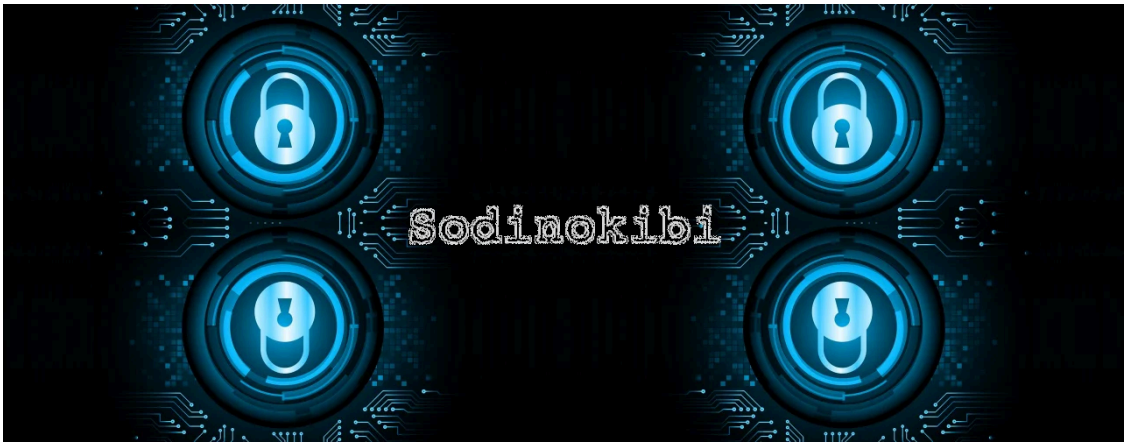
A Look Inside the Highly Profitable Sodinokibi Ransomware Business

By Ionut Ilascu

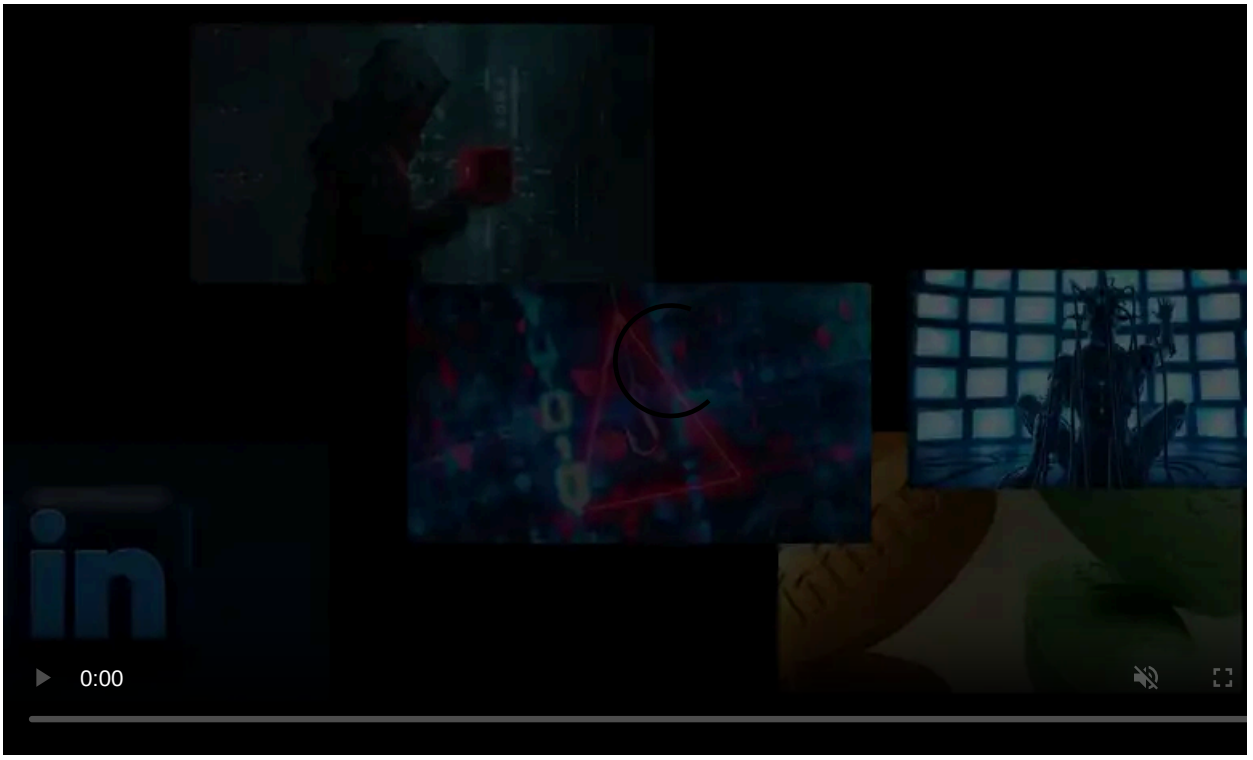
Published: 2019-08-30 · Archived: 2026-04-05 17:25:06 UTC

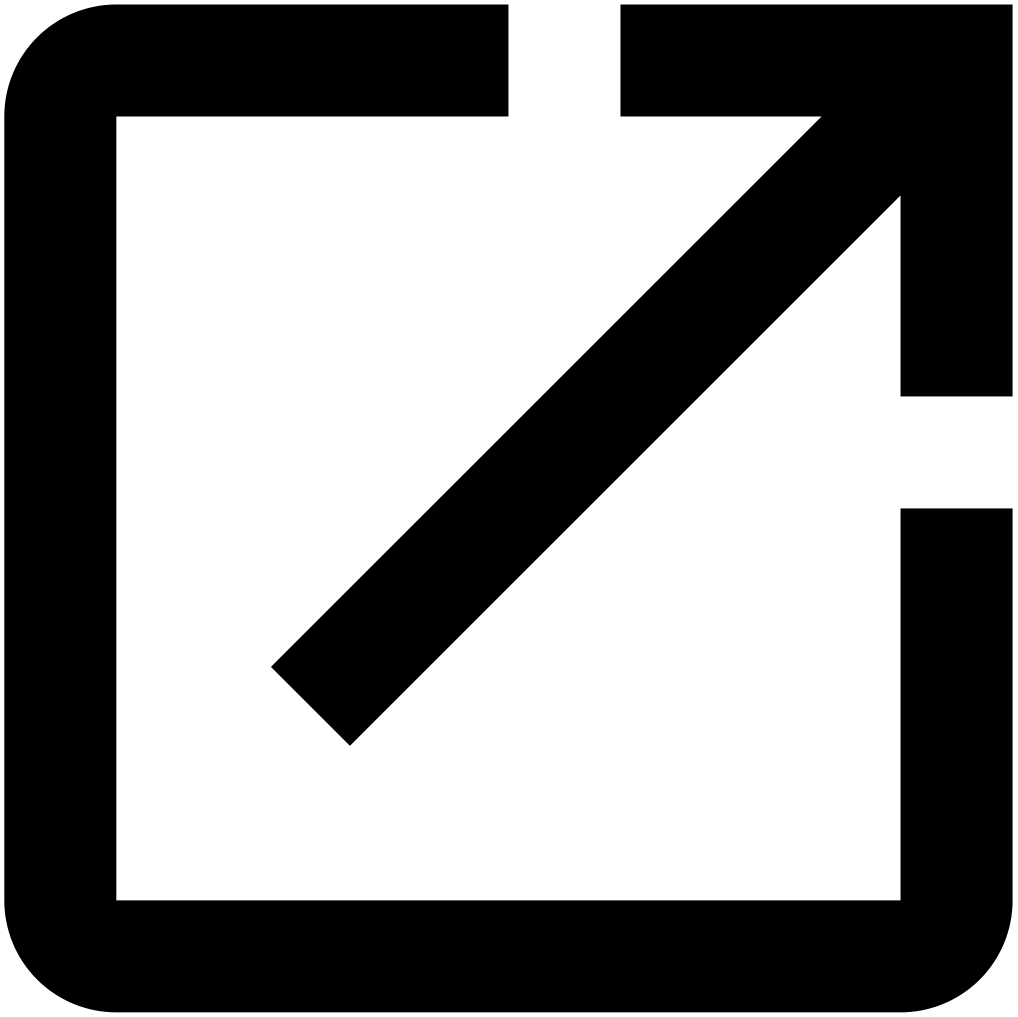


Relatively new on the ransomware scene, Sodinokibi has already made impressive profits for its administrators and affiliates, some victims paying as much as $240,000, while a network infection netted $150,000 on average.

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.


0:00



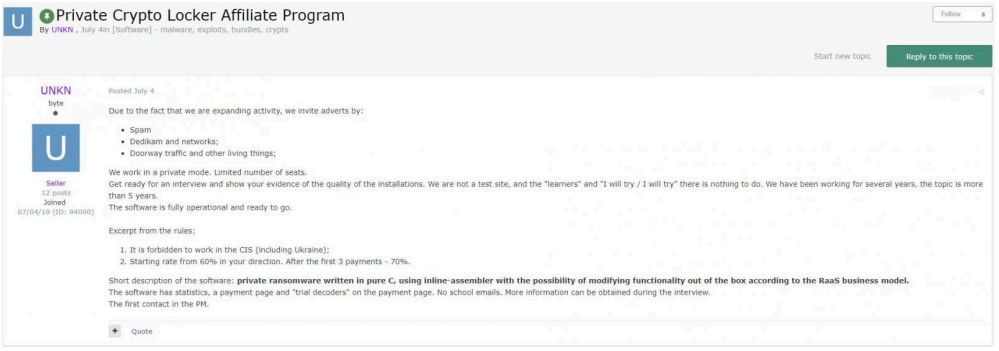
Setting the rules of the game

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.

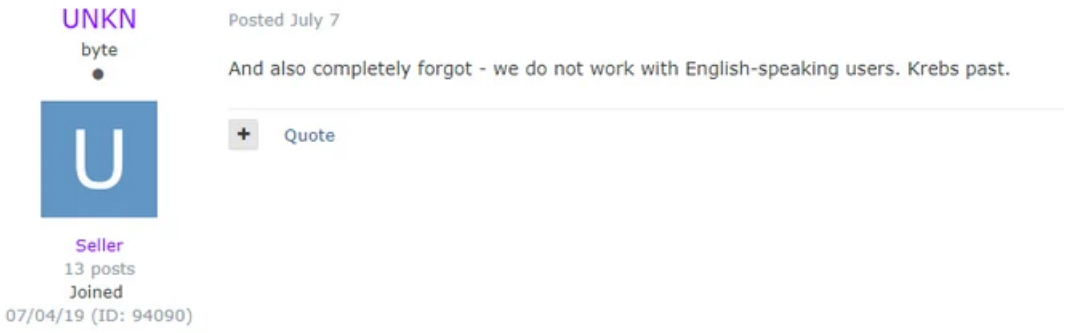
Advertisements for the new file-encrypting malware started in early July on at least two forums. UNKN said that they were looking to expand their activity and that it was a private operation with "limited number of seats" available for experienced individuals.

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.



Post promoting REvil or Sodinokibi RaaS

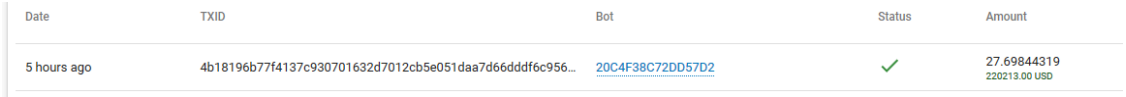
UNKN offered affiliates 60% of the payments at the beginning and a 10% increase after the first three transactions. The actor also made it clear that they would not be working with English-speaking affiliates as part of this private program.



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.

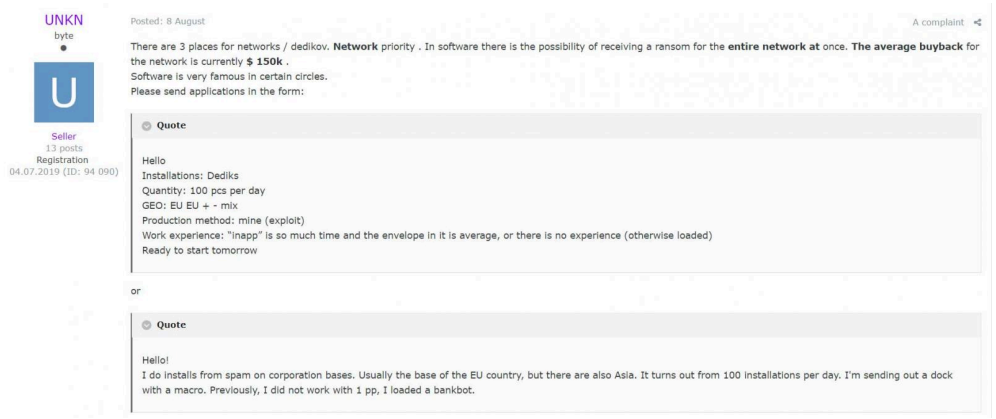


Another capture from Damian makes it clear that this particular ransomware program is highly profitable with some victims paying as little as .4 bitcoins (~$4,000) while others shelling out 26 bitcoins or approximately $240,000 at the moment of

the conversion.

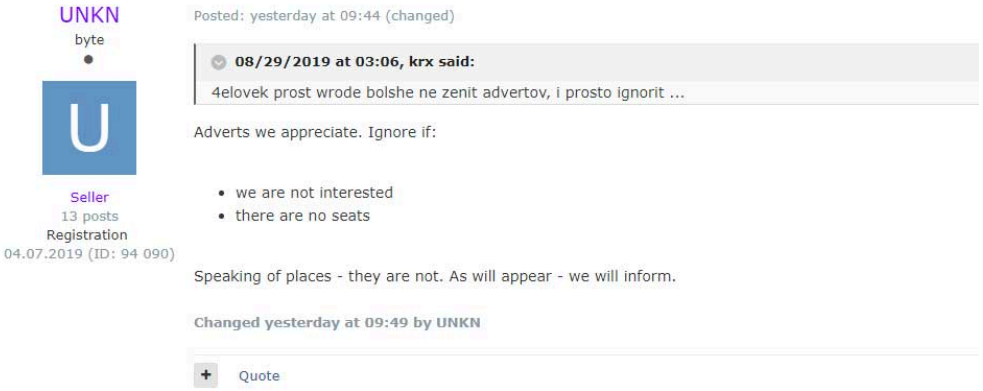
Date	TXID	Bot	Status	Amount
7 hours ago	048c100a3bd9ed6a9a5d90791a78290d4a1367880415d2c069...	[redacted]	✓	0.43707153 3988.98 USD
11 hours ago	16cd37ba2ab29973c202bbeab6dea3a9a1e9d0bf69a46952ec7...	[redacted]	✓	26.38798971 240143.00 USD
12 hours ago	278dfb8f03f49f892bd2fbf17fd3dcf54fee33d32d580acb2c2856...	[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	91480ae15884f9b56f5fb83f26b016cefeb5302133504fcbb2145...	[redacted]	✓	0.43909627 4018.53 USD
2 days ago	d569cef16b5e7f142dcae523a51d3a08074790053a630ff6d606...	[redacted]	✓	1.71205268 15102.40 USD
2 days ago	5d97529a3a09a0a888156877357c63e4a3a0c72c1205a92998e...	[redacted]	✓	0.45300601 3984.26 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.



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.



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.

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.

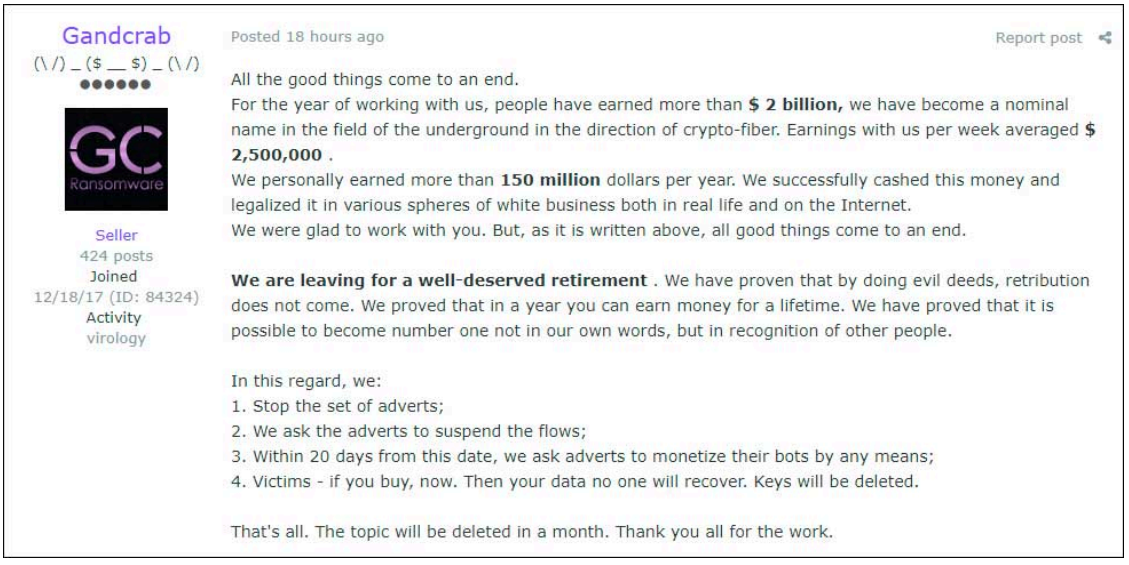
"For instance, when "JSWorm" and "NEMTY" were introduced, the community reacted with extreme skepticism and aggression."

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.



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.

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