

N3TW0RM ransomware emerges in wave of cyberattacks in Israel

bleepingcomputer.com/news/security/n3tw0rm-ransomware-emerges-in-wave-of-cyberattacks-in-israel/

Lawrence Abrams

By

[Lawrence Abrams](#)

- May 3, 2021
- 05:46 PM
- 1



A new ransomware gang known as 'N3TW0RM' is targeting Israeli companies in a wave of cyberattacks starting last week.

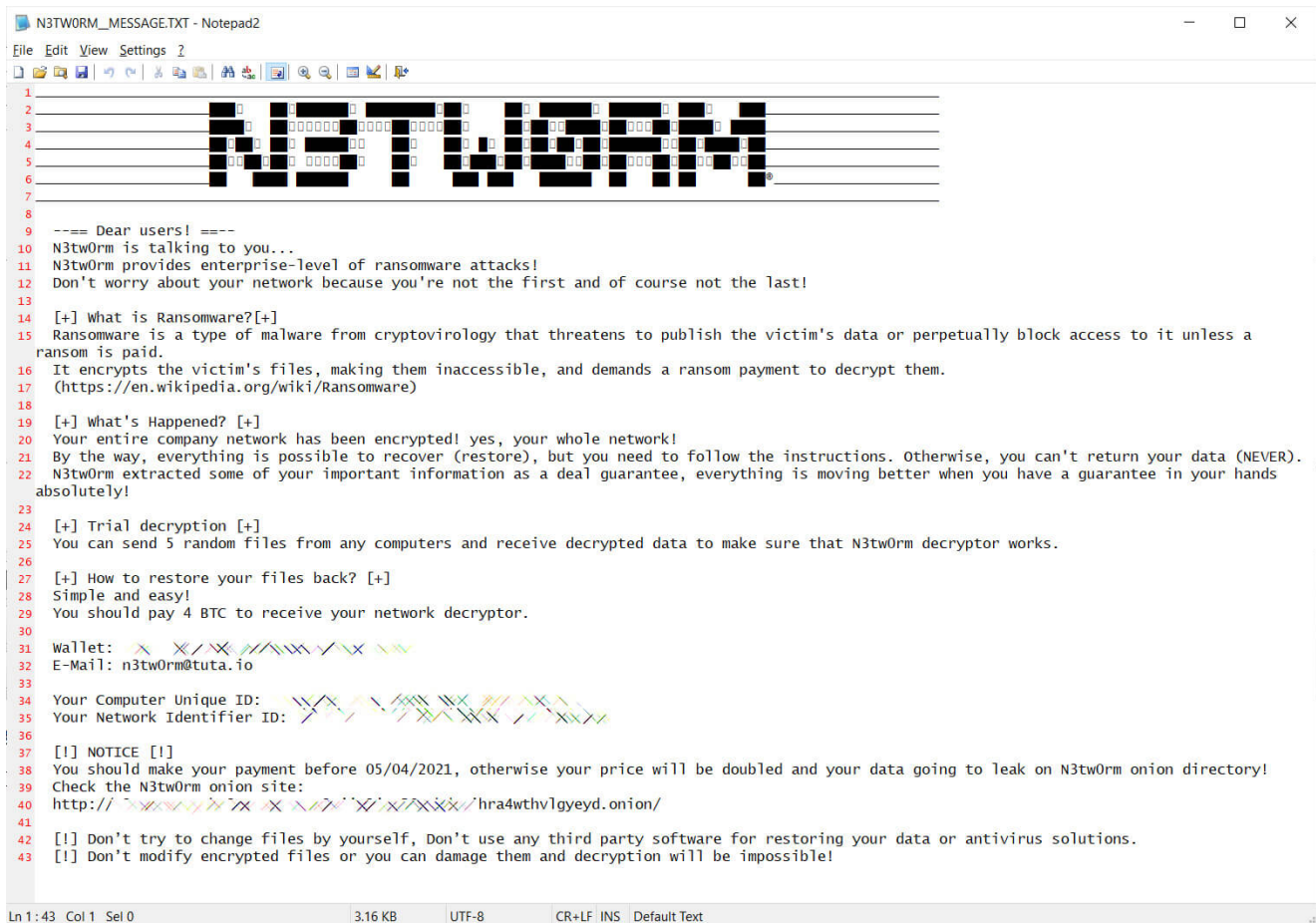
Israeli media Haaretz reported that at least four Israeli companies and one nonprofit organization had been successfully breached in this wave of attacks.

Like other ransomware gangs, N3TW0RM has created a data leak site where they threaten to leak stolen files as a way to scare their victims into paying a ransom.

Two of the Israeli businesses, H&M Israel and Veritas Logistic's networks, have already been listed on the ransomware gang's data leak, with the threat actors already leaking data allegedly stolen during the attack on Veritas.

From the ransom notes seen by Israeli media and BleepingComputer, the ransomware gang has not been asking for particularly large ransom demands compared to other enterprise-targeting attacks.

Haaretz [reports](#) that Veritas' ransom demand was three bitcoin, or approximately \$173,000, while another ransom note shared with BleepingComputer shows a ransom demand of 4 bitcoins, or roughly \$231,000.



```
1
2
3
4
5
6
7
8
9 --- Dear users! ---
10 N3tw0rm is talking to you...
11 N3tw0rm provides enterprise-level of ransomware attacks!
12 Don't worry about your network because you're not the first and of course not the last!
13
14 [+] What is Ransomware? [+]
15 Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a
ransom is paid.
16 It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.
17 (https://en.wikipedia.org/wiki/Ransomware)
18
19 [+] What's Happened? [+]
20 Your entire company network has been encrypted! yes, your whole network!
21 By the way, everything is possible to recover (restore), but you need to follow the instructions. Otherwise, you can't return your data (NEVER).
22 N3tw0rm extracted some of your important information as a deal guarantee, everything is moving better when you have a guarantee in your hands
absolutely!
23
24 [+] Trial decryption [+]
25 You can send 5 random files from any computers and receive decrypted data to make sure that N3tw0rm decryptor works.
26
27 [+] How to restore your files back? [+]
28 Simple and easy!
29 You should pay 4 BTC to receive your network decryptor.
30
31 Wallet:
32 E-Mail: n3tw0rm@tuta.io
33
34 Your Computer Unique ID:
35 Your Network Identifier ID:
36
37 [!] NOTICE [!]
38 You should make your payment before 05/04/2021, otherwise your price will be doubled and your data going to leak on N3tw0rm onion directory!
39 Check the N3tw0rm onion site:
40 http://
41
42 [!] Don't try to change files by yourself, Don't use any third party software for restoring your data or antivirus solutions.
43 [!] Don't modify encrypted files or you can damage them and decryption will be impossible!
```

N3TW0RM ransom note

Source: *BleepingComputer*

A WhatsApp message shared among Israeli cybesrecurity researchers also states that the N3TW0RM ransomware shares some characteristics with the Pay2Key attacks conducted in November 2020 and February 2021.

Forwarded

חברים, לתשומת לבכם שנראה שמתחיל גל תקיפות Ransom מקבוצת תקיפה שמזדהה כ N3tw0rm. היא עושה שימוש ב"שם מסחרי" וב"מותג" של בלוגר סייבר רוסי מוכר (ככל הנראה כדי להסתוות לרוסים), אבל אין לה כל נוכחות אחרת, מלבד "אתר שיווקי" חדש ב-TOR, שריק מתכנים. התקשורת עם התוקף הדליקה נורות אזהרה, וצוות טכנולוגי שמנהל את האירוע (עומר פינסקר) הצליח לזהות מספר סממנים דומים ל-ל-FoxKitten האיראני (Pay2Key מנובמבר וגל שני בפברואר). נראה שהוא עושה שימוש באותן ספריות, קורא לפרמטרים באותו השם. הועבר עדכון ראשוני למערך הסייבר. ממליצים להיות עירנים, ובשום מקרה לא לשלם את הכופר.

WhatsApp message shared among security researchers

Pay2Key has been linked to an Iranian nation-state hacking group known as Fox Kitten, whose goal was to cause disruption and damage to Israeli interests rather than generate a ransom payment.

The N3TW0RM attacks have not been attributed to any hacking groups at this time.

Due to the low ransom demands and lack of response to negotiations, one source in the Israeli cybersecurity industry has told BleepingComputer that they believe N3TW0RM is also being used for sowing chaos for Israeli interests.

However, Arik Nachmias, CEO of incident response firm Honey Badger Security, told BleepingComputer that he believes that in N3TW0RM's case, the attacks are motivated by money.

Unusual client-server model to encryption

When encrypting a network, threat actors will usually distribute a standalone ransomware executable to every device they wish to encrypt.

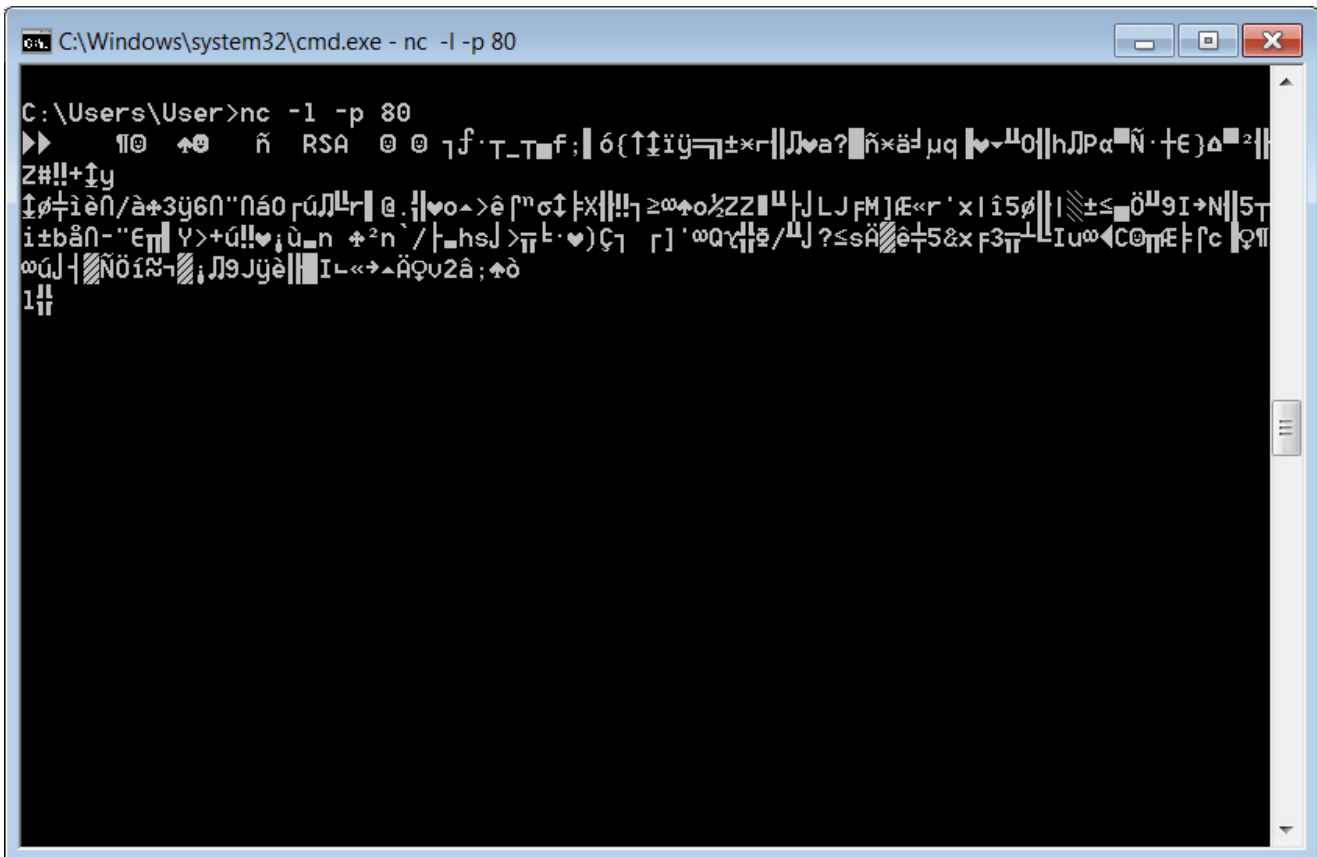
N3TW0RM does it a bit differently by using a client-server model instead.

From samples [[VirusTotal](#)] of the ransomware seen by BleepingComputer and discussions with Nachmias, the N3TW0RM threat actors install a program on a victim's server that will listen for connections from the workstations.

Nachmias states that the threat actors then use [PAExec](#) to deploy and execute the 'slave.exe' client executable on every device that the ransomware will encrypt. When encrypting files, the files will have the '.n3tw0rm' extension appended to their names.

While BleepingComputer does not have access to the server executable, we set up NetCat to listen and wait for connections on port 80. We then launched the slave.exe client, so it connects back to our IP address on that port.

As you can see below, when the client connects back to port 80 on our device running NetCat, it will send an RSA key to the server.



Sending an RSA key back to the N3TW0RM server

Source: BleepingComputer

Nachmias told BleepingComputer that the server component would save these keys in a file and then direct the clients to begin encrypting devices.

This approach allows the threat actor to keep all aspects of the ransomware operation within the victim's network without being traced back to a remote command & control server.

However, it also adds complexity to the attack and could allow a victim to recover their decryption keys if all of the files are not removed after an attack.

Related Articles:

[Costa Rica declares national emergency after Conti ransomware attacks](#)

[New Black Basta ransomware springs into action with a dozen breaches](#)

[American Dental Association hit by new Black Basta ransomware](#)

[Wind turbine firm Nordex hit by Conti ransomware attack](#)

[Hackers use Conti's leaked ransomware to attack Russian companies](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.