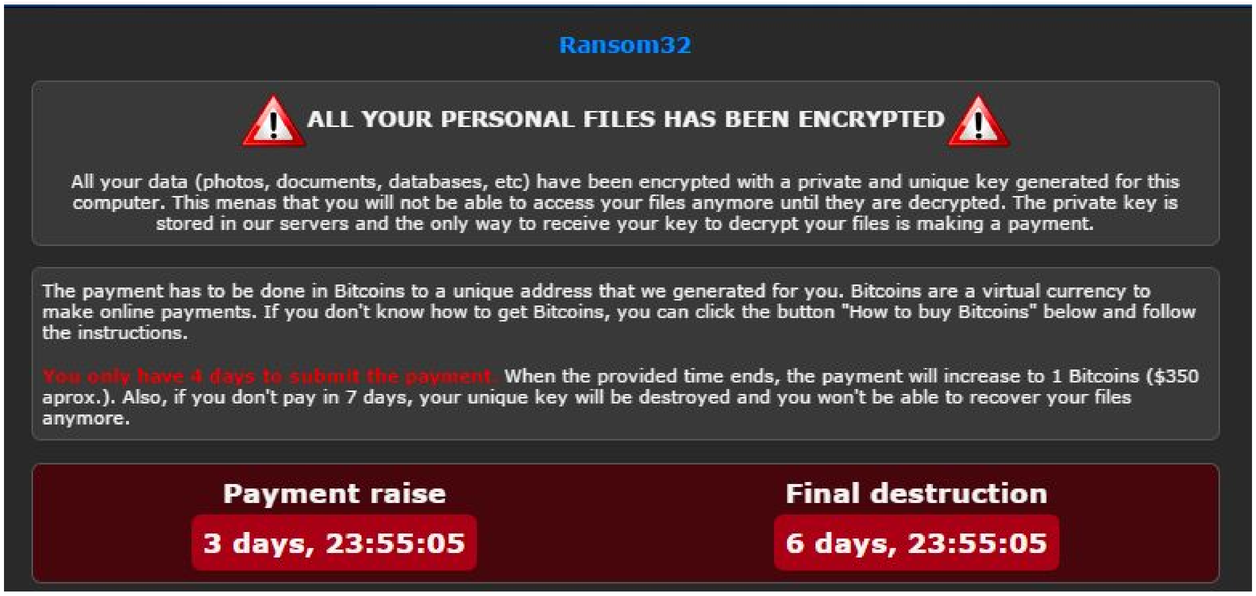

Ransom32

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, 23:55:05

Final destruction
6 days, 23:55:05

Ransom32 – look at the malicious package

January 11, 2016 by hasherezade

Last updated: March 30, 2016

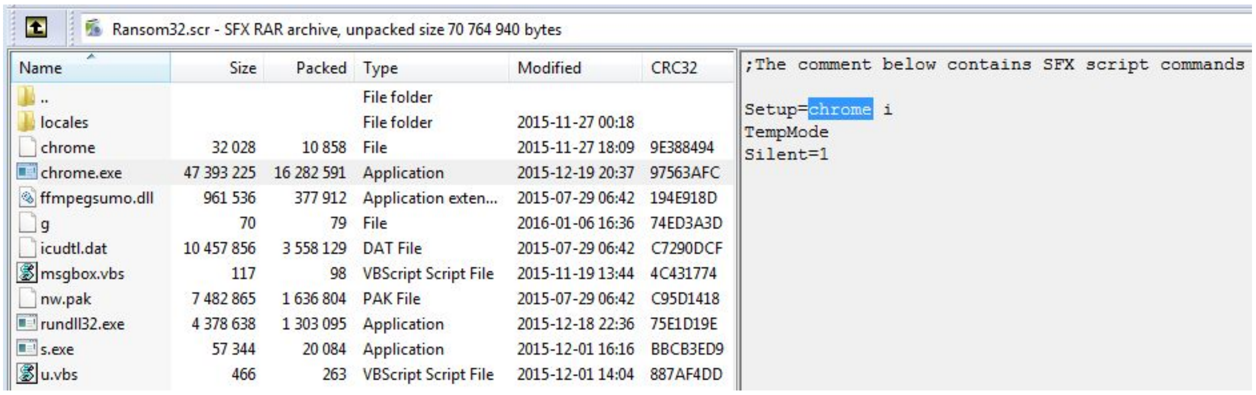
Ransom32 is a new ransomware implemented in a very atypical style. Emisoft provides a good description of its functionality here. In our post, we will focus on some implementation details of the malicious package.

Analyzed sample: 09f21eefaf8f52496d4e8b06920fe6fa

Overview

Ransom32 is delivered as an executable, that is in reality a autoextracting WinRAR archive. By default it is distributed as a file with .scr extension:

The WinRAR script is used to drop files in the specified place and autorun the unpacked content.



Ransom32.scr - SFX RAR archive, unpacked size 70 764 940 bytes

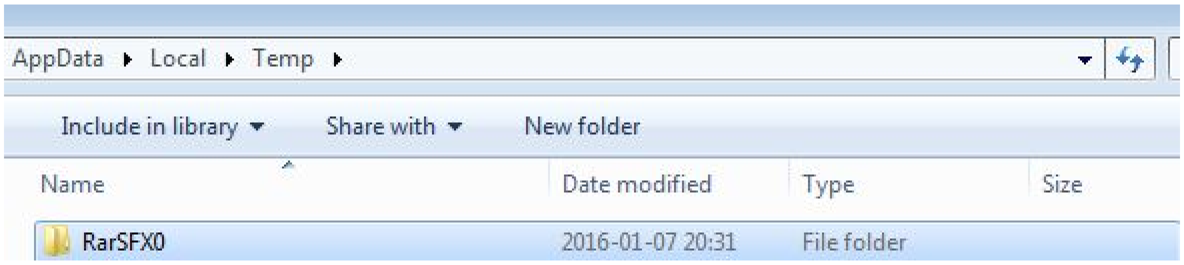
Name	Size	Packed	Type	Modified	CRC32
..			File folder		
locales			File folder	2015-11-27 00:18	
chrome	32 028	10 858	File	2015-11-27 18:09	9E388494
chrome.exe	47 393 225	16 282 591	Application	2015-12-19 20:37	97563AFC
ffmpegsumo.dll	961 536	377 912	Application exten...	2015-07-29 06:42	194E918D
g	70	79	File	2016-01-06 16:36	74ED3A3D
icudtl.dat	10 457 856	3 558 129	DAT File	2015-07-29 06:42	C7290DCF
msgbox.vbs	117	98	VBScript Script File	2015-11-19 13:44	4C431774
nw.pak	7 482 865	1 636 804	PAK File	2015-07-29 06:42	C95D1418
rundll32.exe	4 378 638	1 303 095	Application	2015-12-18 22:36	75E1D19E
s.exe	57 344	20 084	Application	2015-12-01 16:16	BBCB3ED9
u.vbs	466	263	VBScript Script File	2015-12-01 14:04	887AF4DD

```
;The comment below contains SFX script commands

Setup=chrome i
TempMode
Silent=1
```

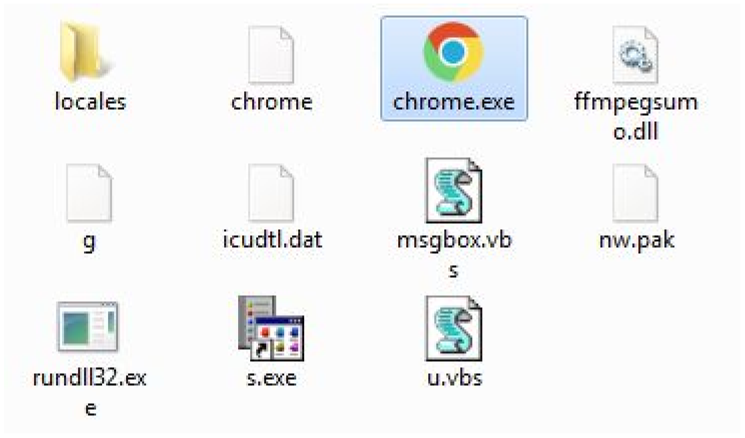
- **Setup=chrome i –** Setup value specifies the executable that is going to be run after file extraction. In this case it is **chrome.exe**
- **TempMode** means files are going to be dropped in the %TEMP% folder
- **Silent=1** means installation will be done without additional pop-ups about the progress

Installation directory created in %TEMP%:



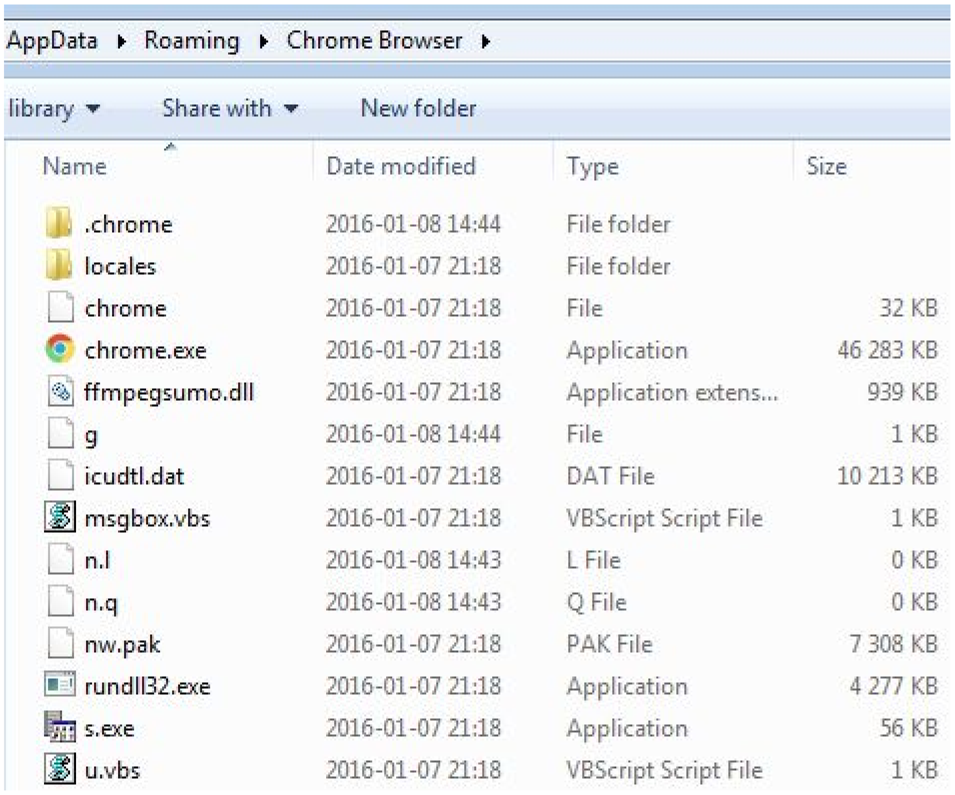
Name	Date modified	Type	Size
RarSFX0	2016-01-07 20:31	File folder	

The unpacked content consist of following files:



chrome.exe spoofs Google's browser, but in reality it is an element responsible for preparing and running the Node JS application (that is the main part of the ransomware).

After the **chrome.exe** is run from the %TEMP% folder, it installs the above files into %APPDATA% -in folder ***Chrome Browser***:



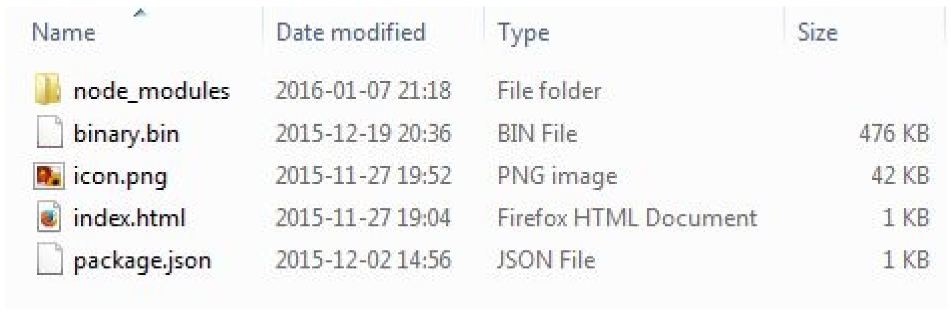
Name	Date modified	Type	Size
.chrome	2016-01-08 14:44	File folder	
locales	2016-01-07 21:18	File folder	
chrome	2016-01-07 21:18	File	32 KB
chrome.exe	2016-01-07 21:18	Application	46 283 KB
ffmpegsumo.dll	2016-01-07 21:18	Application extens...	939 KB
g	2016-01-08 14:44	File	1 KB
icudtl.dat	2016-01-07 21:18	DAT File	10 213 KB
msgbox.vbs	2016-01-07 21:18	VBScript Script File	1 KB
n.l	2016-01-08 14:43	L File	0 KB
n.q	2016-01-08 14:43	Q File	0 KB
nw.pak	2016-01-07 21:18	PAK File	7 308 KB
rundll32.exe	2016-01-07 21:18	Application	4 277 KB
s.exe	2016-01-07 21:18	Application	56 KB
u.vbs	2016-01-07 21:18	VBScript Script File	1 KB

Files stored in the folder ***Chrome Browser*** are just the environment to run the real malware.

Although the package as a whole is eclectic and contains various files belonging to various technologies, the core responsible for malicious actions consists of JavaScript files (NodeJS package). They are unpacked again into %TEMP% – in a new folder (its name follows the pattern: *nw[number]_[number]).* Let's take a look…

Scripts

Content of the malicious NodeJS package:

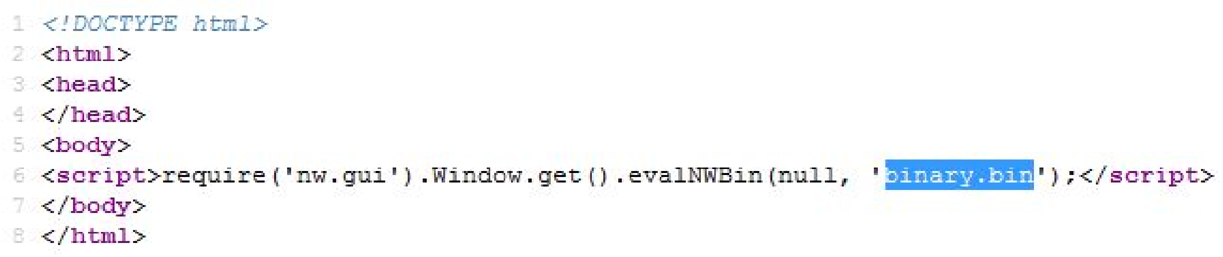


Name	Date modified	Type	Size
node_modules	2016-01-07 21:18	File folder	
binary.bin	2015-12-19 20:36	BIN File	476 KB
icon.png	2015-11-27 19:52	PNG image	42 KB
index.html	2015-11-27 19:04	Firefox HTML Document	1 KB
package.json	2015-12-02 14:56	JSON File	1 KB

The file **package.json** is a manifest, that defines a startup configuration and dependencies.

```
{
  "name": "app",
  "version": "1.0.0",
  "description": "",
  "main": "index.html",
  "single-instance": false,
  "scripts": {
    "test": "echo \"Error: no test specified\" &amp;&amp; exit 1"
  },
  "chromium-args": "--disable-accelerated-video",
  "author": "",
  "window": {
    "frame": false,
    "resizable": false,
    "visible-on-all-workspaces": true,
    "show_in_taskbar": true,
    "toolbar": false,
    "width": 800,
    "height": 500,
    "show": false,
    "title": "Ransom32",
    "icon": "icon.png"
  },
  "license": "ISC",
  "dependencies": {
    "minimatch": "^2.0.10",
    "ncp": "^2.0.0",
    "node-rsa": "^0.2.26",
    "socksv5": "^0.0.6"
  }
}
```

Entry point of the package is defined to be in **index.html**, that looks as below:



```
<!DOCTYPE html>
<html>
<head>
</head>
<body>
<script>require('nw.gui').Window.get().evalNWBin(null, 'binary.bin');</script>
</body>
</html>
```

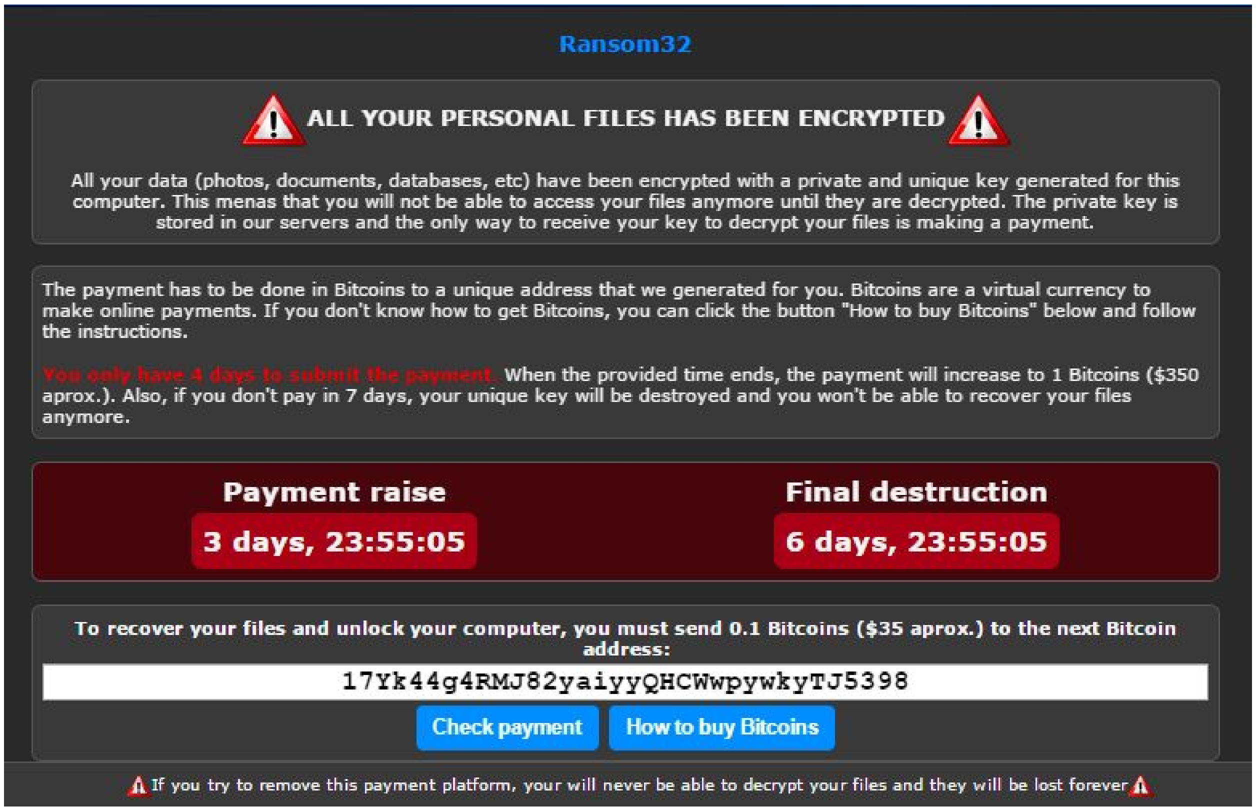
The heart of the ransomware is inside **binary.bin** – a JavaScript compiled to a native code and loaded using function evalNWBin. All other components are called from inside of this binary.

It is responsible for encrypting and decrypting files, as well as for displaying ransom note and guiding a victim. Compiling the javascript to a native code has been used as a form of protection. However, strings of **binary.bin** can tell us a lot about the functionality of this application.

We can find for example:

- attacked extensions
- names of functions deployed by the binary
- names of other binaries deployed from inside
- configuration of AES used to encrypt files: CTR (Integer Counter Mode) with 128 bit key
- CSS used to format the ransom information window
- the ransom note.
- instructions how to buy bitcoins
- the message displayed if the payment was received
- 3 base64 encoded elements – a png, a gif and an ogg (audio).

After encrypting the files, the ransom nag-window is displayed. The gui is generated by javascript, with the layout defined by the included CSS.



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, 23:55:05

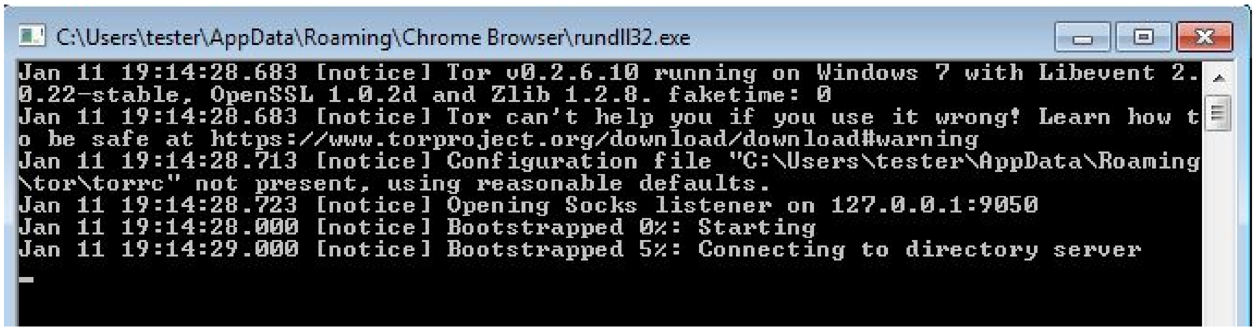
Final destruction
6 days, 23:55:05

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

17Yk44g4RMJ82yaiyyQHCWwpywkyTJ5398

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

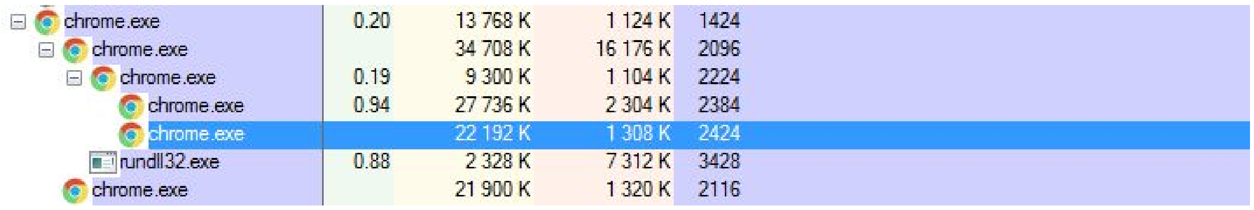
The internet connection is operated via included Tor client – renamed to *rundll32.exe*



C:\Users\tester\AppData\Roaming\Chrome Browser\rundll32.exe

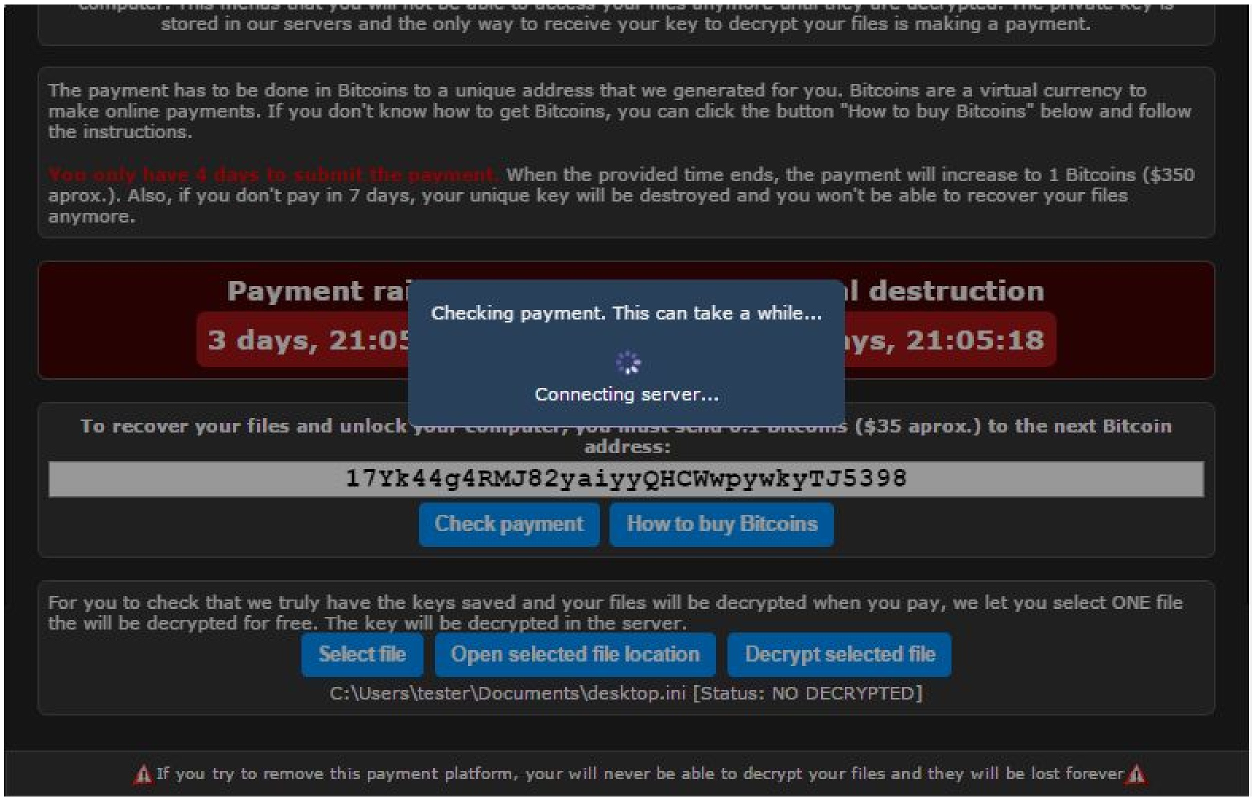
```
Jan 11 19:14:28.683 [notice] Tor v0.2.6.10 running on Windows 7 with Libevent 2.
0.22-stable, OpenSSL 1.0.2d and Zlib 1.2.8. faketime: 0
Jan 11 19:14:28.683 [notice] Tor can't help you if you use it wrong! Learn how t
o be safe at https://www.torproject.org/download/download#warning
Jan 11 19:14:28.713 [notice] Configuration file "C:\Users\tester\AppData\Roaming
\tor\torrc" not present, using reasonable defaults.
Jan 11 19:14:28.723 [notice] Opening Socks listener on 127.0.0.1:9050
Jan 11 19:14:28.000 [notice] Bootstrapped 0%: Starting
Jan 11 19:14:29.000 [notice] Bootstrapped 5%: Connecting to directory server
_
```

The tor client spawned by *chrome.exe:*



chrome.exe	0.20	13 768 K	1 124 K	1424
chrome.exe		34 708 K	16 176 K	2096
chrome.exe	0.19	9 300 K	1 104 K	2224
chrome.exe	0.94	27 736 K	2 304 K	2384
chrome.exe		22 192 K	1 308 K	2424
rundll32.exe	0.88	2 328 K	7 312 K	3428
chrome.exe		21 900 K	1 320 K	2116

When we click a button "*Check payment*" a request is sent via Tor client, in order to verify if the payment has been received:



computer. This means 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 rai **l destruction**

3 days, 21:05 **ys, 21:05:18**

Checking payment. This can take a while...

Connecting server...

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

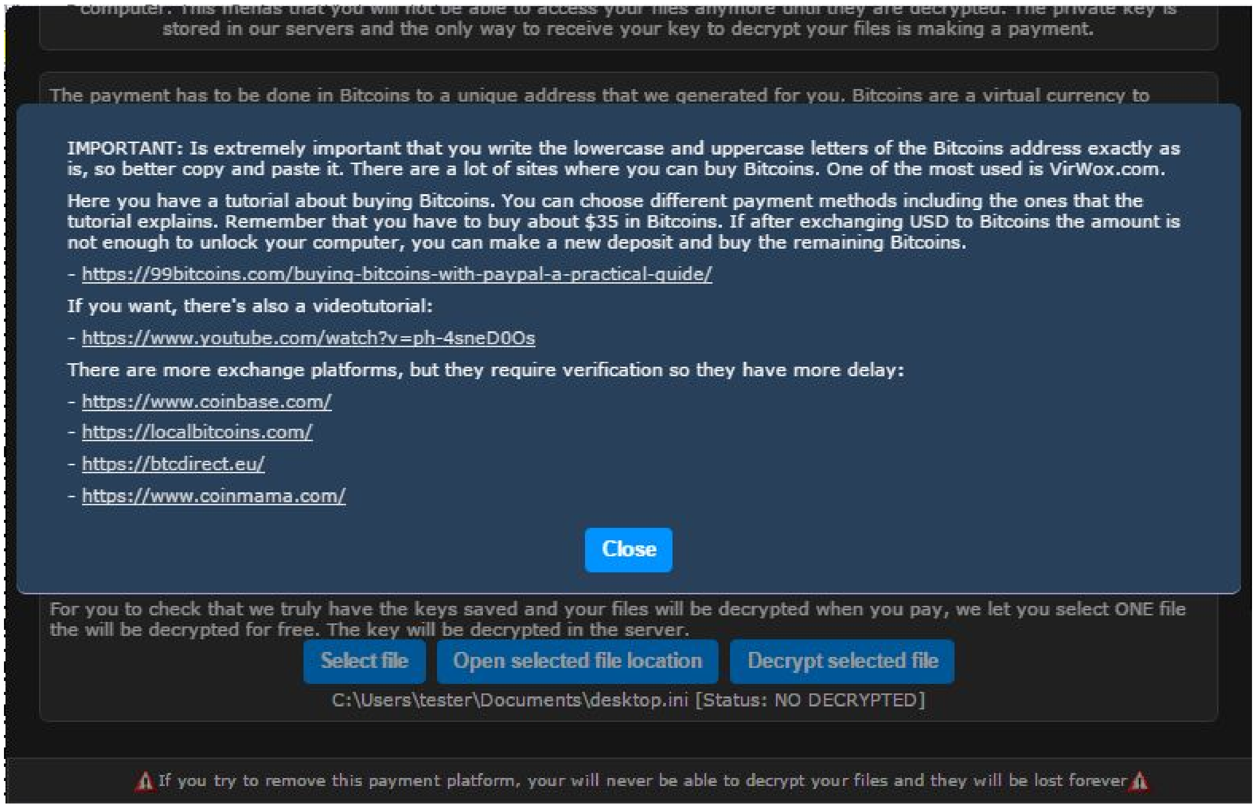
`17Yk44g4RMJ82yaiyyQHCWwpywkyTJ5398`

For you to check that we truly have the keys saved and your files will be decrypted when you pay, we let you select ONE file the will be decrypted for free. The key will be decrypted in the server.

C:\Users\tester\Documents\desktop.ini [Status: NO DECRYPTED]

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

Users who don't know how to use bitcoins are provided with extensive list of helpful links, available after clicking the button "How to buy Bitcoins":


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

IMPORTANT: Is extremely important that you write the lowercase and uppercase letters of the Bitcoins address exactly as is, so better copy and paste it. There are a lot of sites where you can buy Bitcoins. One of the most used is VirWox.com.

Here you have a tutorial about buying Bitcoins. You can choose different payment methods including the ones that the tutorial explains. Remember that you have to buy about $35 in Bitcoins. If after exchanging USD to Bitcoins the amount is not enough to unlock your computer, you can make a new deposit and buy the remaining Bitcoins.

- https://99bitcoins.com/buying-bitcoins-with-paypal-a-practical-guide/

If you want, there's also a videotutorial:

- https://www.youtube.com/watch?v=ph-4sneD0Os

There are more exchange platforms, but they require verification so they have more delay:

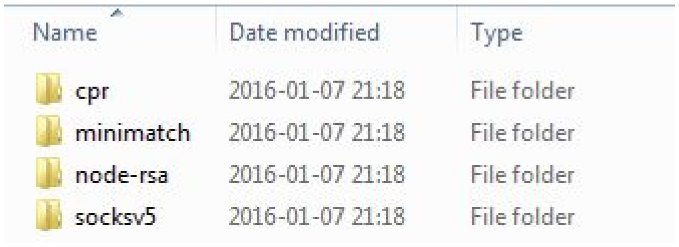
- https://www.coinbase.com/
- https://localbitcoins.com/
- https://btcdirect.eu/
- https://www.coinmama.com/

For you to check that we truly have the keys saved and your files will be decrypted when you pay, we let you select ONE file the will be decrypted for free. The key will be decrypted in the server.

C:\Users\tester\Documents\desktop.ini [Status: NO DECRYPTED]

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

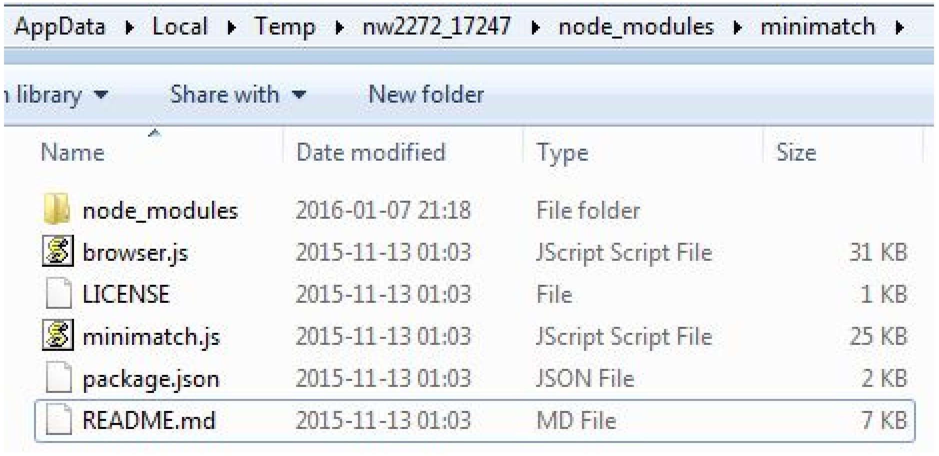
Other used elements are in the folder ***node_modules*** (written in NodeJS):



Name	Date modified	Type
cpr	2016-01-07 21:18	File folder
minimatch	2016-01-07 21:18	File folder
node-rsa	2016-01-07 21:18	File folder
socksv5	2016-01-07 21:18	File folder

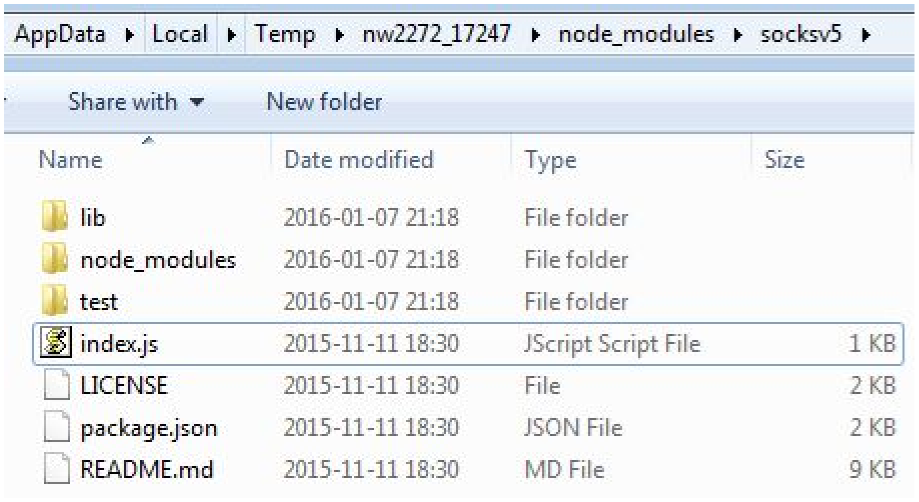
It uses open source components:

- minimatch: https://github.com/isaacs/minimatch


AppData ▸ Local ▸ Temp ▸ nw2272_17247 ▸ node_modules ▸ minimatch ▸

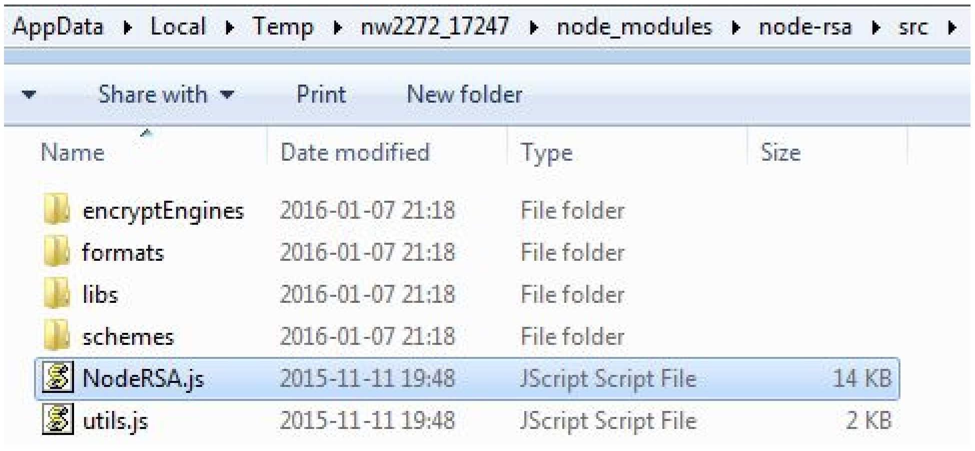
Name	Date modified	Type	Size
node_modules	2016-01-07 21:18	File folder	
browser.js	2015-11-13 01:03	JScript Script File	31 KB
LICENSE	2015-11-13 01:03	File	1 KB
minimatch.js	2015-11-13 01:03	JScript Script File	25 KB
package.json	2015-11-13 01:03	JSON File	2 KB
README.md	2015-11-13 01:03	MD File	7 KB

- socks5: https://github.com/mscdex/socksv5


AppData ▸ Local ▸ Temp ▸ nw2272_17247 ▸ node_modules ▸ socksv5 ▸

Name	Date modified	Type	Size
lib	2016-01-07 21:18	File folder	
node_modules	2016-01-07 21:18	File folder	
test	2016-01-07 21:18	File folder	
index.js	2015-11-11 18:30	JScript Script File	1 KB
LICENSE	2015-11-11 18:30	File	2 KB
package.json	2015-11-11 18:30	JSON File	2 KB
README.md	2015-11-11 18:30	MD File	9 KB

- node-rsa : https://github.com/rzcoder/node-rsa/tree/master/src


AppData ▸ Local ▸ Temp ▸ nw2272_17247 ▸ node_modules ▸ node-rsa ▸ src ▸

Name	Date modified	Type	Size
encryptEngines	2016-01-07 21:18	File folder	
formats	2016-01-07 21:18	File folder	
libs	2016-01-07 21:18	File folder	
schemes	2016-01-07 21:18	File folder	
NodeRSA.js	2015-11-11 19:48	JScript Script File	14 KB
utils.js	2015-11-11 19:48	JScript Script File	2 KB

Conclusion

In the past, malware authors cared mostly about small size of their applications – that’s why early viruses were written in assembler. Nowadays, technologies used and goals have changed. The most important consideration is not the size, but the ability to imitate legitimate applications, for the purpose of avoiding detection.

Authors of Ransom32 went really far in this direction. Their package is huge in comparison to typical samples. It consists of various elements, including legitimate applications – i.e the tor client (renamed to rundll32.exe). The technology that they have chosen for the core – Node JS – is a complete change of direction from the malware written in low-level languages.

However, compiled Java Script (although it works about 30 percent slower than not compiled) is not very popular and there is lack of tools to analyze it – which makes it a good point for malware authors, who gain some level of code protection.

Appendix

Other posts about **Ransom32**:

- by Emisoft
- by BleepingComputer

See also our posts about **other examples of ransomware**:

- Chimera
- TeslaCrypt