  - XOR key 0x819C33AE (par ex. pour VersionInfo dans le registre)

http://blog.emsisoft.com/2013/09/10/cryptolocker-a-new-ransomware-variant/
http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware

Exec. – 2/4

- DGA – Domain Generation Algorithm

```
Key = Temp ^ (Temp >> 0x12)
⇒ NewKey = (((Key * 0x10624DD3) >> 6) * 0xFFFFFC18) + Key
CurrentDay = GetSystemTime (Current Day)
⇒ DayKey = (CurrentDay << 0x10) ^ CurrentDay
    if (DayKey <= 1) {
      DayKey = CurrentDay << 0x18
    }
CurrentMonth = GetSystemTime (Current Month)
⇒ MonthKey = (CurrentMonth << 0x10) ^ CurrentMonth
    if (MonthKey <= 7) {
      MonthKey = CurrentMonth << 0x18              // == *2^24
      if (MonthKey <= 7) {
        MonthKey = !(MonthKey)
      }
    }
CurrentYear = GetSystemTime (Current Year)
⇒ YearKey = ((CurrentYear + NewKey) << 0x10) ^ (CurrentYear + NewKey)
    if (YearKey <= 0xF) {
      YearKey = ((CurrentYear + NewKey) << 0x18)
    }
StringLength = (((DayKey ^ ((YearKey ^ 8 * YearKey ^ ((DayKey ^ ((MonthKey ^ 4 * MonthKey) >> 6)) >> 8)) >> 5)) >> 6) & 3) + 0xC
i = 0
  do {
    MonthKey = ((MonthKey ^ 4 * MonthKey) >> 0x19) ^ 0x10 * (MonthKey & 0xFFFFFFF8)
    DayKey = (DayKey >> 0x13)) ^ ((DayKey >> 6) ^ (DayKey << 0xC)) & 0x1FFF ^ (DayKey << 0xC)
    YearKey = ((YearKey ^ 8 * YearKey) >> 0xB) ^ ((YearKey & 0xFFFFFFF0) << 0x11)
    i = i + 1
    ServerName [i - 1] = (DayKey ^ MonthKey ^ YearKey) % 0x19 + 'a'
  } while (i < StringLength)
TLD = .ru .org .co.uk .info .com .net .biz
```

- ⇒ 1000 FQDN / jour

http://blog.fortinet.com/A-Closer-Look-at-Cryptolocker-s-DGA/

W

Exec. – 3/4

C

➡ POST http://xeogrhyqquuubt.com

K-RSA-pub^{C} (donne-moi 1 K-RSA-pub^{W})

[K-RSA-priv^{W}]

K-RSA-priv^{C} (K-RSA-pub^{W}) ⬅

[K-RSA-pub^{W}]

URL POST: ..&version=<version du malware>&id=<num?>&name=<hostname>&group=<groupid>&lid=en-US

K-RSA-priv = 2048 bits

Exec. – 4/4

- Pour chaque fichier à chiffrer
- [K-AES^{W}] = rand (256 bits)
- fichier chiffré =
  - 00 .. 19 [hdr#1] = SHA1 (0000 . header#2)
  - 20 .. 275 [hdr#2] = K-RSA-pub^{W} (K-AES^{W})
  - 276 … [data] = K-AES^{W} (fichier en clair)
- HKEY_CURRENT_USER\Software\CryptoLocker\Files = fichier chiffré °1, fichier chiffré °2, …

Offset	Length	Description
0×00	0×14	SHA1 hash of '\x00'*4 followed by the next 0×100 bytes (the "file header")
0×14	0×100	File header containing the AES key encrypted with RSA-2048 with PKCS#1 v1.5 padding
0×100	remainder	File contents encrypted with above AES key

Once the file header is decrypted, The `CryptImportKey` Win32 CryptoAPI function is used to interpret a Microsoft `PUBLICKEYSTRUC` structure. The format of the `PUBLICKEYSTRUC` structure is:

```
typedef struct _PUBLICKEYSTRUC {
  BYTE   bType;
  BYTE   bVersion;
  WORD   reserved;
  ALG_ID aiKeyAlg;
} BLOBHEADER, PUBLICKEYSTRUC;
```

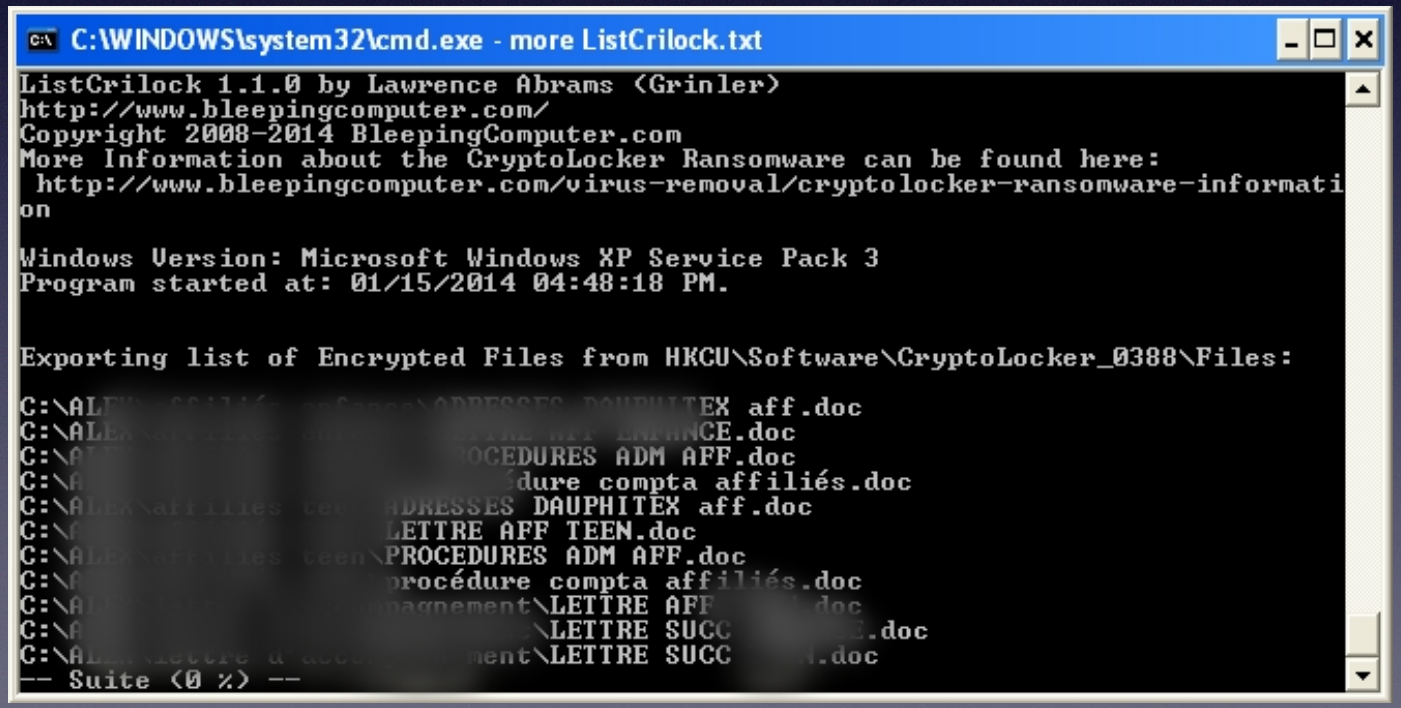
For CryptoLocker, the following values are used:

Field	Value
bType	8 (PLAINTEXTKEYBLOB)
bVersion	2
reserved	0
aiKeyAlg	0×6610 (CALG_AES_256)

http://www.kyrus-tech.com/cryptolocker-decryption-engine/

Infecté ? – 1/4

- Retirer la machine du réseau
- Lister les fichiers chiffrés



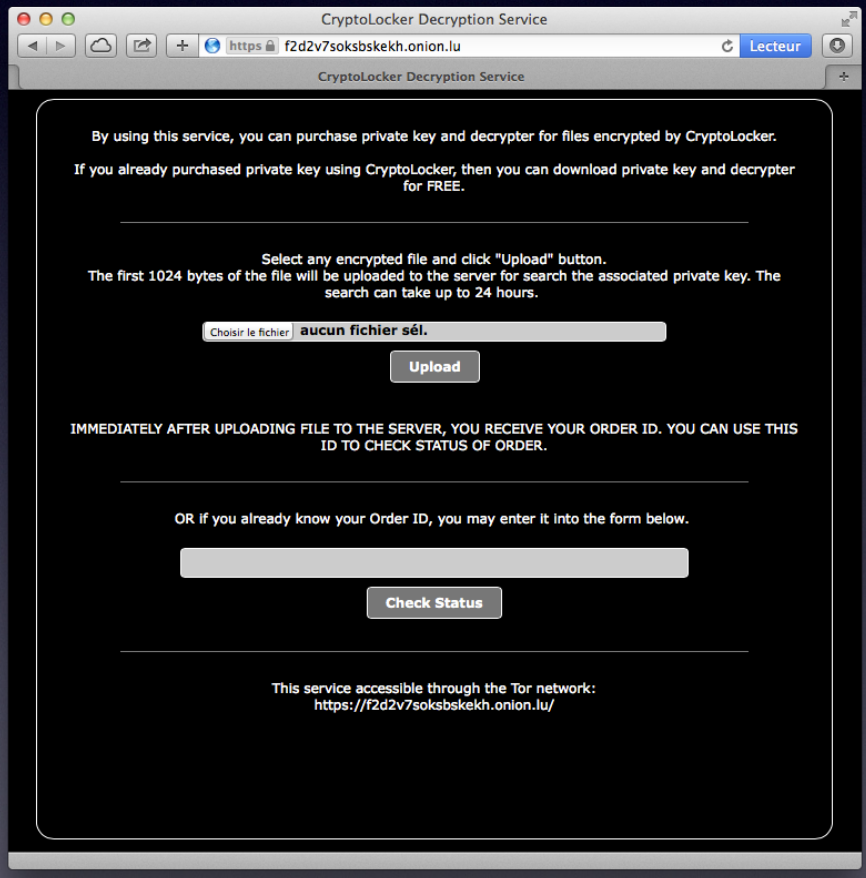
http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

^{w} Infecté ? – 2/4

- Si < 72 heures, payez 0,5 BTC
- En retour :
  - [K-RSA-priv^{W}]
  - URL.onion pour télécharger `CryptoLockerDecrypter.exe`

^{W} Infecté ? – 3/4

- Si > 72 heures : http://f2d2v7soksbskekh.onion
- Uploader un fichier chiffré
- Payer 3,0 BTC
- En retour :
  - [K-RSA-priv^{W}]
  - `CryptoLockerDecrypter.exe`



Infecté ? – 4/4

- Porter plainte :
  - BEFTI
  - 01 55 75 26 19

Decrypt. Srv – 1/3

- CryptoLocker Decryption Service
  - f2d2v7soksbskekh.onion
  - xjqrbcpinwxg.com
- Registrar: bizcn.com
  - Creation Date: 02-feb-2014
  - IP Geo loc ⇒ Country: RU
- Server: nginx/1.4.5
- <title>CryptoLocker Decryption Service</title>

Decrypt. Srv – 2/3

- Upload de fichier chiffré – code

```
<script type="text/javascript">
 //<![CDATA[
 var g_chunkSize = 1024;
 //]]>
</script>

<form id="file-form" method="post" action="/">
  <input id="file-data" name="file" type="hidden" value="">
  <input id="file-source" type="file">
</form>

<script type="text/javascript">
  var b = $("#file-source")[0].files;
  var c = b[0];
  var a = new FileReader();
  a.readAsArrayBuffer(c.slice(0, g_chunkSize))

  var h = "";
  var e = new Uint8Array(g.target.result);
  for (var f = 0; f < e.byteLength; f++) {
    h += String.fromCharCode(e[f])
  }
  $("#file-data").val(btoa(h));
  $("#file-form")[0].submit()
</script>
```

Decrypt. Srv - 3/3

- Upload de fichier chiffré - tests
- curl -A 'Mozilla/5.0' -sik -H 'Content-Type: application/x-www-form-urlencoded' -H 'Content-Length: 1361' -d "file=..incorrect.." http://xjqrbcpinwxg.com
  ⇒ Internal error. Please try again later.
- curl -A 'Mozilla/5.0' -sik -H 'Content-Type: application/x-www-form-urlencoded' -H 'Content-Length: 1477' -d "file=..correct.." http://xjqrbcpinwxg.com
  ⇒ Location: /?order=6eb05dbf734763ae9402d537e09cea74ef0c99f2
- curl -A 'Mozilla/5.0' -sik 'http://xjqrbcpinwxg.com/?order=fb3d2431dd6e84ebafc02f0678e16c439ace5e66&download'
  ⇒ .exe, contenant (strings):
  - order id (xxxxx-xxxxx-...)
  - priv key
  - fct *File*, Crypt*

Démo

- `dd bs=1 skip=20 count=256 < file | perl -e 'print scalar reverse <>' > file.aes.enc`

- `openssl rsautl -inkey priv.pem -decrypt -hexdump -in file.aes.enc`

```
0000 - 08 02 00 00 10 66 00 00-20 00 00 00 cb 31 4c e8   .....f.. ....1L.
0010 - 0b 8c ca 30 6e 1d 52 3c-60 cc c9 3a f8 78 c7 ba   ...0n.R<`..:.x..
0020 - 59 55 6f 9d f9 60 11 41-72 b4 15 b8               YUo..`.Ar...
```

`08…` = PUBLICKEYSTRUC (`08`: PLAINTEXTKEYBLOB, `02`: version, 0x`6610`: CALG_AES_256)
`cb 31 4C …` = K-AES

- `k=cb314ce80b8cca306e1d523c60ccc93af878c7ba59556f9df960114172b415b8`

- `dd bs=1 skip=276 < file > file.enc`

- `openssl enc -in file.enc -d -aes-256-cbc -K $k -iv 0`

Questions ?

- ?? patrick.asty@gmail.com
- $$ patrick.asty@iqqing.com