EMSISOFT Blog

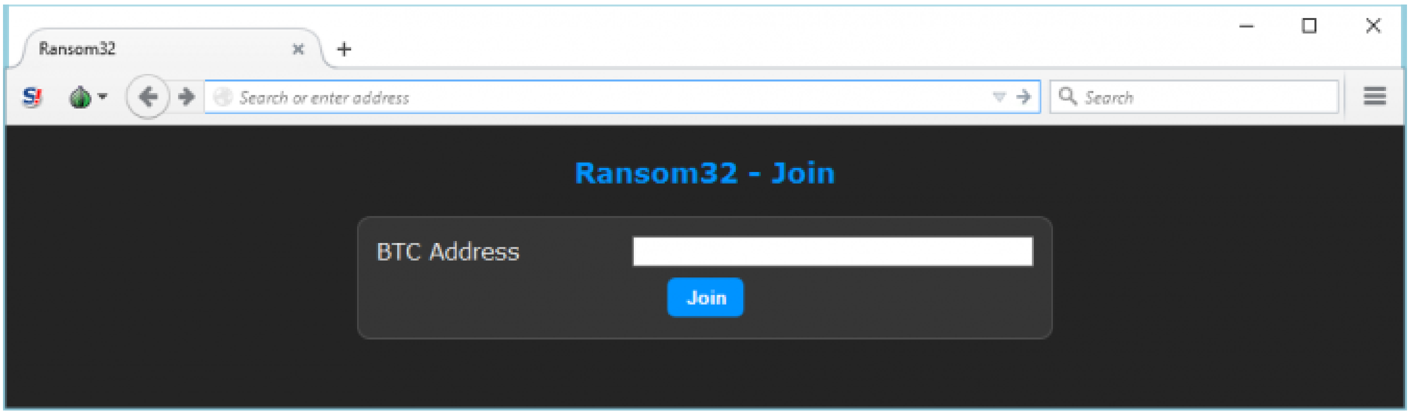
Meet Ransom32: The first JavaScript ransomware

In Security Knowledge by Fabian on January 1, 2016 | English

Software as a service (or SaaS) is a relatively new model of how a lot of software companies are conducting their business today – often to great success. So it comes as no surprise that malware writers and cyber crooks are attempting to adopt this model for their own nefarious purposes. In the past year a whole bunch of these “Ransomware as a Service” campaigns appeared, like for example Tox, Fakben or Radamant. Today we want to spotlight the newest of these campaigns.

Meet Ransom32

At first glance Ransom32 looks like a dime a dozen among many similar malware campaigns. Signups are handled via a hidden server in the Tor network. A simple Bitcoin address where you want the funds generated by your ransomware to be sent to is enough to signup.



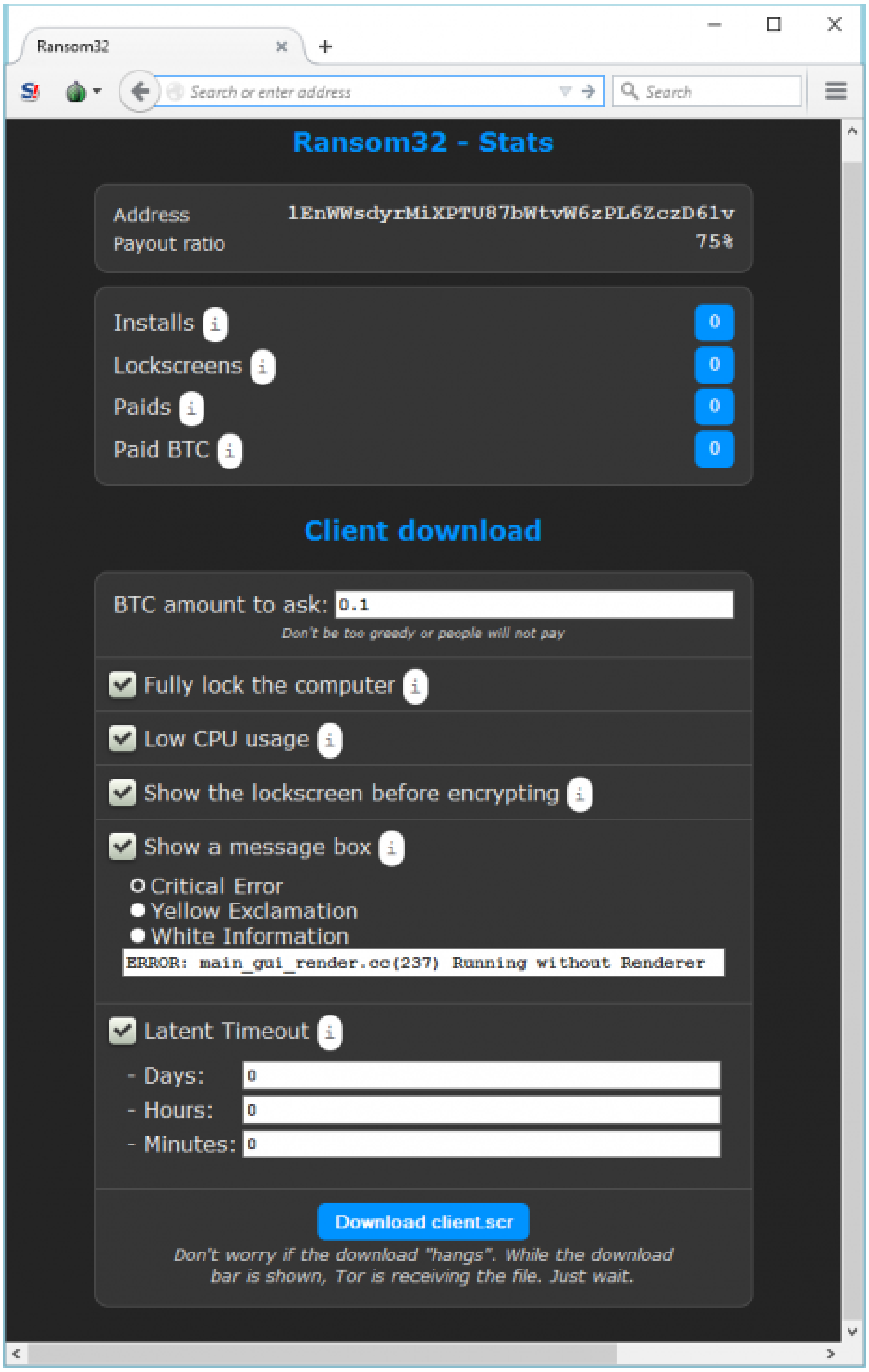
Ransom32 - Join

BTC Address

Join

All you need to get your own customized ransomware is a Bitcoin address to send your earnings to

After you type in your Bitcoin address, you will get access to the rudimentary administration panel. In the admin panel, you can get various statistics, like for example how many people already paid or how many systems were infected. You can also configure your “client”, which is their term for the actual malware. It is possible to change the amount of Bitcoins the malware will ask for, as well as configure parameters like fake message boxes the malware is supposed to show during install.



Ransom32 - Stats

Address 1EnWWsdyrMiXPTU87bWtvW6zPL6ZczD61v
Payout ratio 75%

Installs 0
Lockscreens 0
Paids 0
Paid BTC 0

Client download

BTC amount to ask: 0.1
Don't be too greedy or people will not pay

☑ Fully lock the computer

☑ Low CPU usage

☑ Show the lockscreen before encrypting

☑ Show a message box
○ Critical Error
● Yellow Exclamation
● White Information
ERROR: main_gui_render.cc(237) Running without Renderer

☑ Latent Timeout
- Days: 0
- Hours: 0
- Minutes: 0

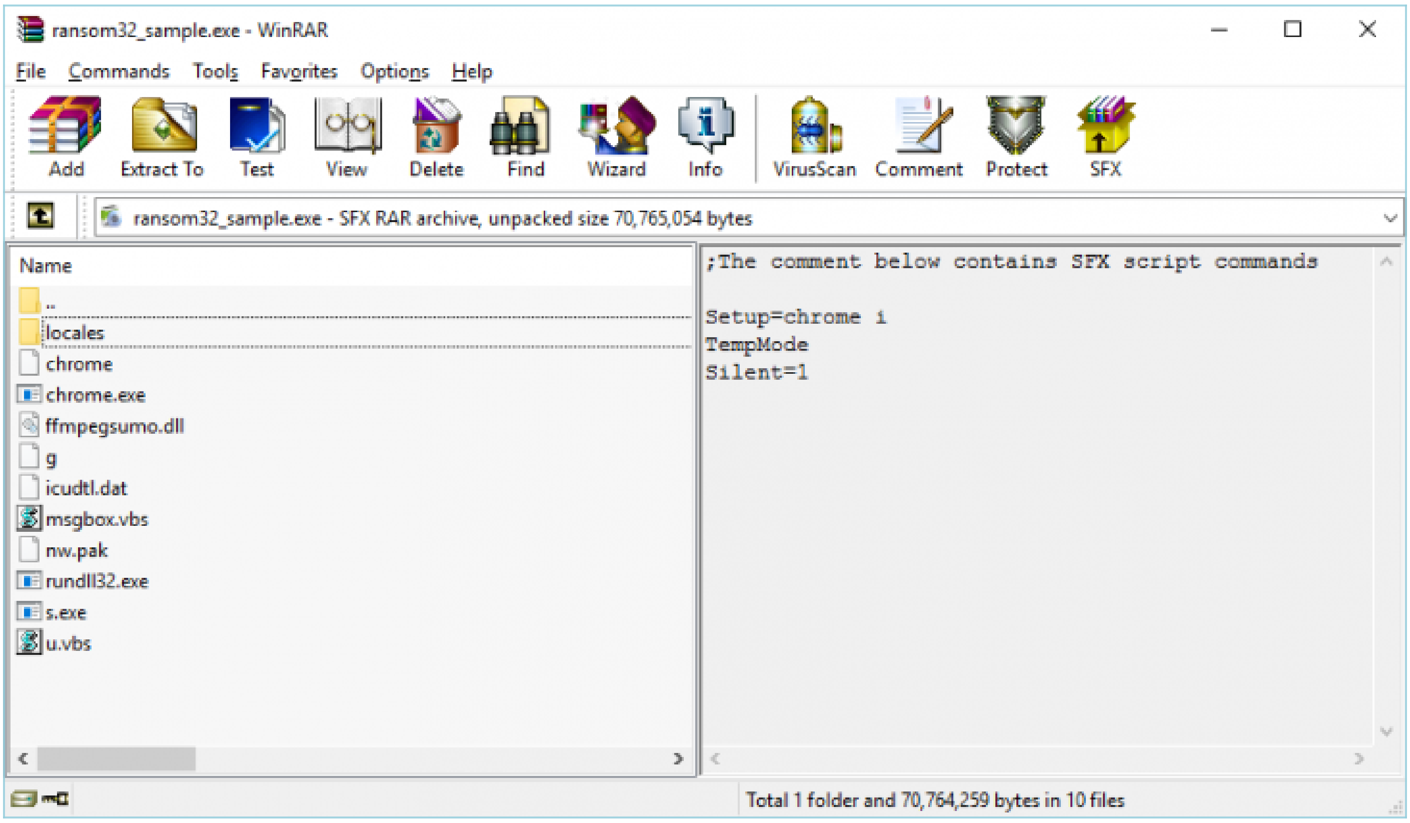
Download client.scr
Don't worry if the download "hangs". While the download bar is shown, Tor is receiving the file. Just wait.

A web interface allows you to see how many systems the malware has infected, how many Bitcoins it earned and allows you to further customize the malware

A click on “Download client.scr” will then generate the malware according to the specifications and will start the download of the more than 22 MB large malware file. At this point it becomes evident that Ransom32 is very different to other ransomware, which rarely exceed 1 MB in size. In fact, most ransomware authors use the small size of their malicious files as some kind of unique selling point when advertising their campaigns in underground hacker communities. Ransom32 definitely had our interest.

Unwrapping the behemoth

After further examination the downloaded file turned out to be a WinRAR self-extracting archive:



ransom32_sample.exe - SFX RAR archive, unpacked size 70,765,054 bytes

..
locales
chrome
chrome.exe
ffmpegsumo.dll
g
icudtl.dat
msgbox.vbs
nw.pak
rundll32.exe
s.exe
u.vbs

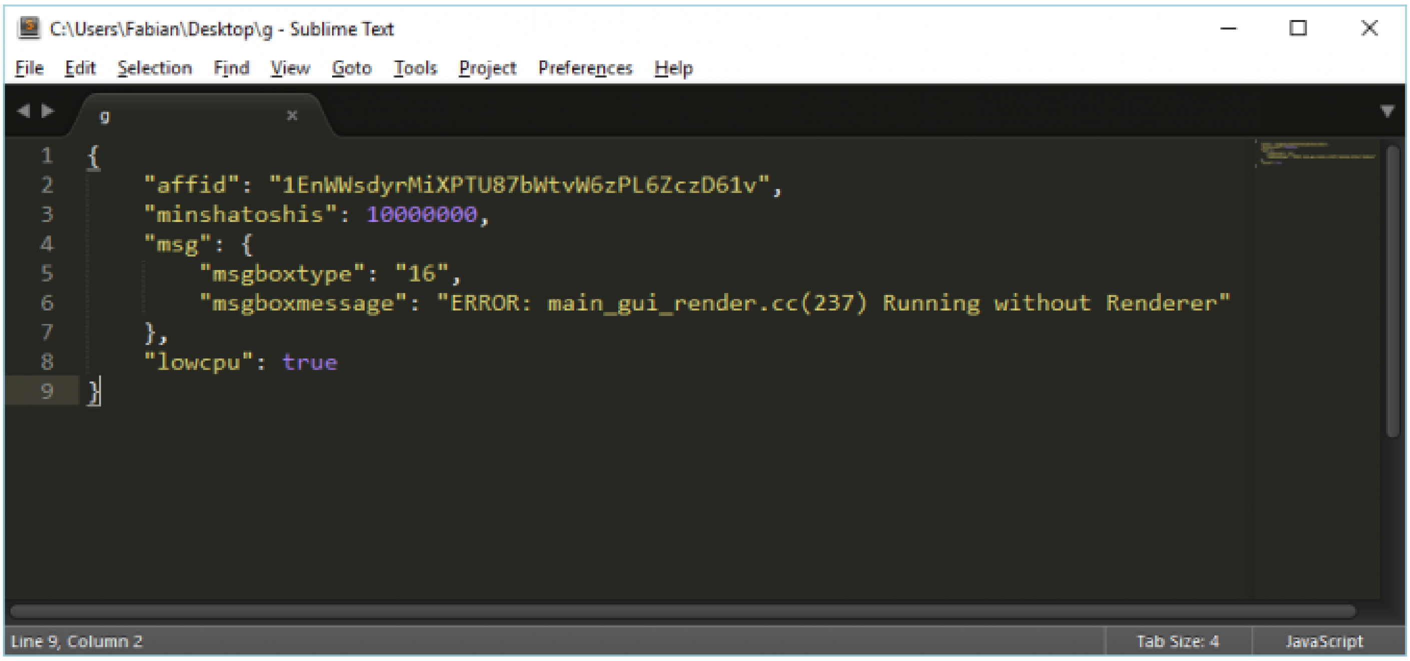
```
;The comment below contains SFX script commands

Setup=chrome i
TempMode
Silent=1
```

Total 1 folder and 70,764,259 bytes in 10 files

The content of the Ransom32 SFX archive

The malware uses the script language implemented in WinRAR to automatically unpack the content of the archive into the user’s temporary files directory and execute the “chrome.exe” file contained in the archive. The files within the archive have the following purposes:

- “chrome” contains a copy of the GPL license agreement.
- “chrome.exe” is a packaged NW.js application and contains the actual malware code as well as the framework required to run the malware.
- “ffmpegsumo.dll”, “nw.pak”, “icudtl.dat” and “locales” contain data that are required by the NW.js framework to function properly.
- “rundll32.exe” is a renamed copy of the Tor client.
- “s.exe” is a renamed copy of Optimum X Shortcut, a utility to create and manipulate Desktop and start menu shortcuts.
- “g” contains the malware’s configuration information as configured in the web interface.
- “msgbox.vbs” is a small script that displays a customizable popup message and is used to display the configured message box.
- “u.vbs” is a small script that enumerates, and deletes all files and folders in a given directory.


C:\Users\Fabian\Desktop\g - Sublime Text
File Edit Selection Find View Goto Tools Project Preferences Help
g
Line 9, Column 2
Tab Size: 4
JavaScript

```
{
    "affid": "1EnWWsdyrMiXPTU87bWtvW6zPL6ZczD61v",
    "minshatoshis": 10000000,
    "msg": {
        "msgboxtype": "16",
        "msgboxmessage": "ERROR: main_gui_render.cc(237) Running without Renderer"
    },
    "lowcpu": true
}
```

The “g” file contains the malware’s configuration formatted as JSON

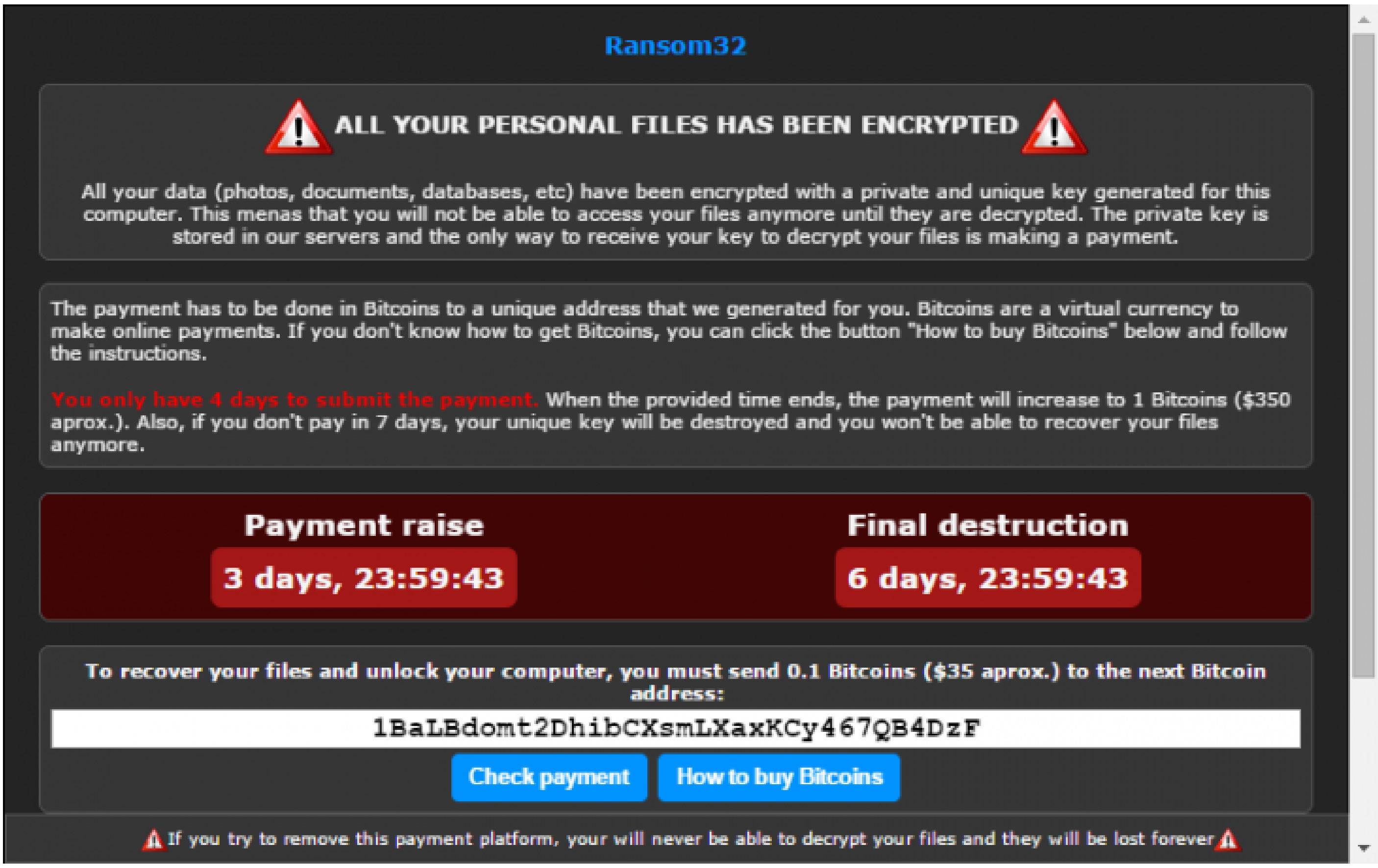
The most interesting part by far in that package is the “chrome.exe”. Upon first inspection, “chrome.exe” looks suspiciously like a copy of the actual Chrome browser. Only the lack of a proper digital signature and version information hints that this file is not the actual Chrome browser. Upon further inspection, it turned out that this file is a packaged NW.js application.

Using modern web-based technologies for ransomware

So what is NW.js exactly? NW.js is essentially a framework that allows you to develop normal desktop applications for Windows, Linux and MacOS X using JavaScript. It is based upon the popular Node.js and Chromium projects. So while JavaScript is usually tightly sandboxed in your browser and can’t really touch the system it runs upon, NW.js allows for much more control and interaction with the underlying operating system, enabling JavaScript to do almost everything “normal” programming languages like C++ or Delphi can do. The benefit for the developer is that they can turn their web applications into normal desktop applications relatively easily. For normal desktop application developers it has the benefit that NW.js is able to run the same JavaScript on different platforms. So a NW.js application only needs to be written once and is instantly usable on Windows, Linux and MacOS X.

This also means, that at least in theory, Ransom32 could easily be packaged for both Linux and Mac OS X. That being said at this point we haven’t seen any such packages, which at least for the moment makes Ransom32 most likely Windows-only. Another large benefit for the malware author is that NW.js is a legitimate framework and application. So it is no surprise that even almost 2 weeks after the malware was first created, signature coverage is still incredibly bad.

Once Ransom32 arrives on a system and is executed, it will first unpack all its files into the temporary files folder. From there it copies itself into the “%AppData%\Chrome Browser” directory. It uses the bundled “s.exe” file to create a shortcut in the user’s Startup folder named “ChromeService” that will make sure the malware is being executed on every boot. The malware will then start the bundled Tor client to establish a connection to its command and control server (C2 server) hidden inside the Tor network on port 85. After a successful connection with the C2 server to negotiate the Bitcoin address the affected user is supposed to send the ransom to, as well as exchanging the cryptographic key used for encryption, the malware will eventually display its ransom note.



Ransom32

ALL YOUR PERSONAL FILES HAS BEEN ENCRYPTED

All your data (photos, documents, databases, etc) have been encrypted with a private and unique key generated for this computer. This menas that you will not be able to access your files anymore until they are decrypted. The private key is stored in our servers and the only way to receive your key to decrypt your files is making a payment.

The payment has to be done in Bitcoins to a unique address that we generated for you. Bitcoins are a virtual currency to make online payments. If you don't know how to get Bitcoins, you can click the button "How to buy Bitcoins" below and follow the instructions.

You only have 4 days to submit the payment. When the provided time ends, the payment will increase to 1 Bitcoins ($350 aprox.). Also, if you don't pay in 7 days, your unique key will be destroyed and you won't be able to recover your files anymore.

Payment raise
3 days, 23:59:43

Final destruction
6 days, 23:59:43

To recover your files and unlock your computer, you must send 0.1 Bitcoins ($35 aprox.) to the next Bitcoin address:

1BaLBdomt2DhibCXsmLXaxKCy467QB4DzF

⚠ If you try to remove this payment platform, your will never be able to decrypt your files and they will be lost forever ⚠

The ransom note displayed by the malware

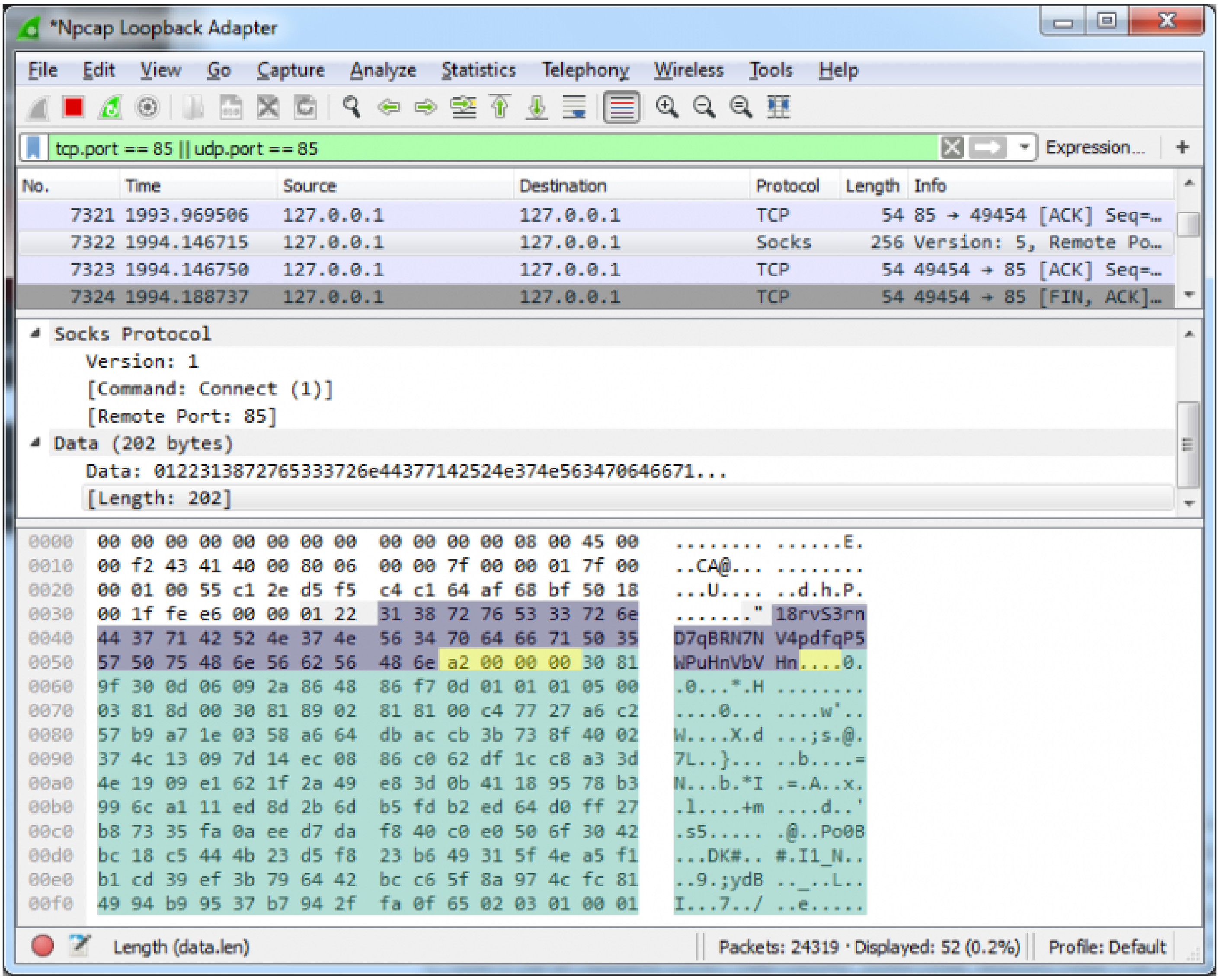
It then starts encrypting the user's files. All files with one of the following file extensions are being targeted:

> *.jpg, *.jpeg, *.raw, *.tif, *.gif, *.png, *.bmp, *.3dm, *.max, *.accdb, *.db, *.dbf, *.mdb, *.pdb, *.sql, *.*sav*, *.*spv*,
> *.*grle*, *.*mlx*, *.*sv5*, *.*game*, *.*slot*, *.dwg, *.dxf, *.c, *.cpp, *.cs, *.h, *.php, *.asp, *.rb, *.java, *.jar, *.class, *.a
> *.aep, *.aepx, *.plb, *.prel, *.prproj, *.aet, *.ppj, *.psd, *.indd, *.indl, *.indt, *.indb, *.inx, *.idml, *.pmd, *.xqx, *.xqx, *.a
> *.eps, *.ps, *.svg, *.swf, *.fla, *.as3, *.as, *.txt, *.doc, *.dot, *.docx, *.docm, *.dotx, *.dotm, *.docb, *.rtf, *.wpd, *.wps,
> *.msg, *.pdf, *.xls, *.xlt, *.xlm, *.xlsx, *.xlsm, *.xltx, *.xltm, *.xlsb, *.xla, *.xlam, *.xll, *.xlw, *.ppt, *.pot, *.pps, *.pptx,
> *.pptm, *.potx, *.potm, *.ppam, *.ppsx, *.ppsm, *.sldx, *.sldm, *.wav, *.mp3, *.aif, *.iff, *.m3u, *.m4u, *.mid, *.mpa,
> *.wma, *.ra, *.avi, *.mov, *.mp4, *.3gp, *.mpeg, *.3g2, *.asf, *.asx, *.flv, *.mpg, *.wmv, *.vob, *.m3u8, *.csv, *.efx, *.s
> *.vcf, *.xml, *.ses, *.dat

The malware will not attempt to encrypt any files if they are located in a directory that contains any of the following strings:

- :\windows\
- :\winnt\
- programdata\
- boot\
- temp\
- tmp\
- $recycle.bin\

Files are being encrypted using AES with a 128 bit key using CTR as a block mode. A new key is being generated for every file. The key is encrypted using the RSA algorithm and a public key that is being obtained from the C2 server during the first communication.


*Npcap Loopback Adapter
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... +

```
tcp.port == 85 || udp.port == 85

No.   Time          Source      Destination  Protocol  Length  Info
 7321 1993.969506   127.0.0.1   127.0.0.1    TCP           54  85 → 49454 [ACK] Seq=…
 7322 1994.146715   127.0.0.1   127.0.0.1    Socks        256  Version: 5, Remote Po…
 7323 1994.146750   127.0.0.1   127.0.0.1    TCP           54  49454 → 85 [ACK] Seq=…
 7324 1994.188737   127.0.0.1   127.0.0.1    TCP           54  49454 → 85 [FIN, ACK]…

◢ Socks Protocol
    Version: 1
    [Command: Connect (1)]
    [Remote Port: 85]
◢ Data (202 bytes)
    Data: 0122313872765333726e44377142524e374e563470646671...
    [Length: 202]

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 f2 43 41 40 00 80 06  00 00 7f 00 00 01 7f 00   ..CA@... ........
0020  00 01 00 55 c1 2e d5 f5  c4 c1 64 af 68 bf 50 18   ...U.... ..d.h.P.
0030  00 1f fe e6 00 00 01 22  31 38 72 76 53 33 72 6e   ......." 18rvS3rn
0040  44 37 71 42 52 4e 37 4e  56 34 70 64 66 71 50 35   D7qBRN7N V4pdfqP5
0050  57 50 75 48 6e 56 62 56  48 6e a2 00 00 00 30 81   WPuHnVbV Hn....0.
0060  9f 30 0d 06 09 2a 86 48  86 f7 0d 01 01 01 05 00   .0...*.H ........
0070  03 81 8d 00 30 81 89 02  81 81 00 c4 77 27 a6 c2   ....0... ....w'..
0080  57 b9 a7 1e 03 58 a6 64  db ac cb 3b 73 8f 40 02   W....X.d ...;s.@.
0090  37 4c 13 09 7d 14 ec 08  86 c0 62 df 1c c8 a3 3d   7L..}... ..b....=
00a0  4e 19 09 e1 62 1f 2a 49  e8 3d 0b 41 18 95 78 b3   N...b.*I .=.A..x.
00b0  99 6c a1 11 ed 8d 2b 6d  b5 fd b2 ed 64 d0 ff 27   .l....+m ....d..'
00c0  b8 73 35 fa 0a ee d7 da  f8 40 c0 e0 50 6f 30 42   .s5..... .@..Po0B
00d0  bc 18 c5 44 4b 23 d5 f8  23 b6 49 31 5f 4e a5 f1   ...DK#.. #.I1_N..
00e0  b1 cd 39 ef 3b 79 64 42  bc c6 5f 8a 97 4c fc 81   ..9.;ydB .._..L..
00f0  49 94 b9 95 37 b7 94 2f  fa 0f 65 02 03 01 00 01   I...7../ ..e.....

Length (data.len)    Packets: 24319 · Displayed: 52 (0.2%)    Profile: Default
```

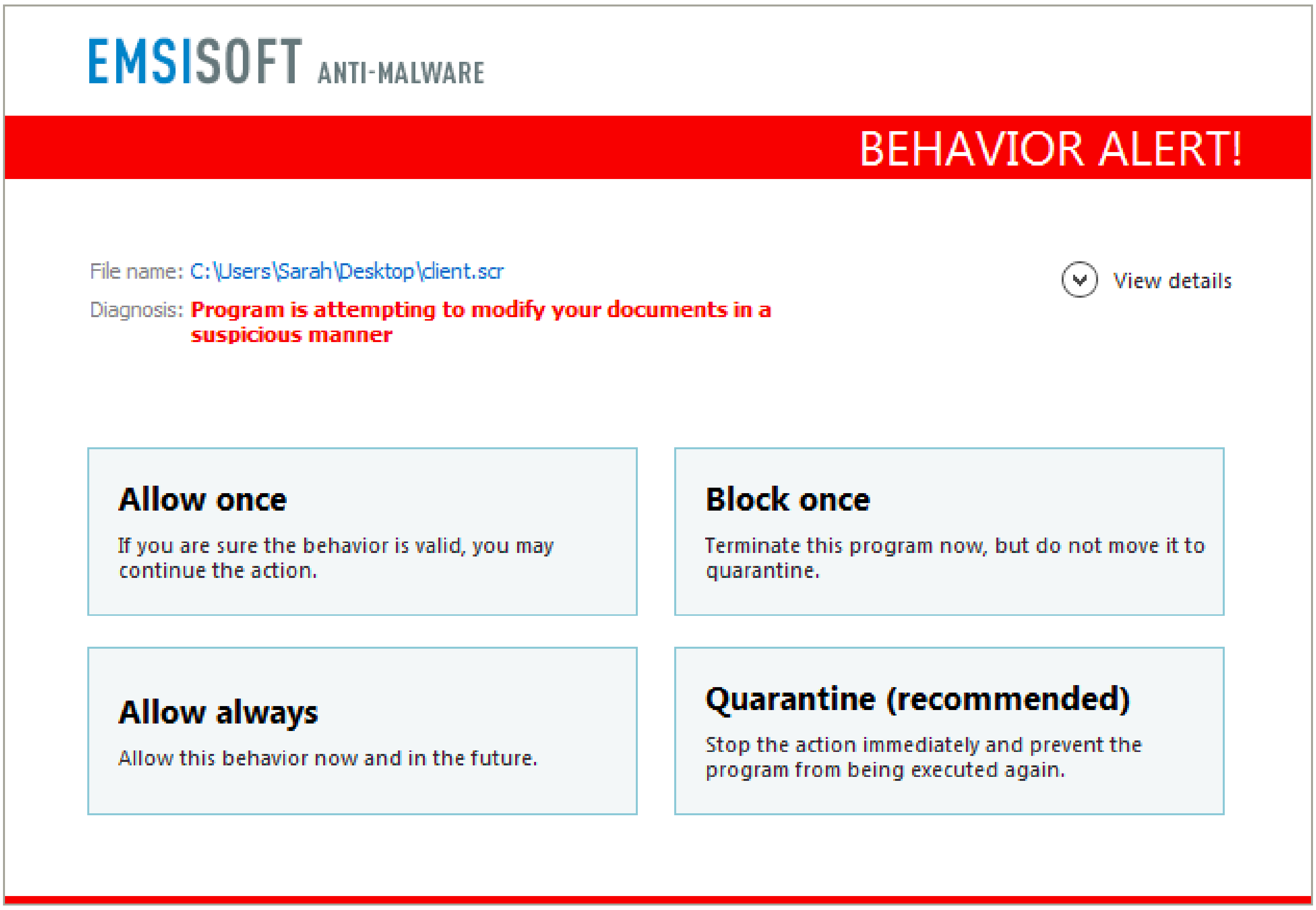
Part of the custom protocol exchange between Ransom32 and its command and control server to exchange Bitcoin address (purple) and public key (length yellow, key green)

The encrypted AES key is being stored together with the AES encrypted data inside the now encrypted file.

The malware also offers to decrypt a single file to demonstrate that the malware author has the capability to reverse the decryption. During this process the malware will send the encrypted AES key from the chosen file to the C2 server and gets the decrypted per-file AES key back in return.

How can I protect myself from Ransom32?

As explained in our recent ransomware article, the best protection remains a solid and proven backup strategy. Once again though, the behavior blocker technology used by Emsisoft Anti-Malware and Emsisoft Internet Security proved to be the second best defense, as all our users once again are protected from this and hundreds of different ransomware variants without the need of signatures.



EMSISOFT ANTI-MALWARE
BEHAVIOR ALERT!
View details

File name: C:\Users\Sarah\Desktop\client.scr

Diagnosis: Program is attempting to modify your documents in a suspicious manner

Allow once
If you are sure the behavior is valid, you may continue the action.
Block once
Terminate this program now, but do not move it to quarantine.
Allow always
Allow this behavior now and in the future.
Quarantine (recommended)
Stop the action immediately and prevent the program from being executed again.

Users of Emsisoft Anti-Malware and Emsisoft Internet Security are protected from Ransom32 and other ransomware families by the behavior blocker

We consider ransomware one of the biggest threats of the past year and plan to do our best to continue our excellent track record in the next year, to keep our users as protected as possible.

On that note, the malware research team here at Emsisoft wishes everyone a happy and malware-free new year.

Last but not least, we want to thank our friends over at BleepingComputer, who brought this threat to our attention first. We also would like to extend our gratitude to **xXToffeeXx** of BleepingComputer in particular, for her invaluable help and input while researching and reverse engineering this particular ransomware.

www.emsisoft.com