

A Look Inside the Highly Profitable Sodinokibi Ransomware Business

bleepingcomputer.com/news/security/a-look-inside-the-highly-profitable-sodinokibi-ransomware-business/

Ionut Ilascu

By

[Ionut Ilascu](#)

- August 30, 2019
- 09:22 AM
- 0



Relatively new on the ransomware scene, Sodinokibi has already made impressive profits for its administrators and affiliates, some victims paying as much as \$240,000, while a network infection netted \$150,000 on average.

These figures are not surprising when you look at the malware's recent activity. On August 16, Sodinokibi hit 22 local administrations in Texas and demanded a collective ransom of \$2.5 million. It compromised multiple MSPs (managed service providers) spreading the malware to their customers.

The latest victim is another MSP that offers data backup service to dental practices. The ransom in this case is allegedly \$5,000 per client; hundreds were impacted.

Setting the rules of the game

Since its discovery in April, Sodinokibi (a.k.a. REvil) has become prolific and quickly gained a reputation among cybercriminals in the ransomware business and security researchers.

In mid-May, a Sodinokibi advertiser using the forum name UNKN deposited over \$100,000 on underground forums to show that they meant serious business.

Advertisements for the new file-encrypting malware started in early July on at least two forums. UNKN said that they were looking to expand their activity and that it was a private operation with "limited number of seats" available for experienced individuals.

A screenshot of the announcement, provided to BleepingComputer by malware researcher Damian shows that UNKN describes the malware as being a "private ransomware" flexible enough to adapt to the RaaS business model.

The screenshot shows a forum post from a user named UNKN, who is a 'Seller' with 12 posts and joined on 07/04/19. The post is titled 'Private Crypto Locker Affiliate Program' and is categorized under 'malware, exploits, bundles, crypts'. The post content includes:

- Posted July 4
- Due to the fact that we are expanding activity, we invite adverts by:
 - Spam
 - Dedikam and networks;
 - Doorway traffic and other living things;
- We work in a private mode. Limited number of seats. Get ready for an interview and show your evidence of the quality of the installations. We are not a test site, and the "learners" and "I will try / I will try" there is nothing to do. We have been working for several years, the topic is more than 5 years. The software is fully operational and ready to go.
- Excerpt from the rules:
 - It is forbidden to work in the CIS (including Ukraine);
 - Starting rate from 60% in your direction. After the first 3 payments - 70%.
- Short description of the software: **private ransomware written in pure C, using inline-assembler with the possibility of modifying functionality out of the box according to the RaaS business model.** The software has statistics, a payment page and "trial decoders" on the payment page. No school emails. More information can be obtained during the interview. The first contact in the PM.

Post promoting REvil or Sodinokibi RaaS

UNKN offered affiliates 60% of the payments at the beginning and a 10% increase after the first three transactions. The actor also made it clear that they would not be working with English-speaking affiliates as part of this private program.

The screenshot shows a forum post from the user UNKN, a 'Seller' with 13 posts and joined on 07/04/19. The post is titled 'Posted July 7' and contains the text: 'And also completely forgot - we do not work with English-speaking users. Krebs past.'

Ransom payments flooding in

The name of the ransomware is not disclosed in the forum posts but the researcher told us that he saw screenshots of the malware's administrative panel showing bot IDs that look the same as those for Sodinokibi.

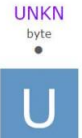
As seen in the screenshot below, one victim paid 27.7 bitcoins, which converted to more than \$220,000 at the time of the transaction.

Date	TXID	Bot	Status	Amount
5 hours ago	4b18196b77f4137c930701632d7012cb5e051daa7d66dddf6c956...	20C4F38C72DD57D2	✓	27.69844319 220213.00 USD

Another capture from Damian makes it clear that this particular ransomware program is highly profitable with some victims paying as little as .4 bitcoins (~\$4,000) while others shelling out 26 bitcoins or approximately \$240,000 at the moment of the conversion.

Date	TXID	Bot	Status	Amount
7 hours ago	048c100a3bd9ed6a9a5d90791a78290d4a1367880415d2c069...	[REDACTED]	✓	0.43707153 3988.98 USD
11 hours ago	16cd37ba2ab29973c202bbeab6dea3a9a1e9d0bf69a46952ec7...	[REDACTED]	✓	26.38798971 240143.00 USD
12 hours ago	278dfb8f03f49f892bd2fbf17fd3dcf54fee33d32d580acb2c2856...	[REDACTED]	✓	0.44554645 4084.89 USD
12 hours ago	26584ef98f78beac075f0f3d11bf88ee601b71cd9aabf9dcb4d0d...	[REDACTED]	✓	0.44322399 4064.02 USD
12 hours ago	0b85c5b69e4b210b42a96eefec07f6f62559b9eaf0c0287659c4...	[REDACTED]	✓	0.44238799 4053.80 USD
12 hours ago	74fcaa7c5b6f5ebdd83d2c962c16325c65e43292f68b4a429a46...	[REDACTED]	✓	0.44189143 4050.42 USD
12 hours ago	91480ae15884f9b56f5fb83f26b016cefeb5302133504fcb2145...	[REDACTED]	✓	0.43909627 4018.53 USD
2 days ago	d569cef16b5e7f142dcae523a51d3a08074790053a630ff6d606...	[REDACTED]	✓	1.71205268 15102.40 USD
2 days ago	5d97529a3a09a0a888156877357c63e4a3a0c72c1205a92998e...	[REDACTED]	✓	0.45300601 3984.28 USD
2 days ago	fce34caa6506d5f02166d8006814f7f7ca11dd3d1fde41b0b1f78...	[REDACTED]	✓	0.45414266 4009.63 USD

For those affiliates who can infect an entire network, the REvil/Sodinokibi developers allow a victim to purchase a decryption tool for the entire fleet of affected computers. According to forum post shared with BleepingComputer, these network-wide decryptors have an average cost of \$150,000.



UNKN
byte

Seller
13 posts
Registration
04.07.2019 (ID: 94 090)

Posted: 8 August A complaint ↩

There are 3 places for networks / dedikov. **Network** priority . In software there is the possibility of receiving a ransom for the **entire network at once**. **The average buyback** for the network is currently **\$ 150k** . Software is very famous in certain circles. Please send applications in the form:

Quote

Hello
Installations: Dediks
Quantity: 100 pcs per day
GEO: EU EU + - mix
Production method: mine (exploit)
Work experience: "inapp" is so much time and the envelope in it is average, or there is no experience (otherwise loaded)
Ready to start tomorrow

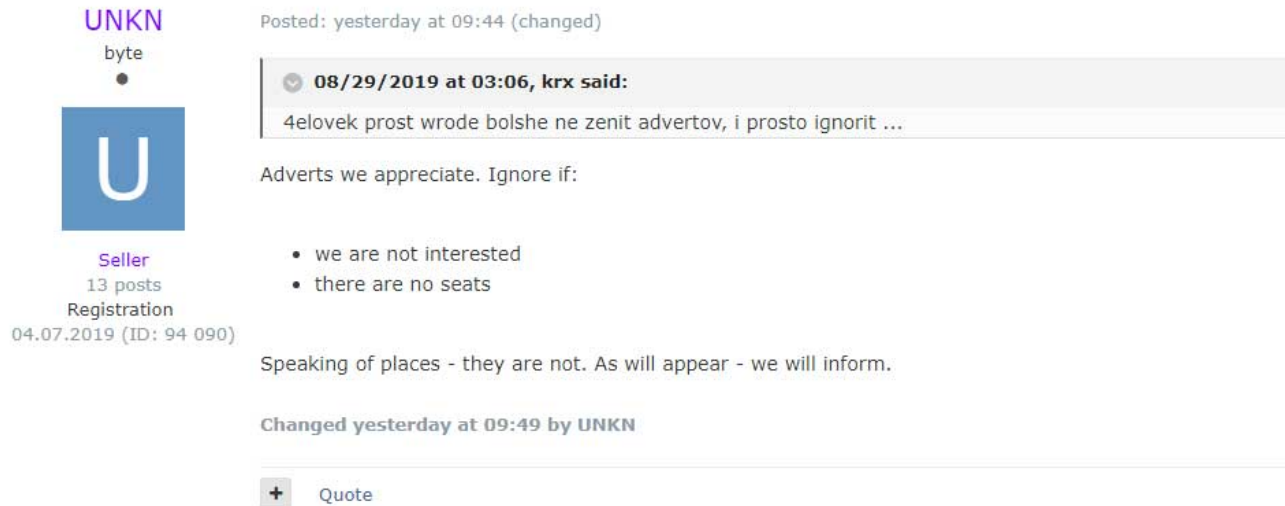
or

Quote

Hello!
I do installs from spam on corporation bases. Usually the base of the EU country, but there are also Asia. It turns out from 100 installations per day. I'm sending out a dock with a macro. Previously, I did not work with 1 pp, I loaded a bankbot.

Forum post about average network-wide decryptor costs

With the revenue flooding in, other malware distributors are trying to gain access to the program, but UNKN has stated yesterday that there are no available openings for affiliates at this time.



UNKN
byte

Posted: yesterday at 09:44 (changed)

08/29/2019 at 03:06, krx said:
4elovek prost wrode bolshe ne zenit advertov, i prosto ignorit ...

Adverts we appreciate. Ignore if:

- we are not interested
- there are no seats

Speaking of places - they are not. As will appear - we will inform.

Changed yesterday at 09:49 by UNKN

+ Quote

RaaS is closed to new members

Serious players in the game

When they started advertising, the threat actor already had the support of respected members of the underground ransomware community.

Yelisey Boguslavskiy, director of security research at Advanced Intelligence ([AdvIntel](#)), told BleepingComputer that UNKN registered an account on one cybercriminal forum on July 4 and that it is clear that they had been active outside this community.

Two high-profile community members specializing in ransomware attacks endorsed UNKN and also revealed that they had joined the affiliate program, indicating that they already knew who they were dealing with.



Lalartu
1283 posts
Joined 12/14/17 (ID: 94236)

Posted July 4

I work with these nice young people, very nice, very.

I switched to them after the crab, what I tell you, the crab was worse, then my envelope not only grew, it broke through the ceiling and grows further. And this is thanks to the fact that people are not being recruited here if only they were, builds are cleaner, sometimes they are missed with closed eyes, sweetie.

I welcome you to this forum. ❤️

+ Quote

In the image above, forum member Lalartu discloses that they started to work with Sodinokibi after the GandCrab operation went belly up. They praise the new RaaS disclosing the move had a significant effect on earnings, which "not only grew, it broke through the ceiling and grows further."

Boguslavskiy told us that positive feedback for a new ransomware strain is very uncommon on that forum. The two members are typically very critical with newcomers.

"For instance, when "JSWorm" and "NEMTY" were introduced, the community reacted with extreme skepticism and aggression."

A discussion thread on Sodinokibi started in June, with most forum members showing skepticism about the new ransomware and its legitimacy. The thread was deleted soon after UNKN presented the affiliation offer.


The GandCrab connection

Sodinokibi was spotted when researchers saw it deployed on Oracle WebLogic servers by exploiting a critical deserialization vulnerability. On the same systems infected with Sodinokibi, cybercriminals also installed GandCrab a few hours later.

At the end of April, GandCrab administrators announced that they would close shop within 20 days. And they kept their word.

Gandcrab Posted 18 hours ago Report post

(\ /) _ (\$ _ \$) _ (\ /)
●●●●●



Seller
424 posts
Joined
12/18/17 (ID: 84324)
Activity
virology

All the good things come to an end.
For the year of working with us, people have earned more than **\$ 2 billion**, we have become a nominal name in the field of the underground in the direction of crypto-fiber. Earnings with us per week averaged **\$ 2,500,000** .
We personally earned more than **150 million** dollars per year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet.
We were glad to work with you. But, as it is written above, all good things come to an end.

We are leaving for a well-deserved retirement . We have proven that by doing evil deeds, retribution does not come. We proved that in a year you can earn money for a lifetime. We have proved that it is possible to become number one not in our own words, but in recognition of other people.

In this regard, we:

1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.

The operators behind the Sodinokibi Ransomware started looking for affiliates to distribute their software soon after the GandCrab ransomware-as-a-service (RaaS) shut down. Underground reactions towards the new product suggest that there may be a connection with the administrators or the affiliates of the now defunct GandCrab operation.

Some malware analysts pointed to code-level similarities between the two ransomware strains, although plenty of differences exist between the two.

However, one similarity is that administrators of both malware families would not carry business in the Commonwealth of Independent States (CIS) area. This includes Russia, Ukraine, Moldova, Belarus, Kyrgyzstan, Kazakhstan, Armenia, Tajikistan, Turkmenistan, and Uzbekistan.

These breadcrumbs along with the rapid ascension of the malware seem to suggest involvement from the GandCrab crew or its affiliates. Already having connections on private forums, it allowed them to quickly promote Sodinokibi and be selective about their partners.

There is no clear, undeniable evidence that Sodinokibi is run by the same individuals that administered GandCrab, but they obviously know the ransomware game and are into the money-making business.

Related Articles:

[BlackCat/ALPHV ransomware asks \\$5 million to unlock Austrian state](#)

[Windows 11 KB5014019 breaks Trend Micro ransomware protection](#)

[Industrial Spy data extortion market gets into the ransomware game](#)

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

[SpiceJet airline passengers stranded after ransomware attack](#)

- [GandCrab](#)
- [Ransomware](#)
- [Sodinokibi](#)

[Ionut Ilascu](#)

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- [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:
