

# Electric Company Ransomware Attack

---

 [appgate.com/blog/electric-company-ransomware-attack-calls-for-14-million-in-ransom](https://appgate.com/blog/electric-company-ransomware-attack-calls-for-14-million-in-ransom)



appgate

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.



**Light** ✓  
@lightclientes



A Light informa que na madrugada de 16 de junho sofreu um ataque cibernético em seus computadores, agindo imediatamente para contê-lo. Estamos trabalhando de forma intensiva na resposta ao incidente. Nossos canais de atendimento permanecem abertos da seguinte forma: (Continua)

[Translate Tweet](#)

*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). Although 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.

All of your files are encrypted!

Find 9nv0y622t-readme.txt and follow instructions

*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.

Current price

**215882.8 XMR**

≈ 14,000,000 USD

*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.

**Your network has been infected!**



Your documents, photos, databases and other important files **encrypted**



To decrypt your files you need to buy our special software - **General-Decryptor**



Follow the instructions below. But remember that you do not have much time

## General-Decryptor price

the price is for all PCs of your infected network

You have **20:07:14**

- \* If you do not pay on time, the price will be doubled
- \* Time ends on Jun 19, 14:44:47

Monero address: [REDACTED]

Current price	<b>106870.19 XMR</b> ≈ 7,000,000 USD
After time ends	<b>213740.38 XMR</b> ≈ 14,000,000 USD

\* XMR will be recalculated in 2 hours with an actual rate.

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

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

## Sodinokibi

You probably already know about us. Many publications call us Sodinokibi.

If you've read them, you know that our Ransomware is different in its **technology and reliability**.

**We've developed the best data encryption and decryption system available today.**

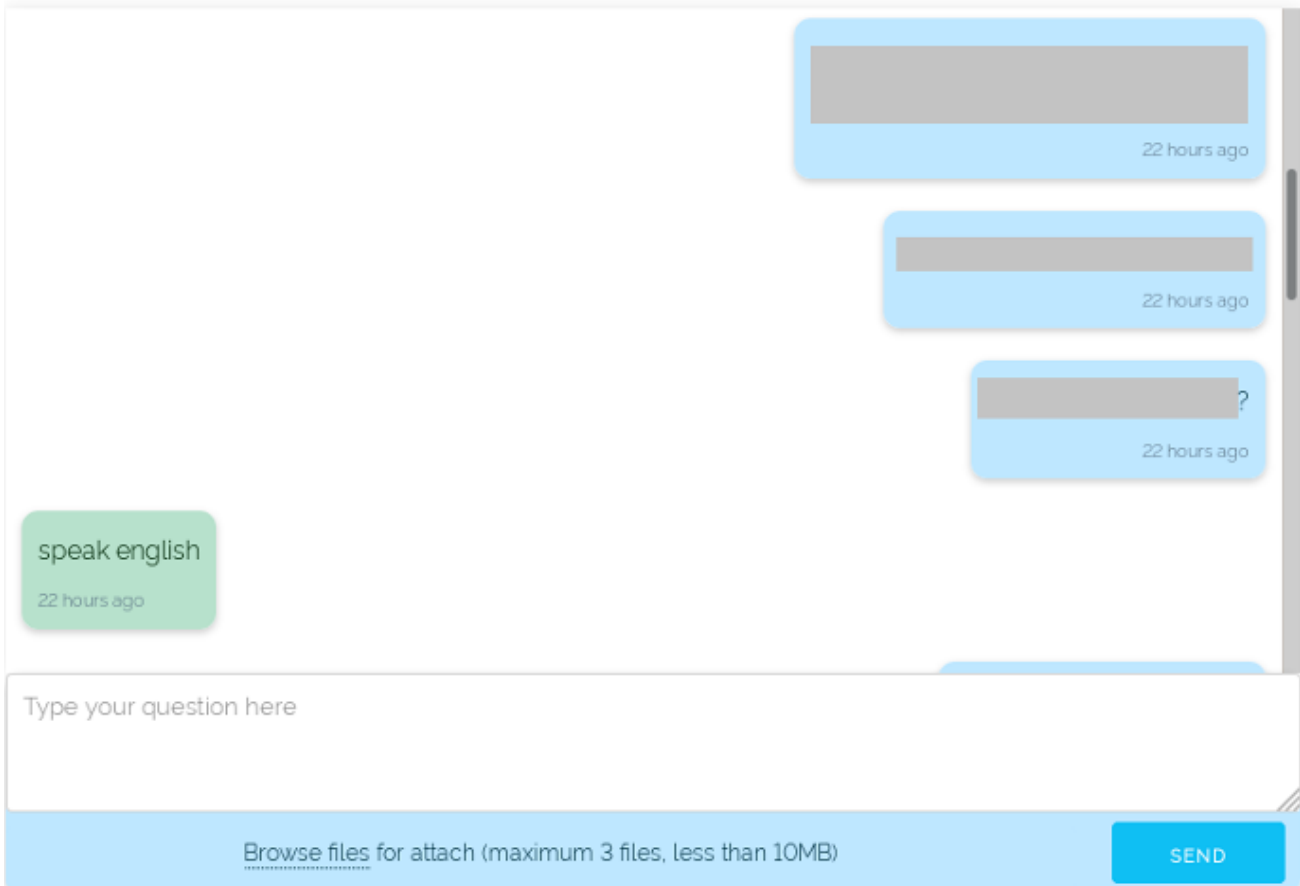
Our competitors allow themselves to lose and destroy their victims' data during the encryption or decryption process, making it impossible to recover the data.

We don't allow ourselves to do that.

So you should be glad you were infected by our guys, not our competitors. This means that when you pay for the decryption, **you can be sure that all your data will be decrypted.**

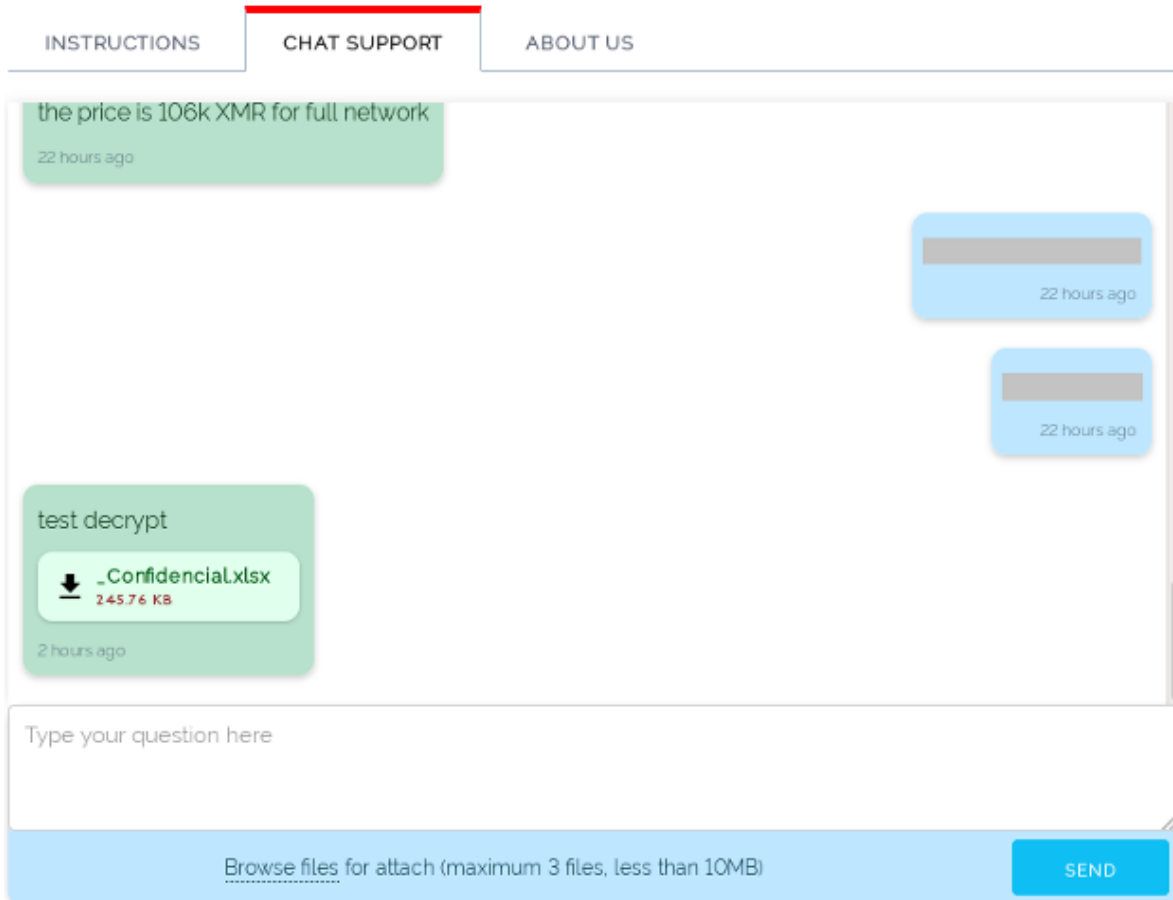
*Sodinokibi Description According to the Web Page.*

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.

Address	Hex	ASCII
02616FD0	EF F6 F5 B4 86 C5 B5 28 F8 7E 1B 3D 6F 1C 61 76	!oo .Au(oo=-o.av
02616FE0	16 FE 30 EF 95 F5 7C F5 20 D7 D2 39 60 62 62 75	.p01.0]0 x09'bbu
02616FF0	3F 90 6A 49 26 D8 CC 58 05 00 DE A4 47 80 8E 3F	? .I&0! .p%g'?
02617000	2A A8 F1 38 AD 9F 2D ED EF 5A DE 56 47 25 C7 45	'N;...-iizPV%CE
02617010	13 38 D1 98 D3 DC A8 41 90 AC F9 8E 69 7F 4A EA	.;N.OU'A.-u.i.je
02617020	25 35 08 81 B9 A9 E2 D3 94 CC A4 17 41 C3 9A 2B	%S.'eao.IE.AA.+
02617030	87 45 84 AF 02 64 D9 DC 50 8C 15 36 D1 89 9C 28	.E.'duup%.6N.(
02617040	23 E8 00 49 11 69 5D 04 3D 42 C9 4F 1E FA E9 76	#e.I.ij=-8EO.uév
02617050	92 A4 EB F9 03 91 36 86 D2 7D DC DB 24 1F 97 5E	#e.uoA.vnii*27..
02617060	03 AD E0 5C 84 91 36 86 D2 7D DC DB 24 1F 97 5E	'...6]0]05..A
02617070	23 22 88 87 2F D5 42 DF 1E 52 20 2D A9 DC 7F 39	#"...0]B.R.-eU.9
02617080	05 C8 AD 8F 34 00 BE 2D DE 93 8A 88 FE 5C 4D 49	.E.4.%p-.p]MI
02617090	F1 23 EA 52 71 95 C0 56 1F 77 55 2B 0E EA 57 27	n#eRq.AV.wu+ew'
026170A0	26 D3 7D 16 0A A0 A0 53 F3 04 2D AB 5E ED 91 6E	&O].S0.«A1.n
026170B0	88 43 F0 CC B6 0A 10 12 B5 E0 64 52 E5 3F C6 0E	.c0]1...jadrA%.
026170C0	AE 3C DC D0 E9 A6 31 6C 98 62 EA F1 DF B6 51 FF	*<Upe]11.benBtoy
026170D0	6A 27 88 27 9F 2F 9E D4 AD CC 0A 65 D3 34 3E 2C	j'.../O.I.e04>
026170E0	21 48 11 03 CD C4 18 6D 68 9A 6A A1 78 99 27 AC	'K.OIA.mk.;j;x.-
026170F0	A3 48 87 BE 73 2C AB 9A FB A8 C4 EE 05 10 07 9B	#eH.%s.«.U'A1...
02617100	4E 0F 46 9E 7E 2B CB D8 77 6D 0A AE BE D4 4F E9	N.F.->Eowm0%0e
02617110	94 07 63 23 2F 0F 5E C0 9E 52 E9 1C 6F 03 35 DE	..c#/.A1.RE.o.5P
02617120	F7 5 C 5E 3D 80 95 68 D8 49 A7 DF EC 58 94 A0 5A	=AA=/.h0]5]Bix.Z
02617130	49 28 07 C2 4A 8D 63 95 78 AC 61 0D 96 7A 29 AB	I(.Aj.c.x-a.z)<
02617140	38 DC 0F 9E AD A6 A7 A9 47 75 D8 43 02 D0 13 04	:U...i]eGuoc.#0.

Encrypted Shellcode

Address	Hex	ASCII
02616FD0	E8 01 00 00 00 C3 55 8B EC 8D 45 C4 83 EC 3C 50	
02616FE0	E8 0D 00 00 00 8D 45 C4 50 E8 88 07 00 00 59 59	
02616FF0	C9 C3 55 8B EC 83 EC 38 53 56 57 8B 45 08 C6 00	
02617000	08 83 65 FC 00 0E 00 00 00 58 89 45 F0 81 45	
02617010	F0 CB 07 00 00 8E 45 08 8E 4D F0 89 48 08 8E 45	
02617020	F0 83 C0 3D 8B 4D 08 89 41 08 68 8E 57 0D 00 68	
02617030	88 4E 0D 00 E8 1A 00 00 00 89 45 F8 68 FA 8B 34	
02617040	00 68 88 4E 0D 00 E8 08 00 00 00 89 45 CC E9 85	
02617050	00 00 00 55 8B EC 53 56 57 51 64 FF 35 30 00 00	
02617060	00 58 88 40 0C 8E 48 0C 8E 11 8E 41 30 6A 02 8B	
02617070	7D 08 57 50 E8 5B 00 00 00 85 C0 74 04 8A C4 EB	
02617080	E7 8B 41 18 50 8B 58 3C 03 8B 58 78 58 50 03 D8	
02617090	D8 8B 48 1C 8B 53 20 8B 58 24 03 C8 03 00 03 03	
026170A0	88 32 58 50 03 F0 6A 01 FF 75 0C 56 E8 23 00 00	
026170B0	00 85 C0 74 08 F3 C2 04 83 C3 02 EB E3 58 33 D2	
026170C0	66 8B 13 C1 E2 02 03 CA 01 01 59 5F 5E 58 8E 5E	
026170D0	5D C2 08 00 55 8B EC 53 52 33 C9 33 DB 33 D2	
026170E0	8B 45 08 8A 10 80 CA 60 03 DA D1 E3 03 45 10 8A	
026170F0	08 84 C9 E0 EE 33 C0 8D 4D 0C 3B D9 74 01 40 5A	
02617100	58 59 8E E5 5D C2 0C 00 8E 45 8B 4D F8 89 48	
02617110	10 8B 45 08 8B 4D CC 89 48 14 83 63 C8 00 83 65	
02617120	F4 00 8B 45 C8 C7 44 05 D0 6B 65 72 6E 8B 45 C8	
02617130	83 C0 04 89 45 C8 8B 45 C8 C7 44 05 D0 65 C6 33	
02617140	32 8B 45 C8 83 C0 04 89 45 C8 8B 45 C8 C7 44 05	

Decrypted Shellcode

Sodinokibi Decrypting First Shellcode.

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

40 83 7D 10 00 75 F1 8B 45 08 5D C3 55 8B EC 8B 4D 08 56 8B 75 0C 8A 01 84 C0 0E 8A 16 84 D2	@f).un<E.]AU<i<M.Vcu.S..At.S..O
74 08 3A C2 75 04 41 46 EB EC 0F BE 06 0F BE 09 2B C1 5E 5D C3 55 8B EC 53 56 8B 75 08 57 8B 7D	t.:Au.AFei.W..W.+A^]AU<iSV<u.W<
0C 0F B7 16 66 85 D2 74 26 0F B7 07 66 85 C0 71 1E 50 E8 25 00 00 00 52 66 8B D8 E8 1C 00 00 00	...f.Ots.'f.At.Pe&...Rf<@e....
59 59 66 3B C3 75 08 83 C6 02 83 C7 02 EB D2 0F B7 07 0F B7 0E 5F 5E 2B C1 5B 5D C3 55 8B EC 8B	YYf:AU.fE.fC.e0...^+A[]AU<i<
45 08 8B 4D 08 56 8B 75 0C 8A 01 84 C0 0E 8A 16 84 D2 08 56 8B 75 08 57 8B 7D	E...H2fU.w.fA ]AU<i.l.i".....lyyyf
C7 85 6C 00 00 00 00 00 83 BD 70 FF FF 0F 06 73 05 33 C0 49 C3 64 A1 30 00 00 00	Q...lyyy'...yU.fapyyy.s.3A@EAd;0..
00 8B 4D 08 56 8B 75 08 57 8B 75 0C 16 85 C9 74 16 83 C0 08 8B	..<^...U.<E...Vcu.W<...Et.fA<
10 3B D2 08 56 8B 75 08 57 8B 75 0C 16 85 C9 74 16 83 C0 08 8B	..<^;*.s.f .fA.Tui 3A^EAU<iv<...
00 56 8B 4D 08 56 8B 75 08 57 8B 75 0C 16 85 C9 74 16 83 C0 08 8B	.vYU.j.yU.;E^t.j.yU.]A...E...E...
00 00 02 00 7E 3E 00 00 E8 EA 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...>..e&..(.....00.00.00.00
00 00 00 00 00 00 00 00 F0 01 00 FC 05 00 00 4D 5A 90 00 03 00 00 00 04 00 00 FF FF 00 00	.....&.u...MZ.....yy..
8B 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....@.....
00 00	.....e.....°.....I].LI!Th
69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6E 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	is program cannot be run in DOS
C6 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	mode....\$......'v&y0.e.y0.e
D6 AD 1D F9 FC F3 18 F8 C6 AD 1B F9 FF F8	E..u00.eZ..u00.eZ..u00.e..0su0.e
20 0C D3 F8 FE F3 18 F8 FD F3 19 F8 E5 F8	.0p0.e.y0.e&0.e .Esu0.ej..u00.e
6A AD 1A F9 FC F3 18 F8 F2 63 68 FD F3 18 F8	j..u00.eRichy0.e.....
00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00	.....PE..L...>^.....à.....
0B 01 0E 00 00 AE 00 00 00 1C 01 00 00 00 00 00 00 00 00 7E 3E 00 00 10 00 00 00 C0 00 00 00 40 00	.....@.....>.....A....@.

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.

Address	Hex	ASCII
00400000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....yy..
00400010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....@.....
00400020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....e.....
00400030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....I].LI!Th
00400040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....t be run in DOS
00400050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	mode....\$......
00400060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....'v&y0.e.y0.e
00400070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....E..u00.e.u00.e.u00.e..0su0.e
00400080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	......0p0.e.y0.e&0.e .Esu0.ej..u00.e
00400090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....j..u00.eRichy0.e.....
004000A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....PE..L...>^.....à.....
004000B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....@.....>.....A....@.
004000C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....I].LI!Th
004000D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....t be run in DOS
004000E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	mode....\$......
004000F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....E..u00.e.u00.e.u00.e..0su0.e
00400100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	......0p0.e.y0.e&0.e .Esu0.ej..u00.e
00400110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....j..u00.eRichy0.e.....
00400120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....PE..L...>^.....à.....
00400130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....@.....>.....A....@.
00400140	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....I].LI!Th
00400150	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....t be run in DOS
00400160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	mode....\$......
00400170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....E..u00.e.u00.e.u00.e..0su0.e
00400180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	......0p0.e.y0.e&0.e .Esu0.ej..u00.e
00400190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....j..u00.eRichy0.e.....
004001A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....PE..L...>^.....à.....
004001B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....@.....>.....A....@.

Original PE wiped from image base

Unpacked Sodin allocated to image base

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	qXC7gIbC5Qm16vcT
00000010	6E	4A	62	6E	74	48	77	4C	67	35	42	65	4D	79	62	75	nJbntHwLq5BeMvbu
00000020	C7	04	03	ED	87	73	00	00	4B	CF	BC	9A	03	45	AB	66	C00 i!s. Kl%0 E<t
00000030	46	95	AE	5B	61	3B	2B	29	16	75	C3	17	45	0F	72	C1	F!@[a;+)0 uA0 E0 rA
00000040	61	52	E7	99	2B	A6	7E	DF	5E	E6	79	52	0F	F0	AA	C2	aRq + ~B^ayF0 8^A
00000050	3E	7E	3D	B6	41	FC	10	0F	F0	8A	6A	CF	1E	D0	76	8B	>~=%Au00 8!j! Dv!
00000060	EF	D3	BC	00	66	E8	D8	36	5B	94	25	D9	82	94	C2	71	i0% fe06[!%U!!Aq
00000070	EA	79	6C	F8	94	A4	90	A1	AB	3B	4A	20	83	D2	07	F9	èylø! i<<;J. !C0 ù
00000080	24	E4	82	BE	F9	6E	A0	4E	DF	FE	AC	B8	97	B1	67	F2	\$a!%ùn NBp~, !tgò

Sodinokibi Encrypted Configuration Stored on PE Section.

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

Address	Hex	ASCII
00BE2000	71 58 43 37	67 4C 62 43
00BE2010	6E 4A 62 6E	74 48 77 4C
00BE2020	C7 04 03 ED	87 73 00 00
00BE2030	46 95 AE 5B	61 3B 2B 29
00BE2040	61 52 E7 99	2B A6 7E DF
00BE2050	3E 7E 3D B6	41 FC 10 0F
00BE2060	EF D3 BC 00	66 E8 D8 36
00BE2070	EA 79 6C F8	94 A4 90 A1
00BE2080	24 E4 82 BE	F9 6E A0 4E
00BE2090	AA 84 1A F7	08 DA 97 E0
00BE20A0	28 9F 7D C2	24 26 C0 81
00BE20B0	7B 4E A4 48	9E 1B 70 31
00BE20C0	29 6E 81 4E	9E 5E 5E 33
00BE20D0	56 6	40 62
00BE20E0	97 F	56 A1
00BE20F0	51 D	73 2A
00BE2100	50 3	99 73
00BE2110	83 9	1E 37
00BE2120	FF 0A C9 6E	7C 73 FE B9
00BE2130	53 A2 C1 3F	DD 7A 00 00
00BE2140	06 A1 E3 91	42 A1 A2 78
00BE2150	5A 1E CA A2	18 C9 60 90
00BE2160	BB D2 0D 05	B4 F7 1F C6
00BE2170	E9 CD 86 57	12 39 84 16

**Encrypted Config**

Address	Hex	ASCII
047DF4A0	78 22 70 68	22 3A 22 35
047DF4B0	49 4C 67 42	58 6D 2B 30
047DF4C0	70 41 64 33	7A 56 68 44
047DF4D0	30 67 3D 22	2C 22 70 69
047DF4E0	31 30 24 44	2F 68 4F 72
047DF4F0	56 6F 64 79	52 45 63 73
047DF500	63 4C 6D 71	6D 51 4A 54
047DF510	68 68 45 5A	58 71 36 32
047DF520	22 34 34 33	30 22 2C 22
047DF530	73 65 2C 22	65 74 22 3A
047DF540	3A 74 22 75	65 2C 22 77
047DF550	64 22 3A 5B	22 70 72 6F
047DF560	65 73 20 28	78 38 36 29
047DF570	72 6F 77 73	65 72 22 2C
047DF580	74 69 6F 6E	20 64 61 74
047DF590	64 6F 77 73	2E 7E 77 73
047DF5A0	6F 6	6C 6
047DF5B0	64 2	65 2
047DF5C0	63 7	62 7
047DF5D0	6C 2	6D 2
047DF5E0	6D 2	6E 2
047DF5F0	74 6	75 6
047DF600	22 70 72 6F	67 72 61 6D
047DF610	72 6F 67 72	61 6D 20 66
047DF620	73 6F 63 61	63 68 65 22
047DF630	77 2E 7E 62	74 22 2C 22
047DF640	22 5D 2C 22	66 6C 73 22
047DF650	75 6E 2E 69	6E 66 22 2C

**Decrypted Config**

### 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
name	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.flx	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.

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

*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
mov dword ptr ss:[ebp-44],422
mov dword ptr ss:[ebp-40],423
mov dword ptr ss:[ebp-3C],428
mov dword ptr ss:[ebp-38],42B
mov dword ptr ss:[ebp-34],42C
mov dword ptr ss:[ebp-30],437
mov dword ptr ss:[ebp-2C],43F
mov dword ptr ss:[ebp-28],440
mov dword ptr ss:[ebp-24],442
mov dword ptr ss:[ebp-20],443
mov dword ptr ss:[ebp-1C],444
mov dword ptr ss:[ebp-18],818
mov dword ptr ss:[ebp-14],819
mov dword ptr ss:[ebp-10],82C
mov dword ptr ss:[ebp-C],843
mov dword ptr ss:[ebp-8],45A
mov dword ptr ss:[ebp-4],2801
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.

```

EAX 0019ED68
EBX 00000000
ECX 106E8B92
EDX 00000000
EBP 0019EF30
ESP 0019ED38
ESI 00000000
EDI 00000001
EIP 73D84510 <kernel32.CreateProcess>

```

```

new 1 x
1 Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
2

```

Sodinokibi Deleting Windows Shadow Copies.

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

All of your files are encrypted!

Find 9nv0y622t-readme.txt and follow instructions

*Sodinokibi Background.*

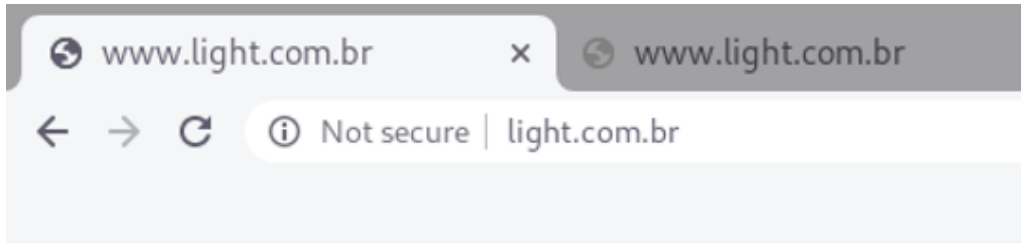
Lastly, it appends a ransom note to every folder where encrypted files can be found.

```
---=== Welcome. Again. ===---  
  
[+] Whats Happen? [+]  
  
Your files are encrypted, and currently unavailable. You can check it: all files on your system  
has extension ln3u310.  
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[REDACTED]byd.onion,[REDACTED]  
  
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[REDACTED]  
  
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.



Cannot connect to the configuration database.

*Light WebSite Offline During Ransomware Attack.*

IOCs

**SHA1:**

f09e5e72b433d11a32efe2e5d63db0bc7b8def59

**SHA256:**

140f831ddd180861481c9531aa6859c56503e77d29d00439c1e71c5b93e01e1a

**SSDEEP:**

3072:oCc99moUMXv84IHesgkSx+oN/7KzTKDyOX6wKamrJPIM8dj09br: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/hOr8pZfTXyeVodyREcseBOIXf2dcLmqmQJTa4y2uSfGkhEZXq62

**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-...>