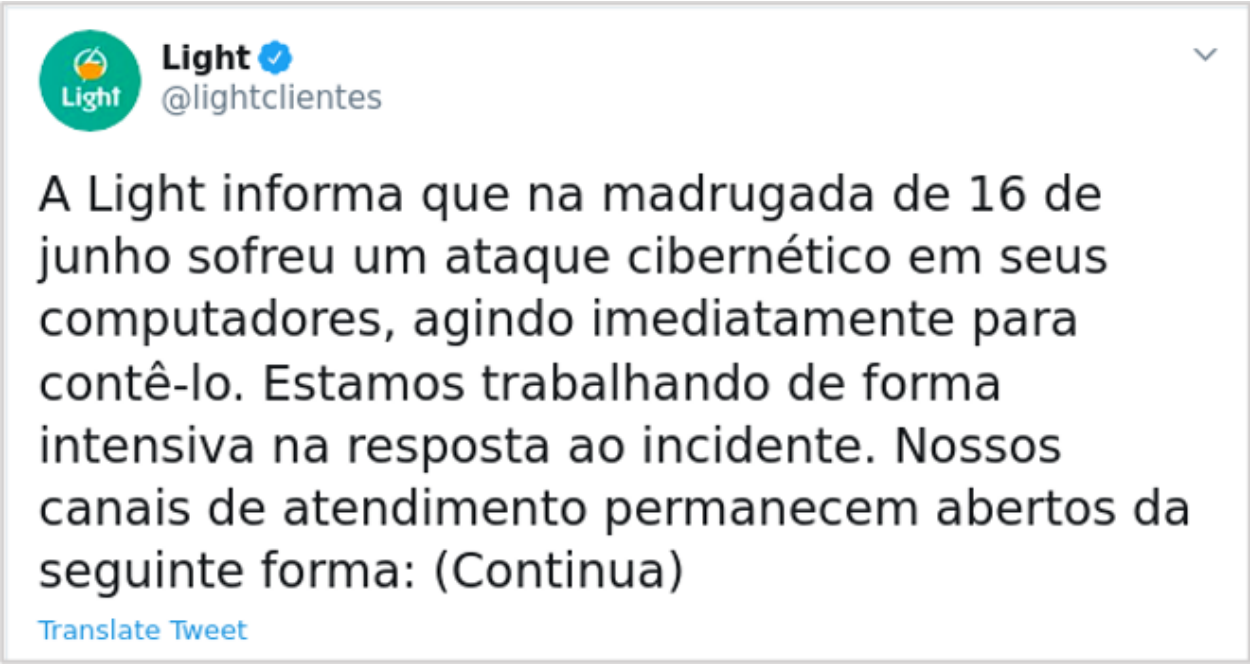
Electric Company Ransomware Attack

appgate.com/blog/electric-company-ransomware-attack-calls-for-14-million-in-ransom

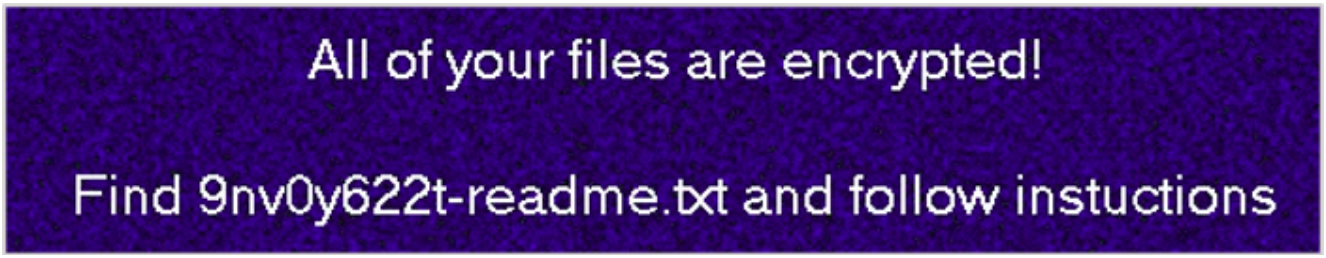
Light S.A., a Brazilian based electrical energy company was recently affected by ransomware where the cybercriminals demanded a payment of 14 million U.S. dollars.

The company issued comments to a local newspaper confirming the attack, however, technical details were not disclosed by the company.



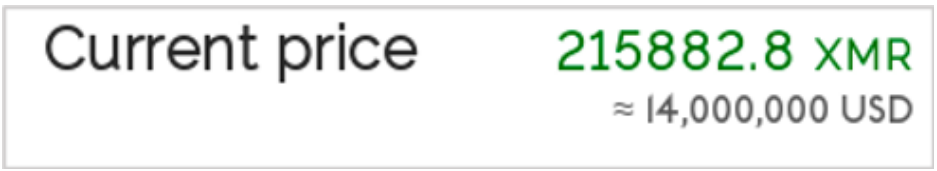
Twitter Post from Light SA Official Account, Confirming the Attack

Our malware analysis team had access to the binary that was likely used in the attack and we were able to confirm that the sample is from a family known as Sodinokibi (aka REvil). Althought we can't confirm that this was the exact same file used in the attack, the evidence points to being connected to the Light SA breach, such as the ransom price, for example. The sample was automatically collected by AppGate Labs on June 17, 2020 through our live hunting process, and as the binary was sent to a public sandbox, this suggests someone from the company submitted that file attempting to understand how it works.



Machine Infected with Sodinokibi Sample.

The sample is packed and works the same as other binaries that we have already identified from this family, and once unpacked, we were able to decrypt its configuration and access relevant data about the threat, such as the actor / campaign ID, and the URL in which the victim must access to get instructions.



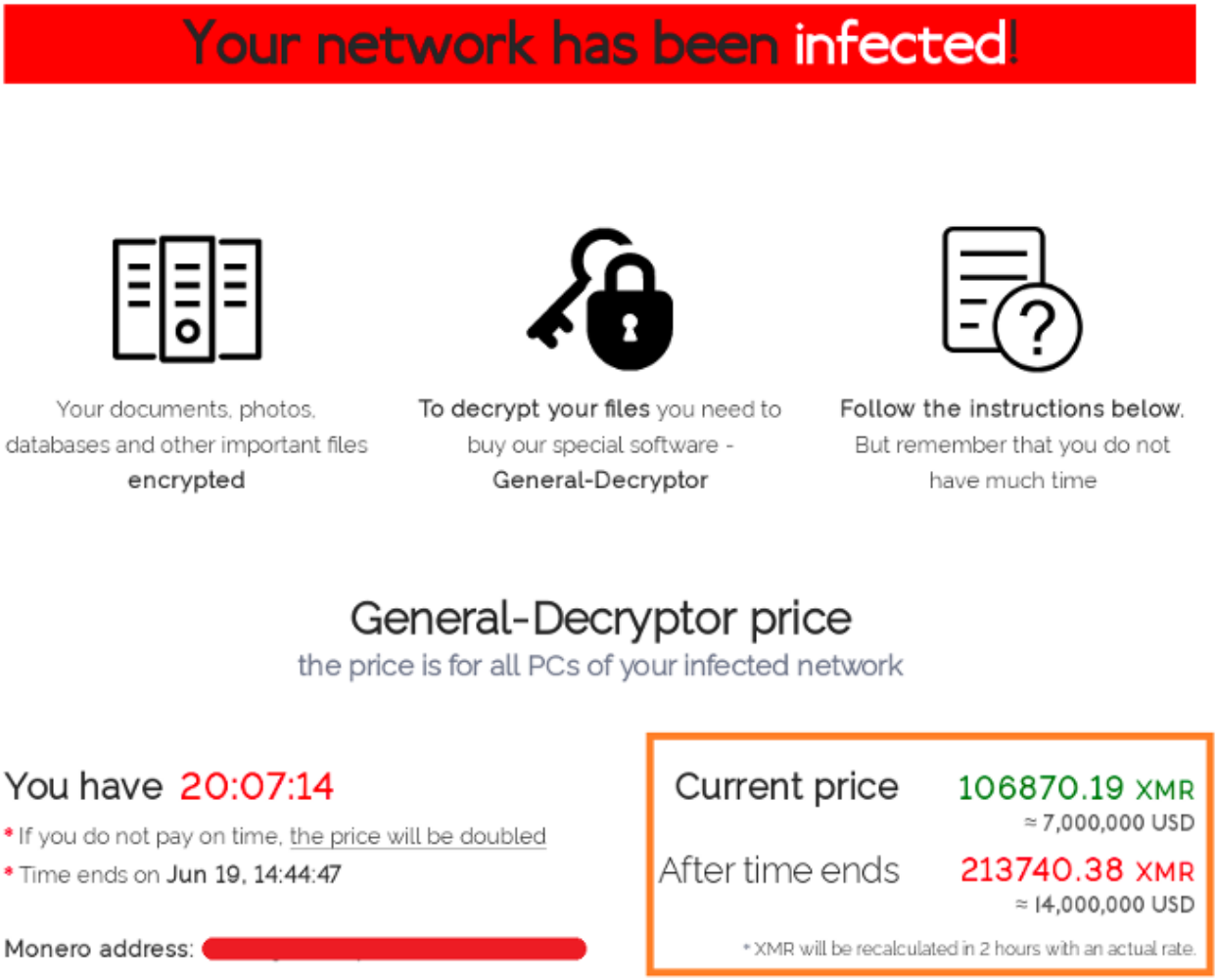
Ransomware Attack Asking 14,000,000 USD.

According to the page that is hosted in the deep web, the ransom amount must be paid using the

virtual currency Monero, and prior to June 19, the total was 106,870.19 XMR, which is equivalent to 7 million USD. However, since the deadline has passed, the price has doubled to 14 million US dollars. The whole attack looks very professional, the web page even includes a chat support, where the victim can speak directly with the attacker. Sodinokibi works as a RaaS (Ransomware as a Service) model, and the group behind the operation seems to be affiliated to "Pinchy Spider", which is the same group behind GandCrab ransomware[1].

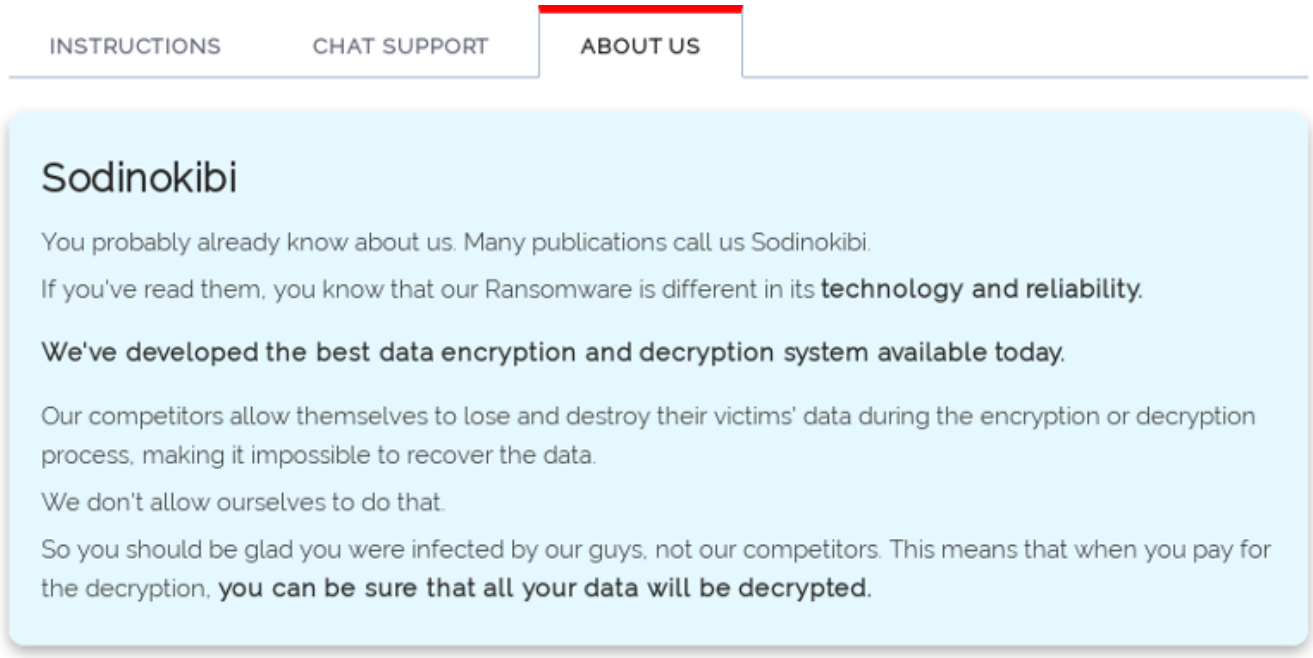
Deep Web Panel

With the URL collected from the binary, we were able to access the webpage (hosted on deep web) and confirm details about the attack. First thing of notice is the ransom price, which is extremely high and likely due to the affected company belonging to an important sector.



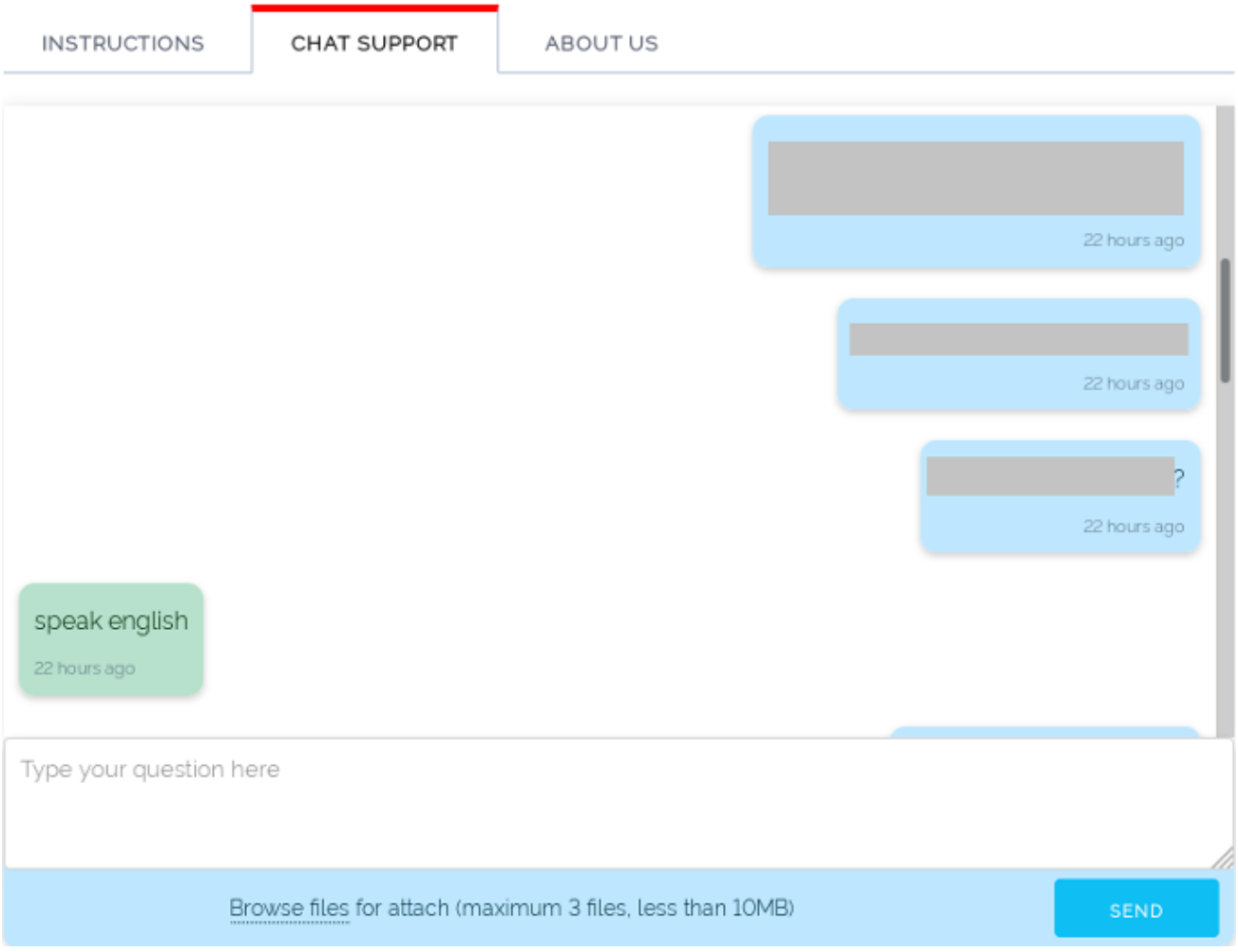
Ransomware Asking for 7,000,000 USD Before Deadline.

There is an ‘About Us’ which contains a small overview about the Sodinokibi family.



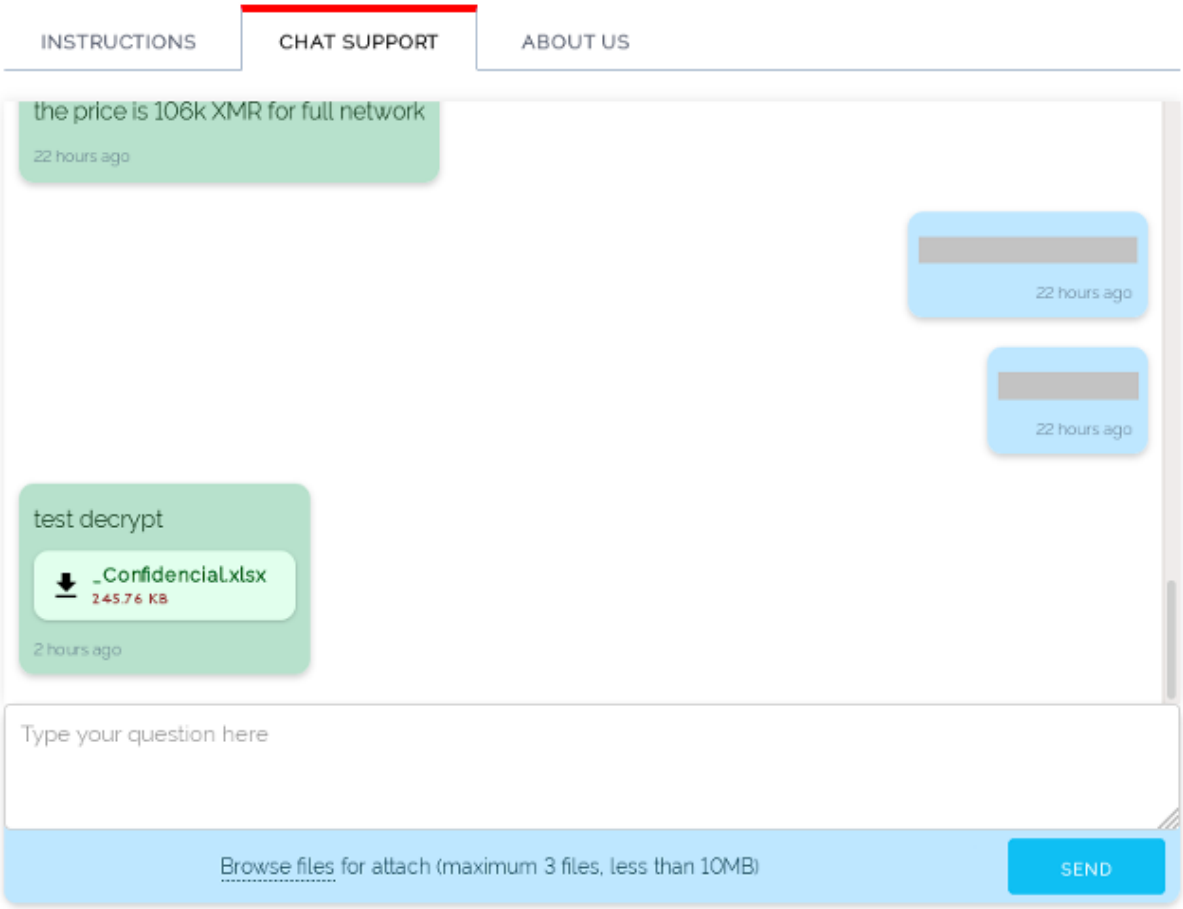
Sodinokibi Description According to the Web Page.

Also, it provides an online chat support, where the victim can interact with the attackers. In the images below, we can see that someone reached out to the attacker. We decided to censor the images to reduce the exposure of the person involved.



Sodinokibi Chat Support.

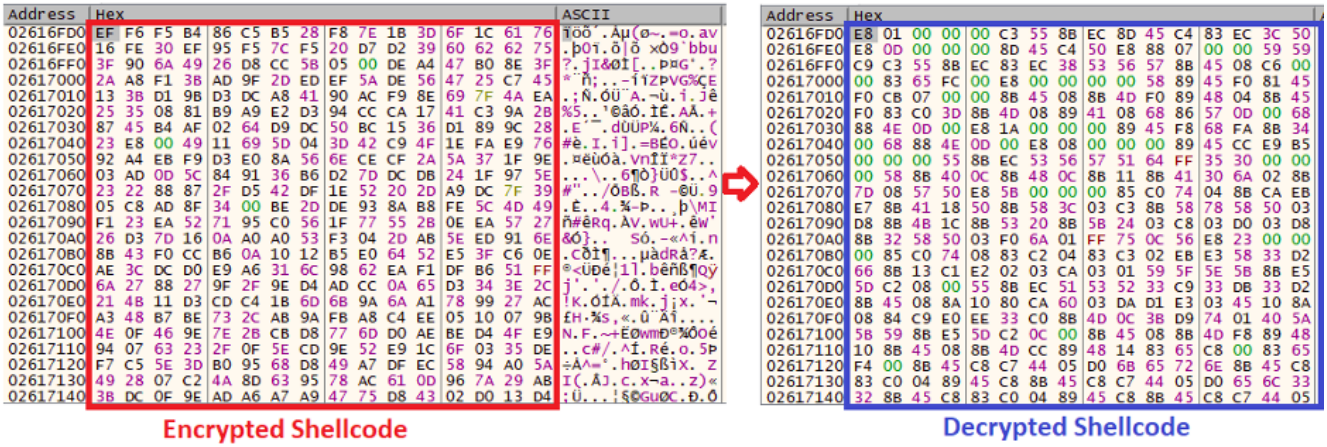
At the end of the chat we can see that the attacker sends a file that is supposedly confidential, proving to the victim that the data can be decrypted and also suggesting that file was probably stolen from the company's network.



Decrypted "_Confidencial.xlsx" File Sent by Attacker.

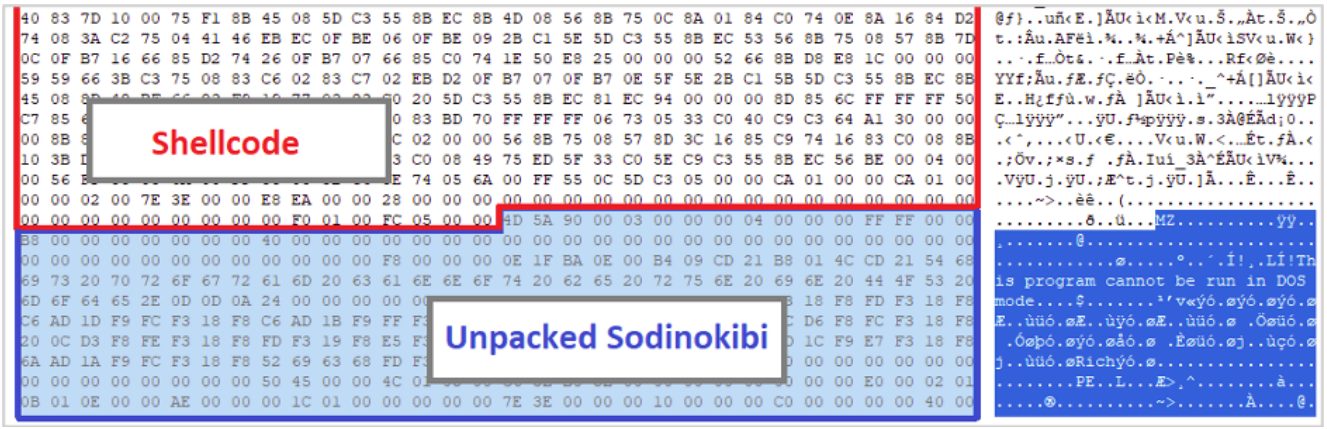
Technical Details

The main file is packed and it uses two shellcodes streams for unpacking and execution process. First, it allocates a memory space using "LocalAlloc[2]" API, writes an encrypted shellcode to it, and transfers execution once decrypted.



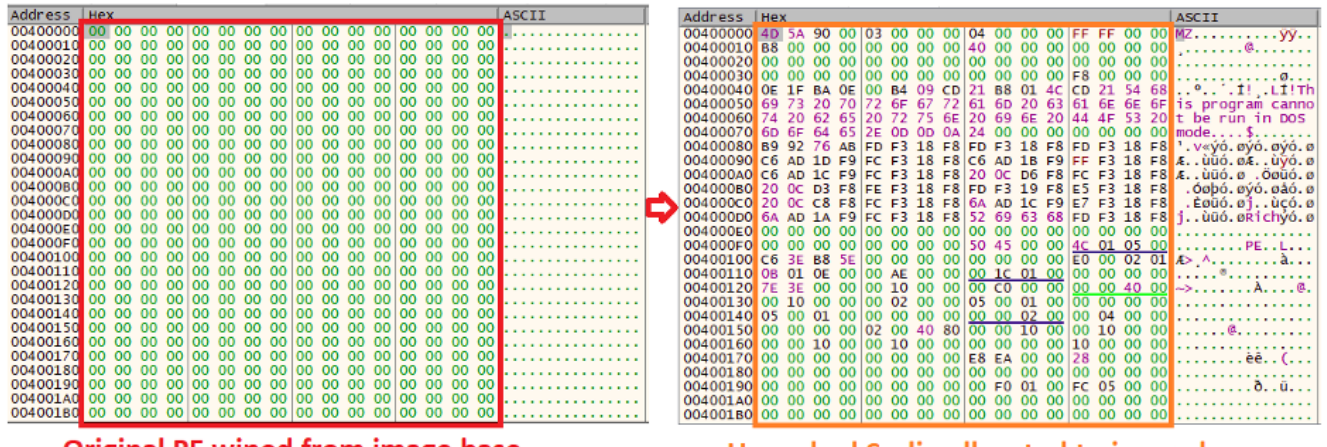
Sodinokibi Decrypting First Shellcode.

This shellcode unpacks Sodinokibi along with a second shellcode, which will eventually load the final binary to memory.



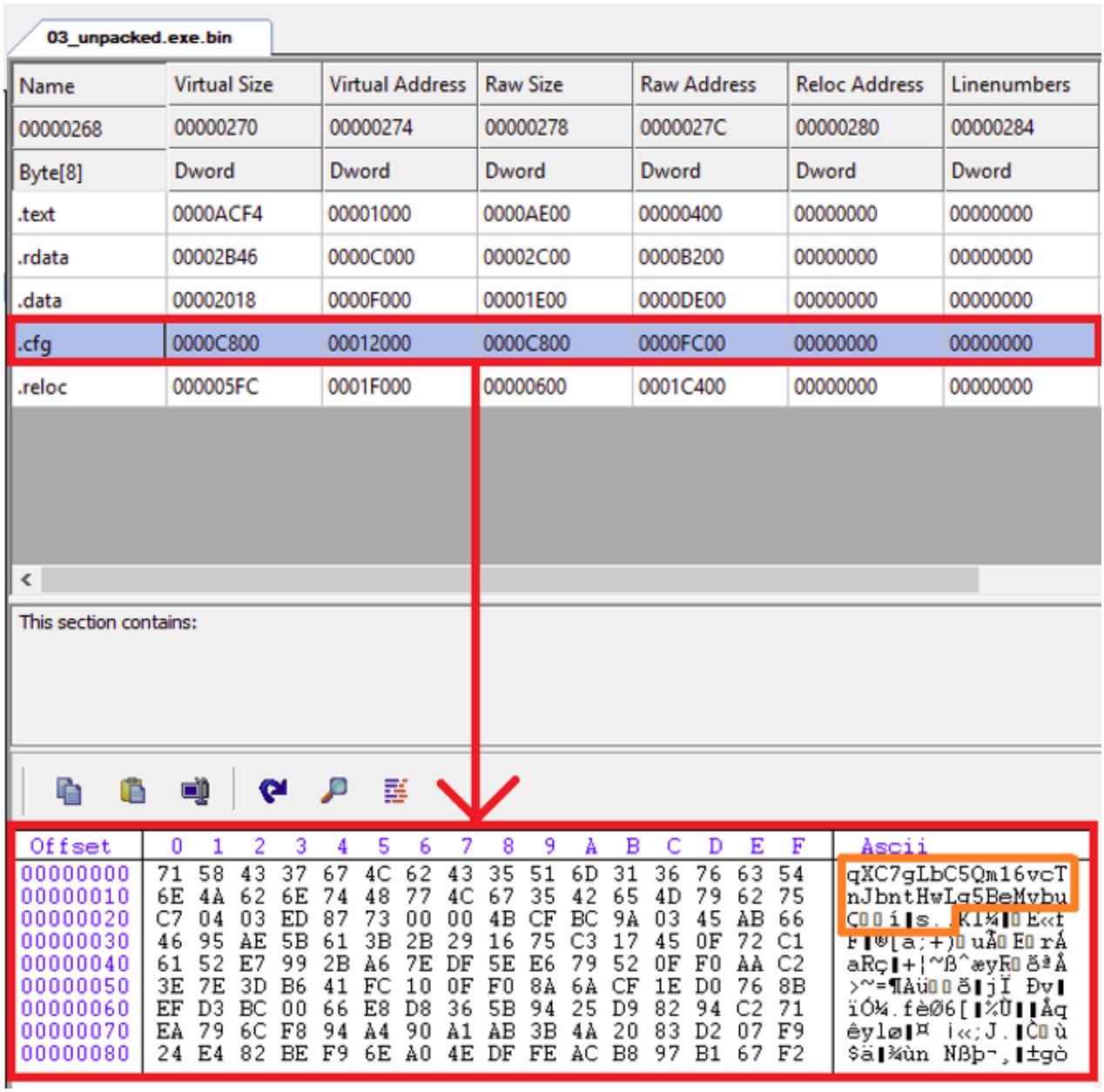
Second Shellcode Along with Unpacked Sodinokibi.

Finally, the shellcode injects the unpacked Sodinokibi binary into the same process space, by wiping the original PE file from memory and writing the new PE.



Sodinokibi Self-Injection.

The binary is highly configurable, the setting is encrypted with RC4 and it's usually stored in a randomly named section, and in this case the section name is ".cfg".



03_unpacked.exe.bin

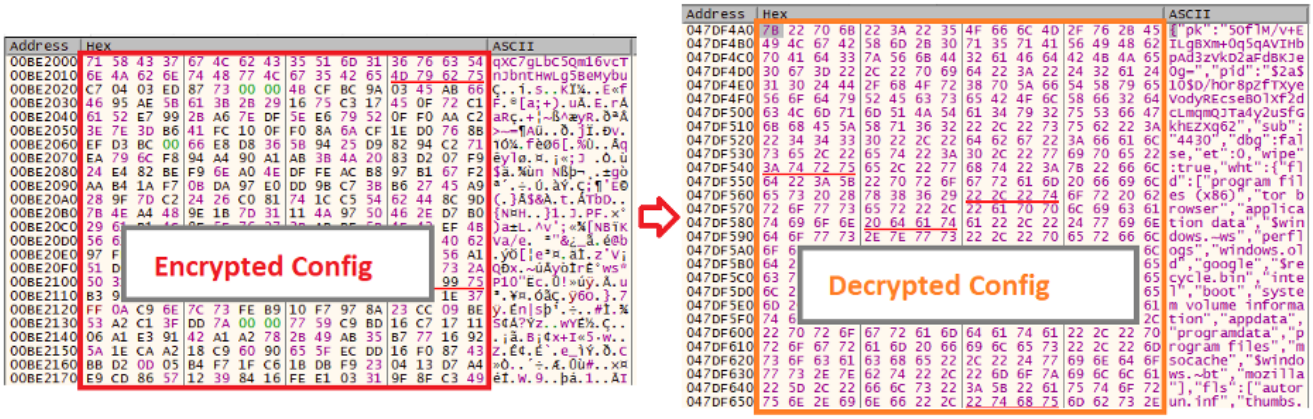
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers
00000268	00000270	00000274	00000278	0000027C	00000280	00000284
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword
.text	0000ACF4	00001000	0000AE00	00000400	00000000	00000000
.rdata	00002B46	0000C000	00002C00	0000B200	00000000	00000000
.data	00002018	0000F000	00001E00	0000DE00	00000000	00000000
.cfg	0000C800	00012000	0000C800	0000FC00	00000000	00000000
.reloc	000005FC	0001F000	00000600	0001C400	00000000	00000000

This section contains:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	71	58	43	37	67	4C	62	43	35	51	6D	31	36	76	63	54	qXC7gLbC5Qm16vcT
00000010	6E	4A	62	6E	74	48	77	4C	67	35	42	65	4D	79	62	75	nJbntHwLg5BeMybu
00000020	C7	04	03	ED	87	73	00	00	4B	CF	BC	9A	03	45	AB	66	Ç□□í‡s..KÏ¼š□E«f
00000030	46	95	AE	5B	61	3B	2B	29	16	75	C3	17	45	0F	72	C1	F•®[a;+)□uÃ□E□rÁ
00000040	61	52	E7	99	2B	A6	7E	DF	5E	E6	79	52	0F	F0	AA	C2	aRç™+¦~ß^æyR□ð ªÂ
00000050	3E	7E	3D	B6	41	FC	10	0F	F0	8A	6A	CF	1E	D0	76	8B	>~=¶Aü□□ð‡jÏ Ðv‡
00000060	EF	D3	BC	00	66	E8	D8	36	5B	94	25	D9	82	94	C2	71	ïÓ¼.fèØ6[‡%Ù‡‡Âq
00000070	EA	79	6C	F8	94	A4	90	A1	AB	3B	4A	20	83	D2	07	F9	êylø‡¤ ¡«;J.‡Ò□ù
00000080	24	E4	82	BE	F9	6E	A0	4E	DF	FE	AC	B8	97	B1	67	F2	$ä‡¾ùn NßÞ¬¸‡±gò

Sodinokibi Encrypted Configuration Stored on PE Section.

Upon execution, it will decrypt the content of this section into an allocated memory space.



Sodinokibi Decrypting its Configuration.

The decrypted configuration is presented in a JSON format and contains several options used by the Malware.

Key	Type	Description
dbg	Boolean	If true, ignores keyboard layout check
dmn	List of strings	List of domains for communication (C2 servers)
exp	Boolean	If true, enables privilege escalation using CVE-2018-8453 as exploit
fast	Boolean	If true, it encrypts just a part of the file
img	String	Message displayed on desktop background
nbody	String	Contents of the “readme” file (base64 encoded)
net	Boolean	If true, sends POST requests to the C2 servers
nname	String	Name of “readme” file
pid	String	Actor ID
pk	String	Public encryption key (base64 encoded)
prc	List of strings	Process to terminate

sub	String	Campaign ID
wfld	List of strings	List of folders to wipe
wht	Dictionary	Contains information about whitelist (to skip encryption)
wht.ext	List of strings	Whitelisted extensions
wht.fld	List of strings	Whitelisted folders
wht.fls	List of strings	Whitelisted files
wipe	Boolean	If true, wipes the folders specified in “wfld”

An interesting capability not utilized by this specific sample is if “exp” is “true”, it tries to escalate privileges by exploiting a vulnerability in “win32k.sys” (CVE-2018-8453[3]) with both 32-bit and 64-bit versions of the exploit, using a technique known as “Heaven’s Gate[4]” to execute 64 bit code in a 32 bit process, located in the “.rdata” section of the PE file.

```
call sodin.F6E3C46          Copies encrypted shellcode to a recently allocated memory
push edi
push esi
push edi
push dword ptr ss:[ebp-4]
push dword ptr ss:[ebp-8]
call sodin.F6E59C2          Decrypts the shellcode
add esp,20
push dword ptr ss:[ebp+8]
call edi                    Calls the entry point of the shellcode
```

Code Decrypting and Executing the Shellcode.

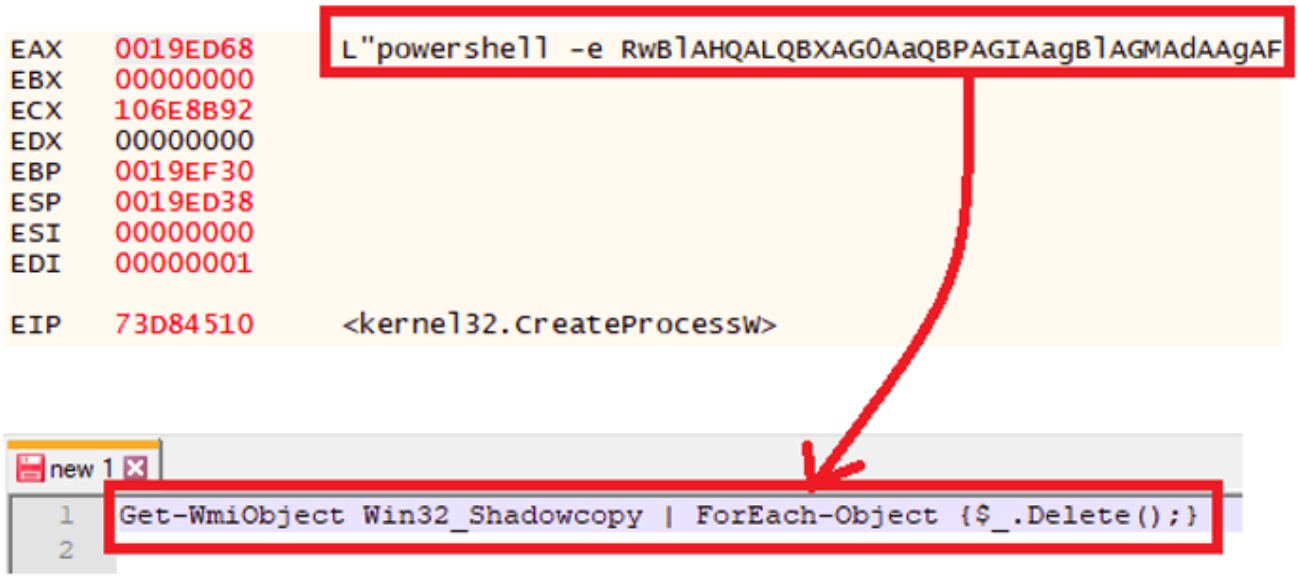
Also, if the “dbg” option is set to “false”, the malware will check the UI language and the keyboard layout of the infected machine.

```
mov dword ptr ss:[ebp-48],419    Russian
mov dword ptr ss:[ebp-44],422    Ukrainian
mov dword ptr ss:[ebp-40],423    Belarusian
mov dword ptr ss:[ebp-3C],428    Tajik
mov dword ptr ss:[ebp-38],42B    Armenian
mov dword ptr ss:[ebp-34],42C    Azeri
mov dword ptr ss:[ebp-30],437    Georgian
mov dword ptr ss:[ebp-2C],43F    Kazakh
mov dword ptr ss:[ebp-28],440    Kygyz
mov dword ptr ss:[ebp-24],442    Turkmen
mov dword ptr ss:[ebp-20],443    Uzbek
mov dword ptr ss:[ebp-1C],444    Tatar
mov dword ptr ss:[ebp-18],818    Romanian
mov dword ptr ss:[ebp-14],819    Russian
mov dword ptr ss:[ebp-10],82C    Azerbaijani
mov dword ptr ss:[ebp-C],843     Uzbek
mov dword ptr ss:[ebp-8],45A     Syriac
mov dword ptr ss:[ebp-4],2801    Arabic Syria
call dword ptr ds:[<&GetUserDefaultUILanguage>]
```

Keyboard Layout Verification.

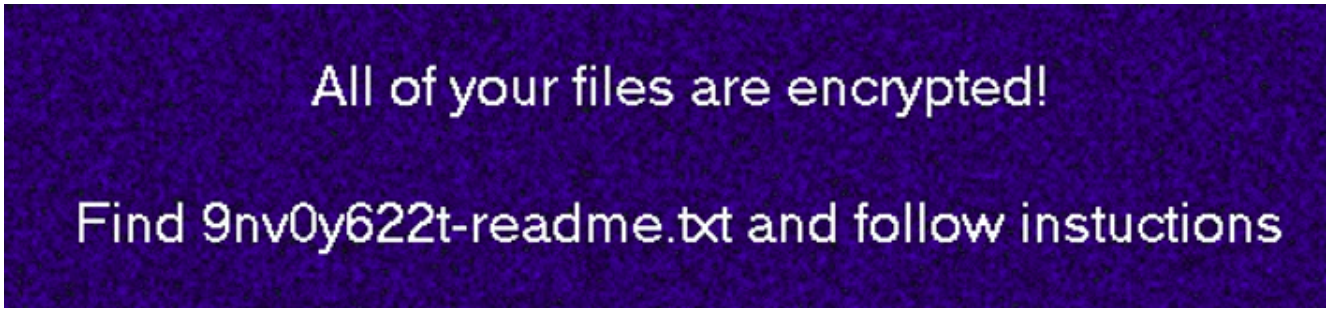
Above, we can see that this Ransomware has a whitelist based on location, if the return value[5] matches any value of the list, it will not encrypt files in the machine.

Furthermore, it uses PowerShell to delete Windows shadow copies.



Sodinokibi Deleting Windows Shadow Copies.

Once encrypting all the files, it changes the background with the following image:



Sodinokibi Background.

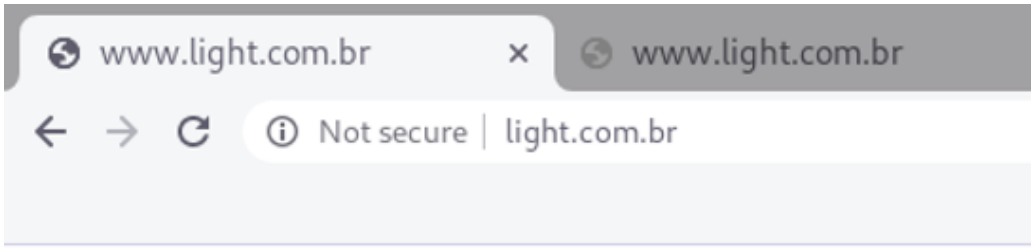
Lastly, it appends a ransom note to every folder where encrypted files can be found.

```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your system
has extension 1n3u310.
By the way, everything is possible to recover (restore), but you need to follow our
instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting
benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not
in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one
file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your
time and data, cause just we have the private key. In practice - time is much more valuable than
money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website:
  http://a                                                  oyd.onion/

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For
this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decryptor.cc

Warning: secondary website can be blocked, thats why first variant much better and more
available.
```

Sodinokibi Ransom Note.

Unfortunately, there is no global decryptor for the family, which means that the attacker's private key is required to decrypt the files.

During the period of the attack, we noticed that the company's website was offline, presenting an error message related to the database, which could be related to the attack.



Light WebSite Offline During Ransomware Attack.

IOCs

SHA1:

f09e5e72b433d11a32efe2e5d63db0bc7b8def59

SHA256:

140f831ddd180861481c9531aa6859c56503e77d29d00439c1e71c5b93e01e1a

SSDEEP:

3072:oCc99moUMXv84IHesgkSx+oN/7KzTKDyOX6wKamrJPlM8dj09br:oCc9wHRtg9xkNq6wK7dq40

Mutex:

Global\57E6EA0F-4648-EF95-9F98-C3221B4D31F9

Registry Keys:

HKLM\SOFTWARE\Facebook_Assistant\s17

HKLM\SOFTWARE\Facebook_Assistant\JYhB

HKLM\SOFTWARE\Facebook_Assistant\jH5dJ

HKLM\SOFTWARE\Facebook_Assistant\nsWSeU

HKLM\SOFTWARE\Facebook_Assistant\CSGtvzp

HKLM\SOFTWARE\Facebook_Assistant\cDQ1QZoS

Sodinokibi Actor ID

$2a$10$D/hOr8pZfTXyeVodyREcseBOlXf2dcLmqmQJTa4y2uSfGkhEZXq62

Sodinokibi Campaign ID

4430

Public Encryption Key (base64 encoded)

5OfIM/v+EILgBXm+0q5qAVIHbpAd3zVkD2aFdBKJe0g=

C2 Servers:

Please find a list here:

https://pastebin.com/nf0i13zc

[1] https://malpedia.caad.fkie.fra...

[2] https://docs.microsoft.com/en-...

[3] https://www.cvedetails.com/cve...

[4] http://www.alex-ionescu.com/?p...

[5] https://docs.microsoft.com/en-...