

# BitPyLock Ransomware Now Threatens to Publish Stolen Data

---

[bleepingcomputer.com/news/security/bitpylock-ransomware-now-threatens-to-publish-stolen-data/](https://bleepingcomputer.com/news/security/bitpylock-ransomware-now-threatens-to-publish-stolen-data/)

Lawrence Abrams

By

[Lawrence Abrams](#)

- January 21, 2020
- 04:04 AM
- 0



A new ransomware called BitPyLock has quickly gone from targeting individual workstations to trying to compromise networks and stealing files before encrypting devices.

BitPyLock was first discovered by MalwareHunterTeam on January 9th, 2020 and has since seen a trickle of new victims daily.

What is interesting is that we can compare the ransom notes of earlier versions with the latest versions to see a clear progression in the types of victims that are targeted.

To make matters worse, as ransomware operators begin stealing data before encrypting victims for use as leverage, BitPyLock actors claim to be adopting this tactic as well.

## The BitPyLock Ransomware

---

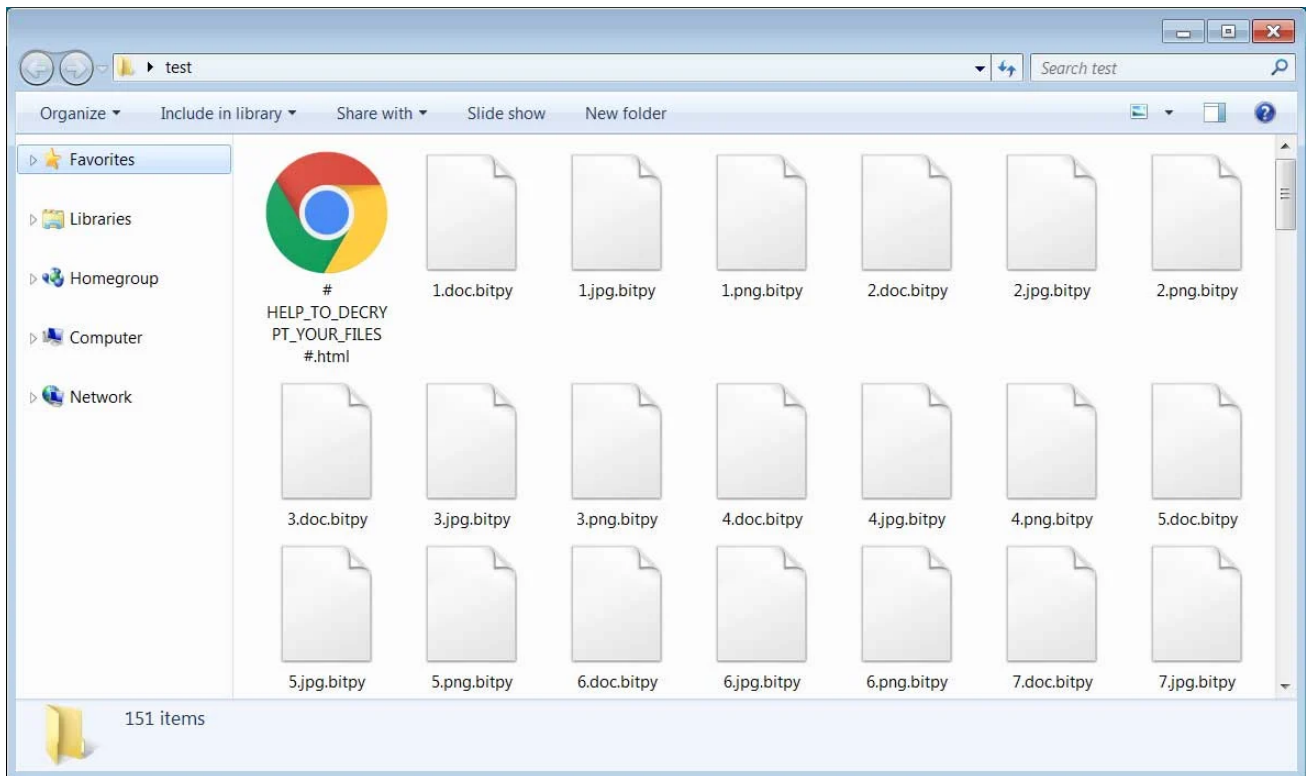
Based on our analysis, when first launched, BitPyLock will attempt to terminate any processes that contain the following strings. This is done to terminate security software and close files being used by backup software, web server daemons, virtual machines, and databases so that they can be encrypted.

backup, cobain, drop, drive, sql, database, vmware, virtual, agent, anti, iis, web, server, apache

While encrypting files, BitPyLock will target 346 extensions (listed in the IOCs section) and will skip any files located in the following folders.

windows  
windows.old  
program files  
program files (x86)  
program data  
\$recycle.bin  
system volume information

For every encrypted file, the ransomware will append the **.bitpy** extension as shown below. For example, a file named 1.doc will be encrypted and renamed to 1.doc.bitpy.



### Encrypted BitPyLock files

In each folder and on the Windows desktop, BitPyLock will create a ransom note named **# HELP\_TO\_DECRYPT YOUR\_FILES #.html** that instructs the users to send a bitcoin ransom to the enclosed bitcoin address. It then instructs the victim to email the listed address to get a decryptor.

In the sample BleepingComputer analyzed, the ransom amount was hardcoded to .8 bitcoins.

The language in the original ransom note also indicated that the attackers were targeting individual machines rather than networks.

# All your files are encrypted!

All your files, including, but not limited to:

Photos, videos, databases and office projects have been encrypted  
- using strong military grade encryption algorithms **AES-256** and **RSA-2048**.

**Recovery tools and other software will not help you!**

**Don't find your backups? because they have been successfully encrypted too or securely wiped!**

The only way to recover your files, are to meet our demands.

1. Create a Bitcoin wallet (we recommend you to create on [Blockchain.com](#))
2. Register on [LocalBitcoins.com](#) (or any other Bitcoin exchange), then buy **0.8** Bitcoin (BTC).
3. Send Bitcoins to our wallet below (in case sensitive. Make sure you copy past it):  

4. Send Bitcoin Transaction ID to our e-mail address along with your "Private ID" below of this page:  
[helpbitpy@cock.li](mailto:helpbitpy@cock.li)
5. You will receive the tools needed to decrypt all of your files immediately!

Note: Before payment you can contact with us for 1 free small file as decryption test!

**Be warned, we won't be able to recover your files if you start fiddling with them!**

**You have 72 hours (3 days) from this moment to send us payment, or you files will be lost in eternity!**

Private ID:



Original

## ransom note

Strangely, the sample that we saw had a static bitcoin address in the executable, which means every victim would have the same bitcoin address and thus it could make it impossible to determine who paid the ransom.

## Evolves to network attacks and the publishing of stolen data

In a more recent version discovered by MalwareHunterTeam, the actors have changed their targeting to focus on network compromise and the claims of stealing data before encrypting devices.

# All your files are encrypted!

If you read this message. That means we've been able to break into your network and encrypt all your machines.

All your files on all network machines, including, but not limited to:

Documents, databases, and office projects have been encrypted using strong military grade encryption algorithm **RSA-4096**.

Break it is impossible! and any effort is a waste of time!

**Recovery tools and other software will not help you!**

**Don't find your backups? because they have been successfully encrypted too or securly wiped!**

The only way to recover your files, are to meet our demand.

1. Create a Bitcoin wallet (we recommend you to create on [Blockchain.com](#))
2. Register on [LocalBitcoins.com](#) (or any other Bitcoin exchange), then buy █████ Bitcoin (BTC).
3. Send Bitcoins to our wallet below (in case sensitive. Make sure you copy past it):  
████████████████████
4. Send Bitcoin Transaction ID to our e-mail address along with our wallet address you pay!  
████████████████████
5. You will receive the tools needed to decrypt all of your machines and files!

Note: Before payment you can contact with us for 1 free small file as decryption test!

**Be warned, we won't be able to recover your files if you start fiddling with them!**

**If you do not wish to negotiate with us. We will make your company's private papers and databases public. This's not a joke!**

**You have 72 hours from this moment to send us payment, or you files and the way we communicate will be lost in eternity!**

## New ransom note targeting networks

In this version of the ransom note, we can see that the attackers are targeting "all your files on all network machines".

For entire network decryption, BitPyLock's ransom amounts are also fairly low compared to other targeted ransomware at only approximately 5 bitcoins for the entire network.

The ransom note further states that they will release stolen data if a ransom payment is not made.

"If you do not wish to negotiate with us. We will make your company's private papers and databases public. This's is not a joke!"

Unlike [Maze Ransomware](#) and [Sodinokibi Ransomware](#) who have already released stolen files belonging to non-paying victims, BitPyLock has not done so at this time.

This could also just be an empty threat like ransomware operators used to make in the past. Unfortunately, there is no way to tell anymore as more ransomware actors begin to actually release stolen data.

## IOCs:

---

## Hashes:

---

274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244

## Associated file names:

---

# HELP\_TO\_DECRYPT\_YOUR\_FILES #.html

## Targeted Extensions:

---

.frx, .jin, .xls, .xlsx, .pdf, .doc, .docx, .ppt, .pptx, .log, .txt, .gif, .png, .conf, .data, .dat, .dwg, .asp, .aspx, .html, .tif, .htm, .php, .jpg, .jsp, .js, .cnf, .cs, .vb, .vbs, .mdb, .mdf, .bak, .bkf, .java, .jar, .war, .pem, .pfx, .rtf, .pst, .dbx, .mp3, .mp4, .mpg, .bin, .nvram, .vmdk, .vmsd, .vmx, .vmxf, .vmsn, .vmem, .gz, .3dm, .3ds, .zip, .rar, .3fr, .3g2, .3gp, .3pr, .7z, .ab4, .accdb, .accde, .accdr, .accdt, .ach, .acr, .act, .adb, .ads, .agdl, .ai, .ait, .al, .apj, .arw, .asf, .asm, .asx, .avi, .awg, .back, .backup, .backupdb, .pbl, .bank, .bay, .bdb, .bgt, .bik, .bkp, .blend, .bpw, .c, .cdf, .cab, .chm, .cdr, .cdr3, .cdr4, .cdr5, .cdr6, .cdrw, .cdx, .ce1, .ce2, .cer, .cfp, .cgm, .cib, .class, .cls, .cmt, .cpi, .cpp, .cr2, .craw, .crt, .crw, .csh, .csl, .csv, .dac, .db, .db3, .dbf, .db-journal, .dc2, .dcr, .dcs, .ddd, .ddoc, .ddrw, .dds, .der, .des, .design, .dgc, .djvu, .dng, .dot, .docm, .dotm, .dotx, .drf, .drw, .dtd, .dxb, .dxf, .jse, .dxg, .eml, .eps, .erbsql, .erf, .exf, .fdb, .ffd, .fff, .fh, .fmb, .fhd, .fla, .flac, .flv, .fpx, .fxg, .gray, .grey, .gry, .h, .hbk, .hpp, .ibank, .ibd, .ibz, .idx, .iif, .iiq, .incpas, .indd, .jpe, .jpeg, .kc2, .kdbx, .kdc, .key, .kpdx, .lua, .m, .m4v, .max, .mdc, .mef, .mfw, .mmw, .moneywell, .mos, .mov, .mrw, .msg, .myd, .nd, .ndd, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf, .nsg, .nsh, .nwb, .nx2, .nx1, .nyf, .oab, .obj, .odb, .odc, .odf, .odg, .odm, .odp, .ods, .odt, .oil, .orf, .ost, .otg, .oth, .otp, .ots, .ott, .p12, .p7b, .p7c, .pab, .pages, .pas, .pat, .pcd, .pct, .pdb, .pdd, .pef, .pl, .plc, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .pptm, .prf, .ps, .psafe3, .psd, .pspimage, .ptx, .py, .qba, .qbb, .qbm, .qbr, .qbw, .qbx, .qby, .r3d, .raf, .rat, .raw, .rdb, .rm, .rw2, .rwl, .rwz, .s3db, .sas7bdat, .say, .sd0, .sda, .sdf, .sldm, .sldx, .sql, .sqlite, .sqlite3, .sqlitedb, .sr2, .srf, .srt, .srw, .st4, .st5, .st6, .st7, .st8, .std, .sti, .stw, .stx, .svg, .swf, .sxc, .sxd, .sxd, .sxi, .sxi, .sxm, .sxw, .tex, .tga, .thm, .tlg, .vob, .wallet, .wav, .wb2, .wmv, .wpd, .wps, .x11, .x3f, .xis, .xla, .xlam, .xlk, .xlm, .xlr, .xlsb, .xlsm, .xlt, .xltm, .xltx, .xlw, .ybcra, .yuv

- [BitPyLock](#)
- [Data Exfiltration](#)
- [Extortion](#)
- [Ransomware](#)

### 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](#)

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:**

---