

CRH:DKK/AFM
F. #2020R00582

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- against -

MOISES LUIS ZAGALA GONZALEZ,
also known as “Nosophoros,”
“Aesculapius” and
“Nebuchadnezzar,”

Defendant.

AMENDED AFFIDAVIT
AND COMPLAINT IN
SUPPORT OF AN
APPLICATION FOR
AN ARREST WARRANT

(T. 18, U.S.C., §§ 1030(a)(5)(A),
1030(a)(7)(C), 1030(b), 1030(c)(3)(A),
1030(c)(4)(B), 371, 2 and 3551 et seq.)

No. 21-M-276

----- X

EASTERN DISTRICT OF NEW YORK, SS:

CHRIS CLARKE, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such:

Count One: Attempted Computer Intrusions

In or about and between April 2019 and March 2021, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant MOISES LUIS ZAGALA GONZALEZ, also known as “Nosophoros,” “Aesculapius” and “Nebuchadnezzar,” did knowingly attempt to cause the transmission of a program, information, code and command and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, resulting in losses in excess of \$5,000 and damage affecting ten or more protected computers during a one-year period; and did, with intent to extort from any person any money or other thing of value, attempt to

transmit in interstate or foreign commerce a demand for money or other things of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.

(Title 18, United States Code, Sections 1030(a)(5)(A), 1030(a)(7)(C), 1030(b), 1030(c)(3)(A), 1030(c)(4)(B), 2 and 3551 et seq.)

Count Two: Conspiracy to Commit Computer Intrusions

In or about and between April 2019 and March 2021, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant MOISES LUIS ZAGALA GONZALEZ, also known as “Nosophoros,” “Aesculapius” and “Nebuchadnezzar,” together with others, did knowingly and willfully conspire to knowingly cause the transmission of a program, information, code and command and, as a result, intentionally cause damage without authorization to a protected computer, resulting in losses in excess of \$5,000 and damage affecting ten or more protected computers during a one-year period; and to, with intent to extort from any person any money or other thing of value, transmit in interstate or foreign commerce a demand for money or other things of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(a)(7)(C), 1030(c)(3)(A), and 1030(c)(4)(B).

(Title 18, United States Code, Sections 371 and 3551 et seq.)

The source of your deponent's information and the grounds for his belief are as follows:¹

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since January 2015. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for cybercrime, financial crime, and money laundering. I have investigated and otherwise participated in numerous matters during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants, and used other investigative techniques to secure relevant information.

2. I am familiar with the facts and circumstances set forth below from my participation in the investigation, from my review of documents obtained pursuant to the investigation, and from reports of other law enforcement officers involved in the investigation. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated. In addition, many of the statements described herein are based on draft English translations of communications that were not originally made in English, and are subject to revision.

¹ Because the purpose of this complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

I. THE DEFENDANT

3. MOISES LUIS ZAGALA GONZALEZ (“ZAGALA”) is a 55-year-old cardiologist who resides in Ciudad Bolivar, Venezuela.

4. In addition to his medical practice, and as set forth in detail below, ZAGALA creates software (“ransomware”) that cybercriminals use to extort money from companies, nonprofits, and other institutions, by encrypting those victims’ files and then demanding a ransom for the decryption key. ZAGALA also creates related software for use by cybercriminals, such as tools to be used for making viruses invisible to antivirus software. In addition, ZAGALA is an expert in reverse engineering, or “cracking,” mobile devices and software to remove protective restrictions imposed by the manufacturer.

5. Using the online nicknames (or “handles”) “Aesculapius,” “Nosophoros” and “Nebuchadnezzar,” ZAGALA posts frequently on online forums frequented by cybercriminals.² As set forth below, ZAGALA’s posts using these nicknames, as well as other information obtained during the investigation, conclusively link the user of those nicknames to ZAGALA.

6. ZAGALA’s involvement in the computer underground began no later than in or around 1997. Online postings in that year reflect ZAGALA’s involvement with “High Cracking University” (“HCU”), a select online community of elite hackers and reverse engineers. Online tutorials published by HCU include articles by an individual identified as

² In keeping with ZAGALA’s vocation as a cardiologist, two of his nicknames have medical connotations: “Aesculapius” is the ancient Greek god of medicine, and “nosophoros” means “disease-bearing” in Greek.

“Aesculapius” about cracking shareware programs, as well as coding challenges created by “Aesculapius” that served as admissions tests for HCU’s elite users. Over the years, ZAGALA continued to code software, and to write online postings, about software reverse engineering.

7. More recently, to make money, ZAGALA has been licensing his ransomware to cybercriminals, many of whom pay him a periodic “license” fee to use the software. ZAGALA provides extensive customer service along with his software, counseling his customers about how most effectively to use his software against their victims. ZAGALA provides his software knowing and intending that his customers use it to commit computer intrusion, extortion and other crimes. In addition, ZAGALA leads a ring of cybercriminals who do not pay a license fee, but instead share with ZAGALA a portion of the ransom money extorted from their victims using ZAGALA’s software.

II. ZAGALA’S RANSOMWARE PROGRAMS

8. Among the ransomware tools ZAGALA has developed and sold are “Jigsaw v. 2,” a ransomware program (hereinafter “Jigsaw”), and “Thanos,”³ a tool that can be used to create other, fully customized ransomware programs.

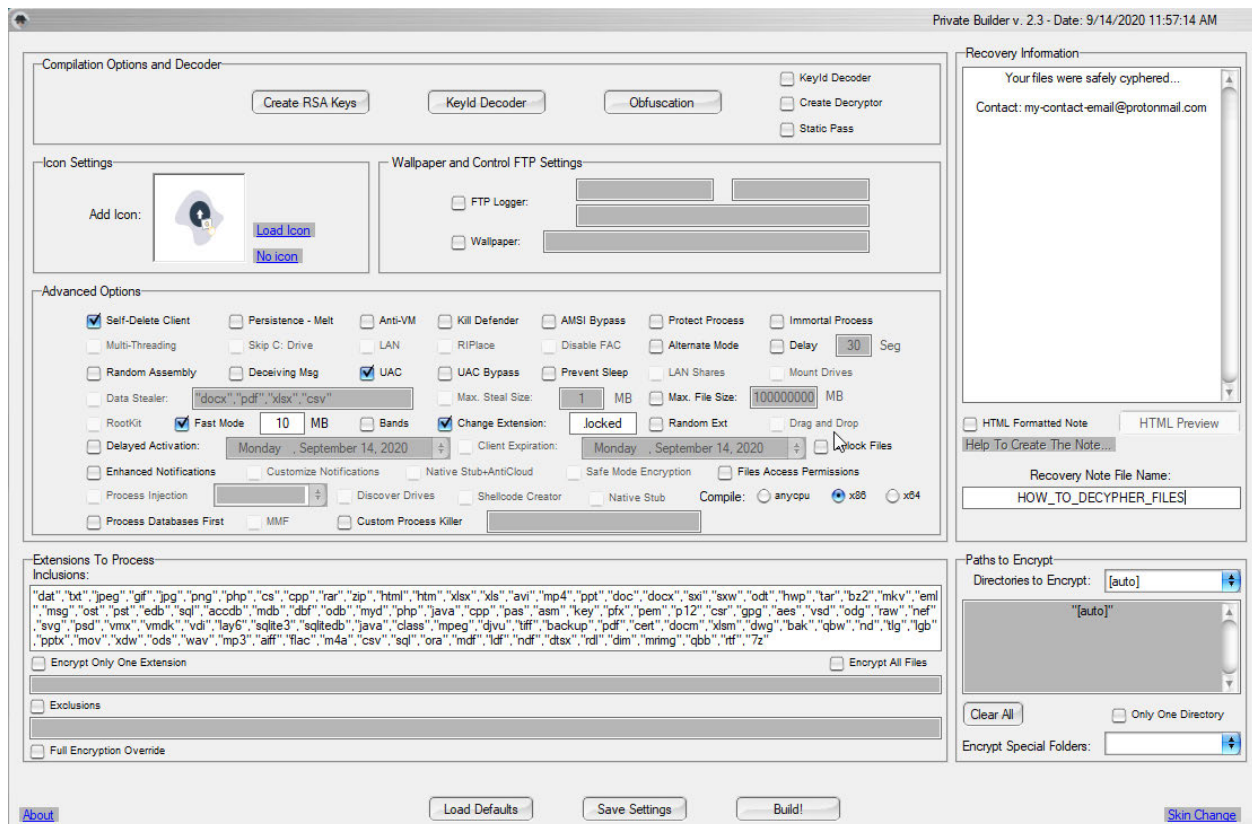
9. With respect to Jigsaw, ZAGALA’s program appears to be designed by him to update an older version of the program. Specifically, ZAGALA’s postings and other

³ “Thanos” appears to be a reference to a fictional cartoon villain named Thanos, who is responsible for destroying half of all life in the universe, as well as a reference to the figure “Thanatos” from Greek mythology, who is associated with death.

statements related herein all refer to “version 2” of the software, and ZAGALA has stated in online postings that he rewrote an existing, outdated “version 1” created by others.

10. On or about September 14, 2020, I purchased a license for the Thanos software from ZAGALA. I downloaded Thanos to a computer located in the Eastern District of New York.

11. A photograph of the user interface for the Thanos software that I downloaded is set forth below:



This screenshot shows, on the right-hand side, an area for “Recovery Information,” in which ZAGALA’s customer can create a customized ransom note. The field at the bottom left, “Extensions to Process,” allows ZAGALA’s customers to select the kinds of files that will be encrypted in the ransomware attack.

12. The Thanos software also allows a customer building a ransomware program to select various “obfuscation options” to help limit the victim’s ability to detect the software.

III. ZAGALA ADVERTISES AND SELLS JIGSAW AND THANOS

13. On or about April 8, 2019, ZAGALA used the handle “Aesculapius” to post on a publicly accessible web forum frequented by cybercriminals (“Forum-1”).

ZAGALA’s post offered Jigsaw’s source code for sale. In advertising Jigsaw, ZAGALA boasted about the software’s sophisticated features, including:

- a. Features that made the ransomware undetectable to antivirus software;
- b. A “Doomsday counter” that kept track of how many times the user had attempted to eradicate the ransomware: “If the user kills the ransomware too many times, then its clear he won’t pay so better erase the whole hard drive”;
- c. The ability to steal the victim’s passwords and credit card information, and to spread laterally to other computers in the same network as the victim computer; and
- d. A feature that increased the ransom demand with the passage of time.

Along with his posting, ZAGALA included multiple screenshots of the software, illustrating ransom notes, demands for Bitcoin, and samples of stolen victim information.

14. On or about November 24, 2019, ZAGALA again advertised Jigsaw in a posting that he placed on a private online forum (“Forum-2”) frequented by cybercriminals. On Forum-2, ZAGALA uses the nickname “Nosophoros.” In his post, ZAGALA boasted that Jigsaw contained numerous sophisticated features, including “Extensive punishment if ransom not paid – goes up to all hard drives deletion and killing boot.” ZAGALA stated

that Jigsaw was programmed to evade antivirus software and could also be used to introduce backdoor access to victim machines and be configured to offer a different Bitcoin address to each victim. ZAGALA advertised the tool for \$500, and the underlying source code for \$3,000.

15. On or about December 7, 2019, ZAGALA posted a reference to “other[s] of my products” in an online forum. The link that ZAGALA posted led to a tweet about Jigsaw by a German cybersecurity firm. The tweet from the cybersecurity firm noted that the following file path appeared in the Jigsaw code:

```
C:\Users\Moises\Desktop\jigsawransomware2019-  
master\JigsawRansomware\obj\Debug\JigsawRansomware.pdb
```

Based upon my training and experience, the reference to “Moises” in the aforementioned file path indicates that the Jigsaw program at issue in the post was created on a Windows computer by a user named “Moises” (i.e. the defendant’s true first name).

16. Beginning in late 2019, ZAGALA began advertising a new tool—a “Private Ransomware Builder” he called “Thanos.” As described by ZAGALA in a posting on another private online cybercriminal forum (“Forum-3”) using the handle “Nosophoros,” Thanos allowed its users to generate one-of-a-kind ransomware tools: “Creation of a ransomware client [program] is as easy as three steps: 1. Change bitcoin address to collect the ransom, 2. Type email for contact (anonymous email service) and ransom amount, 3. Click Build.”

17. In that posting on Forum-3, ZAGALA also invited “[a]ffiliate program candidates”—hackers who were interested in using Thanos in exchange for paying ZAGALA a portion of the profits from their ransomware attacks—to contact him.

18. Numerous users responded to ZAGALA on Forum-3, posting that they had used the software and praising its quality. “I used this product,” one user wrote. “I will say that it is very good.” Another added: “I am using tool and it’s a great one, keep the updates coming.” A third commented that he had used the software to create time-limited ransomware tools for distribution to his affiliates: “Very successful to create your own affiliate programs.”

19. On or about October 10, 2019, ZAGALA advertised Thanos on Forum-1. ZAGALA boasted that the “builder” was nearly undetectable by antivirus programs, and that it was “totally configurable: client name, ransom message, ransom filename, encrypted extension, directories to be attacked, BTC [Bitcoin] address[.]” ZAGALA added that “once encryption is done,” the ransomware would “delete itself,” making detection and recovery “almost impossible” for the victim.

20. ZAGALA’s postings on Forum-1, Forum-2 and Forum-3 share numerous common elements and references to identifiers associated with ZAGALA. For example:

- a. ZAGALA’s postings on Forum-1 (as “Aesculapius”), and on Forum-2 and Forum-3 (as “Nosophoros”) each invite clients to contact him at a certain address using a messaging protocol called Jabber (“Jabber-1”). ZAGALA’s postings on Forum-2 also list a second Jabber contact address that is referred to below (“Jabber-2”), and a third Jabber address that incorporates the name “Aesculapius.”
- b. In his postings as “Aesculapius” on Forum-1, ZAGALA asks buyers of his products (including Jigsaw and Thanos) to make payments to a certain PayPal account (“PayPal-1”). PayPal has indicated that the registered user of PayPal-1 is “Moises Zagala,”

the associated email address is moiseszagala[@]gmail.com,⁴ and the associated street addresses include many addresses in Ciudad Bolivar, Venezuela, one of which is denoted herein as “Address-1.”

- c. Google has indicated that the registered user of moiseszagala[@]gmail.com supplied the name “Moisés Zagala.” The user also provided a telephone number with a Venezuela country code, which number is also a registered telephone number for PayPal-1.

21. In addition, I have reviewed the contents of the

moiseszagala[@]gmail.com email account, which include numerous links to ZAGALA and other content discussed herein. For example:

- a. On or about June 10, 2019, moiseszagala[@]gmail.com sent an email to itself with the subject “WhatsApp Chat with [telephone number].” Based upon my training and experience, WhatsApp is a chat program. The June 10 email attached a text file containing a text message exchange on June 3, 2019 between “Moises Zagala” and another individual, about the Jigsaw ransomware program. That WhatsApp conversation is discussed in more detail below in paragraph 30.
- b. On July 17, 2019, moiseszagala[@]gmail.com sent an email to another email address that the investigation has associated with ZAGALA (“Gmail-1”). Gmail-1 has the same username as PayPal-1. The subject was “Banking Information and Password Dump Report.” The email contained two attachments. One was a file called “C:\\Users\\Moises\\AppData\\Local\\Temp\\0861013C\\Directory\\Wallets\\Monero\\Nosophoros.” Based upon my training and experience, that file contains information about cryptocurrency wallets controlled by ZAGALA under the name “Nosophoros.”⁵ The second file was called “17/07/2019 9:27:30 PM - VictimScreenShoot.jpeg.” The picture shows what appears to be a

⁴ The use of “[@]” instead of “@” is meant to prevent the inadvertent sending of an email to the email address. Where “[@]” is used in the text of this application, the true address at issue does not contain the brackets surrounding the “@” sign.

⁵ Based upon my training and experience, I know that Monero is a cryptocurrency.

screenshot of ZAGALA's computer desktop, created in an apparent effort to test the ability of his software to spy on victim computers. More specifically, the picture is a screenshot of a computer desktop showing a browser open to the Gmail-1 account. One of the emails visible in the screenshot is entitled "Victim's Info and Password Dump!" Another visible email contains the text "hi, sure telegram" and includes the phone number discussed above that is associated with ZAGALA. Also visible in the Gmail window in the screenshot is a link to a different account called "Aesculapius." Finally, in the center of the screenshot is a folder whose path is "Moises Zagala > source > repos > BankingTrojan > BankingTrojan > bin > Debug." Based upon my training and experience, I know that a "Trojan" is a kind of computer virus.

- c. On or about May 26, 2020, an individual sent moiseszagala[[@](mailto:moiseszagala@gmail.com)]gmail.com an email with the subject "Thanos License." The text of the email read: "Hi Moises Zagala, I was having an issue with my Private Ransomware Builder license. Can you help fix my license issue?"

22. In September 2020, when I downloaded the Thanos software, ZAGALA, using Jabber-1, instructed that payment for the software be sent in cryptocurrency to an account hosted by a cryptocurrency trading platform (the "Crypto Platform"). Based upon information provided by the Crypto Platform, the account identified by ZAGALA for payment has "Nosophoros" as the user name, "Moises Luis Zagala Gonzalez" as the full name, and moiseszagala[[@](mailto:moiseszagala@gmail.com)]gmail.com as the email address. The account is also associated with a photograph and driver's license provided to the Crypto Platform that bear ZAGALA's name and image. Copies of those documents are set forth below:⁶

⁶ The government has redacted certain personal identification information from the document.



23. Travel records maintained by United States Customs and Border Protection (“CBP”) indicate that ZAGALA has entered, and reserved flights to enter, the United States multiple times, and has indicated to CBP that his email address was moiseszagala[.]gmail.com. I have compared the photographs associated with these CBP records and the other photographs of ZAGALA set forth in this application, including the

ones set forth above, and, based upon my training and experience, all of these photographs show the same individual.

24. Moreover, in certain postings about Jigsaw, Thanos, and other malware products, ZAGALA directed interested customers to buy his products on a certain e-commerce platform for buying and selling software (“Platform-1”).⁷ ZAGALA registered his account at Platform-1 using an email address hosted by Google (“Gmail-2”). According to Google, the recovery email address for Gmail-2 is moiseszagala[[@](mailto:moiseszagala@gmail.com)]gmail.com.⁸

25. Clients who purchased malware from ZAGALA on Platform-1 made payment either in cryptocurrency or via PayPal. Among the PayPal accounts that ZAGALA used to receive payment were an account (“PayPal-2”) with username “moiseszagala[[@](mailto:moiseszagala@gmail.com)]gmail.com,” registered in the name “Moises Zagala” and associated with Address-1 in Ciudad Bolivar, Venezuela—the same street address associated with PayPal-1, which was advertised by “Aesculapius” on Forum-1. Payments were also made, at times, to a PayPal account registered in the name of an individual who resides in Florida (the “Florida Relative”). Based upon open source information, the Florida Relative is ZAGALA’s brother.

⁷ Based upon information provided by Platform-1, ZAGALA also sold copies of other ransomware, including “Petya,” a program that, based upon my training and experience and open source information, has been used to conduct numerous cyber intrusions.

⁸ The moiseszagala[[@](mailto:moiseszagala@gmail.com)]gmail.com account further shows links between ZAGALA and Gmail-2. Specifically, on or about March 28, 2019, moiseszagala[[@](mailto:moiseszagala@gmail.com)]gmail.com sent an email to Gmail-2 containing a picture of driver’s license bearing the name “MOISES LUIS ZAGALA GONZALEZ” and a photograph of ZAGALA.

26. Information provided by Platform-1 indicates that ZAGALA sold approximately \$4,580 of malware through the platform on or about and between August 2, 2019 and April 13, 2020.

27. The total number of copies of malware sold by ZAGALA is unknown. However, an FBI computer scientist who examined Thanos has determined that active copies of the software make periodic contact with a server in Charlotte, North Carolina (the “Thanos Control Server”). The server company has indicated that the registered user for that server provided Gmail-2 as his contact email and chose, as a username, the same phrase that is the username for PayPal-1 and Gmail-1.

28. Based upon an analysis of the malware and other information obtained from the Thanos Control Server, I have determined that the Thanos program communicates with the Thanos Control Server in order to confirm that the user of the program has an active license. In this manner, ZAGALA can prevent customers who have not paid their monthly license fees from using the Thanos program. Moreover, the Thanos Control Server contained a file that listed the status of 38 customer’s licenses, indicating that at least 38 copies of the ransomware program have been sold.

IV. ZAGALA SELLS THANOS AND JIGSAW INTENDING FOR THEM TO BE USED TO COMMIT COMPUTER INTRUSIONS

29. As set forth in part below, ZAGALA has openly encouraged his customers to use Thanos and Jigsaw to commit computer intrusions and otherwise demonstrated his knowledge that his customers are using Thanos to commit computer intrusions. Moreover, his use of an “affiliate” program allows him to profit directly from such intrusions.

30. For example, the moiseszagala[*@*]gmail.com account contained a copy of a WhatsApp chat that took place on or about June 3, 2019 between ZAGALA and a customer (“Customer-1”), who had apparently purchased the Jigsaw ransomware. In the chat, ZAGALA explains to Customer-1 how Jigsaw works to obtain money from intrusion victims:

- a. “Hi bro,” Customer-1 wrote. “I’m from the ransomware.” Based upon my training and experience and the foregoing, Customer-1’s statement indicated that he or she used ransomware. In response to Customer-1’s questions, ZAGALA walked Customer-1 through various functions, including how to design a ransom note, steal passwords from victim computers, and configure the software with his Bitcoin address for ransom payments. As ZAGALA explained it: “Victim 1 pays at the given btc [Bitcoin] address and decrypts his files.” ZAGALA also noted that “there is a punishment . . . [i]f user reboots. For every rerun it will punish you with 1000 file[s] deleted.” Based on my knowledge, training and experience, the meaning of this remark is that the Jigsaw ransomware is designed to deter victims from trying to evade or uninstall it by “punishing” them when they restart their computers.
- b. ZAGALA explained to Customer-1 his intention to sell five copies of Jigsaw on the dark web for a total of \$2,500, and invited Customer-1 to make him a competing offer for the exclusive right to use the software. Customer-1 responded positively: “I want to spread it and make much money out of it. I will give you more money than darkweb will do.” ZAGALA replied: “Think about it and make me a reasonable offer.”
- c. ZAGALA sent Customer-1 an update to the malware, as well as files to be used in infecting potential victims by tricking them into opening malicious Microsoft Word files. ZAGALA described the repository where the files were kept (known in programming parlance as a “git”) as “Private . . . No on[e] can see it.” Customer-1 responded: “Okay[,] and police?” ZAGALA responded: “No one. Git encrypt[s] it.”
- d. “Sir, I really need to say this,” Customer-1 wrote. “You are the best developer ever.” ZAGALA responded: “Thank you that is nice to hear[.] I[’]m very flattered and proud.” ZAGALA had

only one request: “If you have time and its not much bother to you please describe your experience with me” in an online review.

- e. In the same conversation, ZAGALA also suggested that Customer-1 pay him through an online payment account in the name of a relative, whom ZAGALA also described as “my associate.” ZAGALA explained: “I dont want to use mine [account] because rates for transfer are higher.” ZAGALA then provided an email address for Customer-1 to use in connection with the payment. The email address includes the first name and last name of the Florida Relative.

31. In or around and between August 18, 2020, through October 8, 2020, a confidential human source of the FBI (“CHS-1”)⁹ discussed with ZAGALA how to use the Thanos software to make money, including through the “affiliate program”:

- a. On or about May 1, 2020, CHS-1 contacted ZAGALA on Jabber-1 to ask if CHS-1 could join the “Thanos Ransomware Affiliate Program.” ZAGALA responded, “Not for now. Don’t have spots. Only monthly rent the builder itself or unlimited license.” ZAGALA offered to license the software to CHS-1 for \$500 a month with “basic options,” or \$800 with “full options.”
- b. On or about October 7, 2020, CHS-1 communicated with ZAGALA on Jabber-2. CHS-1 asked ZAGALA how to establish an affiliate program, and ZAGALA explained, in sum and substance, that CHS-1 should find people “versed . . . in LAN hacking” and supply them with a version of the Thanos ransomware that was programmed to expire after a given period of time. Based on my knowledge, training and experience, “LAN” stands for “local area network” and refers to a computer network that interconnects computers within a limited area such as an office building. ZAGALA also explained that, with respect to his affiliates, “If they get contacted then they contact me.” Based on my knowledge, training and experience, ZAGALA was explaining that, if one of his affiliates conducted a ransomware attack and the victim contacted

⁹ CHS-1 has pled guilty to identity theft and access device fraud charges in federal court. He is cooperating with the FBI in hopes of receiving leniency at sentencing. In addition, CHS-1 hopes to receive an immigration benefit from the government that would permit him to remain in the United States rather than being removed to his home country.

the affiliate, the affiliate would then notify ZAGALA of the intrusion.

- c. CHS-1 asked how many affiliates the software could support, and ZAGALA said that he personally had “a maximum of between 10-20” affiliates at a given time, and “sometimes only 5.” ZAGALA explained that hackers would approach him for his software after they had gained access to a victim network: “they come with access to [b]ig LAN, I check and then I accept[.] they lock several big networks and we wait.... If you lock networks without tape or cloud (backups)[,] almost all pay[.]” Based on my knowledge, training and experience, the meaning of ZAGALA’s remark is that ransomware victims are vulnerable to extortion if they lack backup copies of their data, whether local (stored on tape media) or remote (in cloud storage). In such a situation, the victim’s only recourse to recover its data is paying the attackers.
- d. ZAGALA further explained that, sometimes, a victim network turned out to have an unexpected backup: “so no point in locking because they have backups, so in that case we only exfiltrate data,” referring to stealing victim information. ZAGALA further added that he had an associate who “knows how to corrupt tapes,” meaning backups, and how to “disable[] AV,” meaning antivirus software.
- e. Finally, ZAGALA offered to give the CHS an additional two weeks free after the CHS’s one-month license expired, explaining “because 1 month is too little for this business . . . sometimes you need to work a lot to get good profit.”

32. ZAGALA has also publicly discussed his knowledge that his clients are using his software to commit ransomware attacks.

33. For example, on or about November 18, 2019, ZAGALA (using the nickname “Nosophoros”) started a thread on Forum-2 titled “[SALE] Private Ransomware Builder Designed for Companies Targeted Attacks.”

34. On or about and between October 2020 and January 2021, ZAGALA posted more than ten messages to the thread, describing updates to the Thanos software.


Most of ZAGALA's posts offered free support to former clients who needed to decrypt victim information acquired with prior, non-compatible versions of the Thanos software.

35. In addition, multiple users wrote postings on the same thread describing their experiences using Thanos to commit ransomware attacks. For example:

- a. A user named "Drumrlu," who has previously offered for sale access to hacked networks, posted a message praising Thanos on or about July 7, 2020. Drumrlu wrote: "hello everyone, i bought the ransomware from nosophoros and it is very powerful with a lot of future. it also bypass all AV with it's Shellcode Generator. i use that in big network(around 3k PC) and it's work and hit all PCs. I completely recommend This RS." Based on my training and experience, the reference to "3k PC" indicates a victim network comprising three thousand personal computers.
- b. On December 17, 2020, another user named "Nify" wrote a message in Russian stating: "We have been working with this product for over a month now, we have a good profit! Best support I've met."

36. ZAGALA posted messages announcing improvements to Thanos in the same thread within six days on either side of Drumrlu's message and within eight days on either side of Nify's message.

37. In the same thread as the above messages, ZAGALA also posted links to new stories recounting the use of Thanos by an Iranian state-sponsored hacking group to attack Israeli companies, as shown in the following image:

<p>Nosophoros megabyte ●●●</p>  <p>User +9 88 posts Joined 11/17/19 (ID: 97282) Activity</p>	<p>Posted October 24, 2020</p> <p>Change Log:</p> <ul style="list-style-type: none"> --Boosted decryptor speed. --Boosted encryption speed in extensions mode as well as in All files mode. --Boosted speed and increased number of files catch in NTFS mode. --Added new self replication and spreading method that also provides persistence. --Windows server and 10 anti network discovery bypass demonstration: https://mega.nz/file/YcY0 is able to discover the path of the network connection by itself). --News on Thanos used along with other exploits taking advantage of the MBR locking feature: https://exploit.in/2020/13767/ https://www.securitylab.ru/news/513162.php?ref=123
--	--

V. ZAGALA'S RECENT ACTIVITY

38. On or about November 30, 2021, ZAGALA began advertising malicious software online under a new nickname, “Nebuchadnezzar.” Multiple postings in online forums by “Nebuchadnezzar” were identical to contemporaneous postings by “Nosophoros.”


39. On or about March 30, 2022, a second confidential source of the FBI (“CHS-2”) communicated with ZAGALA in an online forum about using ransomware.¹⁰ The FBI has obtained copies of those written communications. ZAGALA, using the nickname “Nosphoros,” explained to CHS-2 that “big profit comes from rdp,” meaning remotely logging in to victims’ computers to encrypt their files. ZAGALA then assured CHS-2 that the “Nebuchadnezzar” nickname also belonged to ZAGALA: “it’s me too . . .

¹⁰ CHS-2 has pled guilty to multiple crimes in federal court, including conspiracy to commit wire fraud and computer intrusion. CHS-2 is cooperating with the FBI in hopes of receiving leniency at sentencing. In addition, CHS-2 hopes to receive an immigration benefit from the government that would permit him to remain in the United States rather than being removed to his home country. CHS-2’s information has been corroborated by other sources.


Nebuchadnezzar.” ZAGALA explained that he had adopted a new alias because of “OPSEC . . . operational security.” ZAGALA added that “malware analysts are all over me.”

40. On or about May 3, 2022, law enforcement agents conducted a voluntary interview of the Florida Relative. During the interview, the Florida Relative acknowledged that he is ZAGALA’s relative. The Florida Relative further stated, in sum and substance, that ZAGALA resides in Venezuela and had taught himself computer programming. The Florida Relative also showed law enforcement his phone, which contains contact information for ZAGALA, including the Gmail-2 email address used to register the Thanos Control Server and the phone number also associated with moiseszagala[.]gmail.com.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendant MOISES LUIS ZAGALA GONZALEZ, also known as “Nosophoros,” “Aesculapius” and “Nebuchadnezzar,” so that he may be dealt with according to law.


CHRIS CLARKE
Special Agent
Federal Bureau of Investigation

by telephone
Sworn to before me this
16th day of May, 2022


THE HONORABLE MARCIA M. HENRY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK