The Nemty affiliate model

By Benoit ANCEL

Published: 2021-01-25 · Archived: 2026-04-05 13:33:12 UTC

Almost a year after the end of the operations of the Nemty ransomware, we are presenting some internal details of their operations between 2019 and 2020 in order to document the business model and the actors that evolved around that group.

This article is not meant to be a technical analysis of the capacities of the ransomware - McAfee has already published an amazing analysis covering the evolution and the technical capacities of Nemty. We are here trying to show how the RaaS was working internally and to characterise the different affiliates in order to document an important ransomware threat of 2019.

Nemty backend

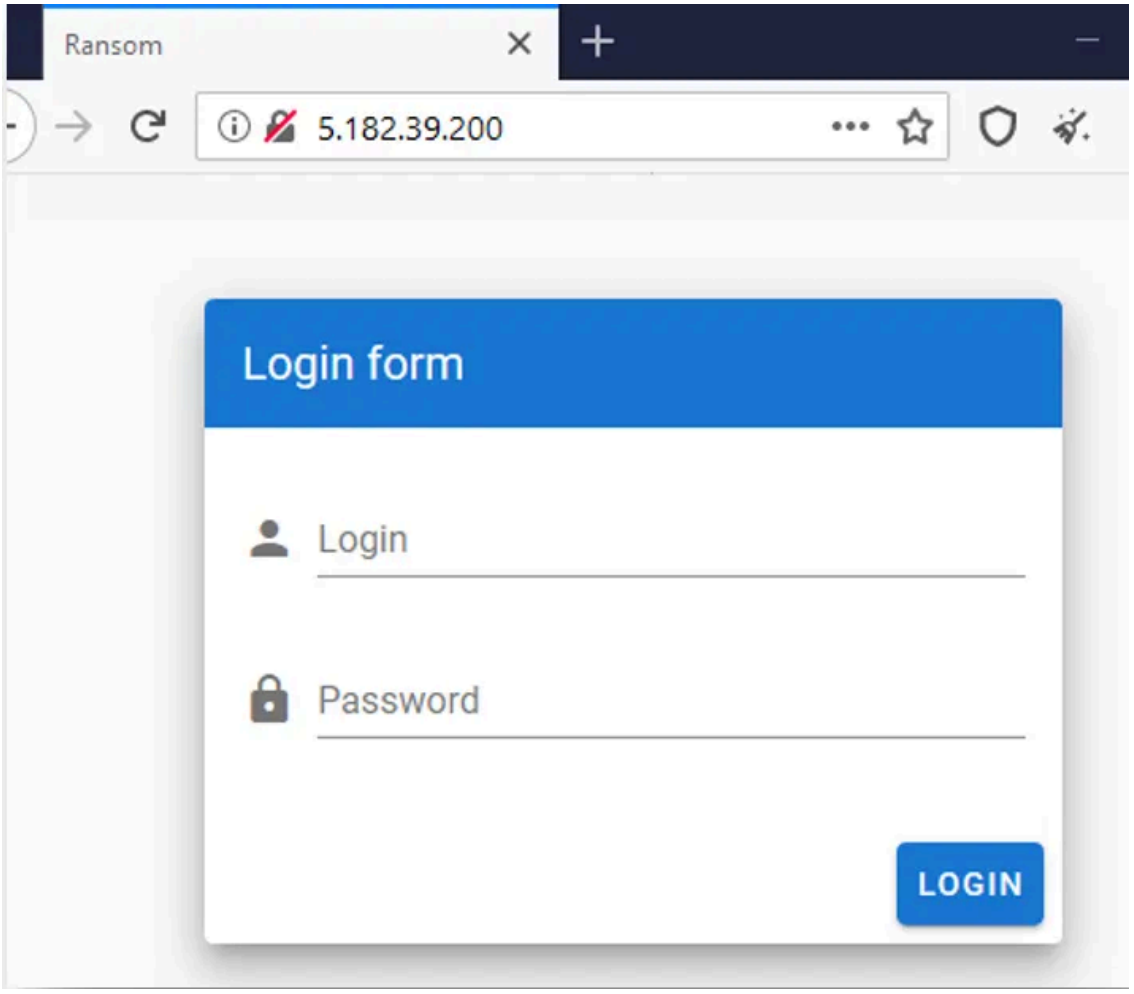
Like lots of threat actors in 2019, the Nemty gang chose to hide their backend behind a Fast Flux called Brazzzer. Both domains nemty[.]top and nemty[.]hk were protected in order to not reveal the real IP of the control server.

The domains were resolving to different temporary IPs (nginx proxies) managed by the Fast Flux, and those proxies were redirecting the traffic to the real server.

However, staying anonymous on the internet is hard. The protection of a fast flux alone is far from enough to protect the IP of a hidden server. Also Nemty eventually leaked the real IP of their server: **5[.]182[.]39[.]200**.

Their control server was poorly configured, allowing anyone to access the CnC directly from the IP, making our investigation much easier:

> Press enter or click to view image in full size



We observed this IP being used over the Nemty domains **throughout the entire operation until the end of the ransomware**.

Nemty backend

Nemty was a Ransomware-as-a-Service. The backend was a central panel poorly developed in JavaScript using the library socket.io. Each affiliate could login with their own credentials. The whole backend was managed through an admin account able to see and manipulate all the affiliate's bots.

Each affiliate could see their own bots, interact with the encrypted victims, build new stubs of the ransomware and discuss with the admin.

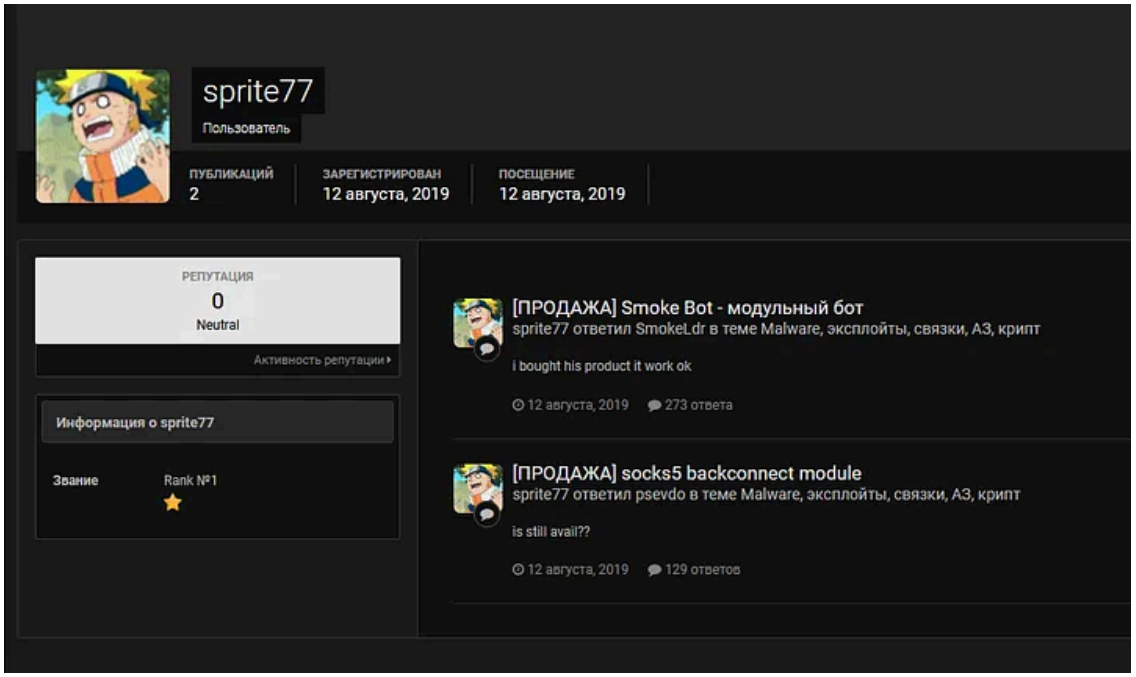
Affiliates

As shown in the last screenshot, the interesting part of the backend was the affiliates list. You can see below the full list of observed affiliates:

Nickname	Status	Registration date
support	user	08.19.2019 14:48:11
sershes	user	08.20.2019 16:51:39
evo	admin	08.20.2019 18:41:07
Polkilo	user	08.20.2019 19:01:14
jokeroo	user	08.21.2019 18:23:08
sprite77	user	08.22.2019 06:29:07
slack25	user	08.22.2019 17:18:44
dodoaska	user	08.30.2019 08:49:29
darma	user	08.30.2019 17:53:52
symmetries	user	09.01.2019 05:58:35
sinner	user	09.01.2019 11:10:26
1337	user	09.25.2019 15:00:26
supra	user	09.04.2019 11:40:49
deadpool	user	09.27.2019 09:03:12
supramet	user	09.25.2019 16:38:11
faceid	user	09.06.2019 10:57:35
droids	user	09.30.2019 10:16:55
vincentvegaaa	user	09.30.2019 10:21:39
quake	user	09.07.2019 19:10:38
phoz	user	10.04.2019 11:45:01
570rm	user	10.04.2019 18:39:36
titan	user	09.11.2019 16:21:41
orthon	user	10.06.2019 12:50:47
sakata	user	09.12.2019 14:26:52
helliscold	user	09.17.2019 19:27:02
bibimik	user	09.21.2019 14:43:52
fvoid	user	09.24.2019 13:41:59
555	user	09.22.2019 04:40:48

If you are familiar with the RaaS ecosystem of 2019/2020, you will quickly see some well-known nicknames. E.g. “jokeroo” was a well-known actor trying to run his own business, symmetries was also known around others RaaS, helliscod was also known on numerous forums buying different malware like Raccoon, and sprite77 was a well- known GandCrab affiliate.

Press enter or click to view image in full size



All those nicknames can be found all over the place showing that the affiliates of RaaS are not spending their money on only one project. It was/is very common to see the same actors showing up on different RaaS and when we see lots of different campaigns distributing lots of ransomware families, it is, in fact, a small pool of actors. You can still find some of them around Dharma ransomware or DJVU in 2021.

The panel developer's mistakes

As mentioned earlier, Nemty was running between August 2019 and April 2020 and we monitored the same single IP used as backend during the whole operation: **5[.]182[.]39[.]200**.

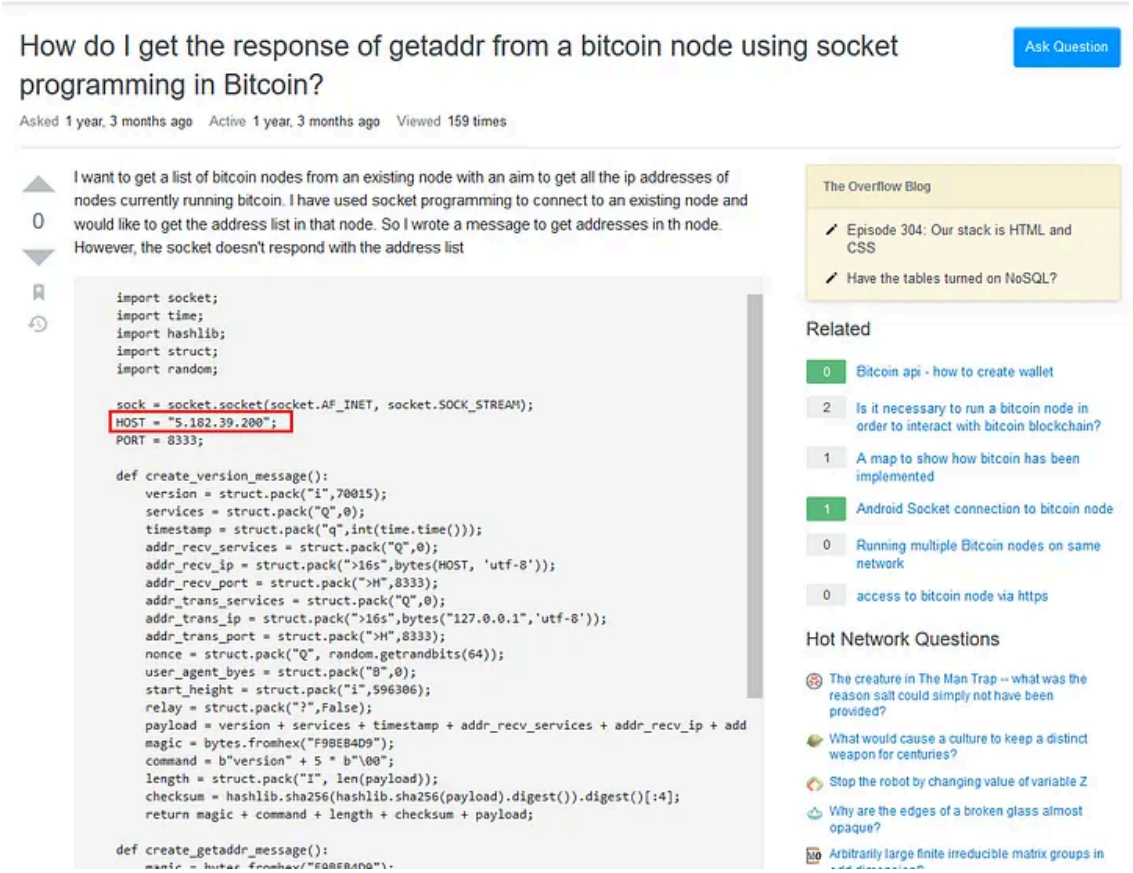
Get Benoit ANCEL's stories in your inbox

When you do try to obtain open sourced intelligence about an infrastructure, one of the best places to dig is **StackOverflow**.

Criminals or not, behind these kind of operations at the end of the day it's still humans developing products and having trouble debugging the code.

The 25th September 2019 a user using the nickname Sajan Maharjan opened a new thread asking for help to debug the implementation of a Bitcoin node:

> Press enter or click to view image in full size



Screenshot of the StackOverflow Post

We can see here the original poster pasting some code mentioning `HOST = "5.182.39[.]200";`. Curiously enough, the Nemty IP had that port 8333 opened too at that time.

That StackOverflow user seems to be working with JavaScript library and UI development and is living in South Korean where Nemty was the most active in the wild in 2019. Those elements can suggest that this user was related to the backend developers of the Nemty operation.

These kinds of mistakes are a good reminder about the power of the data exposed on StackOverflow. It’s not the first actor making that mistake and he will not be the last.

Conclusion

This article tries to document the affiliates model and the actors that evolved around Nemty in 2019/2020 in order to facilitate future investigation of fresh threats potentially used by those criminals.

For the whole history and technical details about Nemty I recommend reading the paper written by McAfee researchers: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/nemty-ransomware-learning-by-doing/

Appendix

Virtual hosts observed on the IP 5.182.39[.]200:

- nemty[.]top

- nemty[.]hk
- nemty10[.]hk

Early Nemty change-log (translated from Russian):

```
- 08.20.2019 16:56:51 Release date
Panel is ready
Cryptolocker is ready
- 08.22.2019 07:22:55 Update 1.0.1 & 1.0.2
Fixed builder page Added page loader Added drives section on bots page
- 08.24.2019 09:32:35 Update 1.1 & 1.0.3
Ransomware:
Encryption speed increased significantly due to asynchronization of threads Extension changed to ._N
Added simple tags like “@admin” (admin will come) Fixed some bugs
- 08.25.2019 09:15:29 WARNING UPDATE BUILDS
- 08.26.2019 08:09:48 update your builds actual version — 1.3
- 08.26.2019 08:49:57 Important to read to everyone
Now two victims from two different countries have tapped, both write the same:
Guy, test decrypt isn’t working, but I can’t pay you so much, because I’m not a rich man.
I went to look for a problem, why didn’t they decrypt the files from them.
Found this file that they were trying to decrypt.
Since I leave the encrypted key and the file extension at the end of the file, I noticed that the fi
It was decided to add a check for the extension in the file body, which will be available today.
- 08.28.2019 12:56:42 UPDATE RANSOMWARE
Added:
No configuration file, everything in ransom note
Fix CD-ROM
- 08.29.2019 19:50:38 SECURITY WARNING
check your BTC address, if you will have no BTC address in settings, victims couldn’t open payment pa
- 08.31.2019 06:51:19 Update
Added saving of any messages
- 09.06.2019 11:19:58 ransomware update
victim will be appeared in the panel before encrypting files
- 09.09.2019 08:46:37 Mini update
update build, now ransomware will skip files with
“nemty”, “exe”, “log”, “cab”, “cmd”, “com”, “cpl”, “exe”, “ini”, “dll”, “url”, “ttf”, “url”
extension and even in upper case
added process kill
“sql”, “winword”, “wordpad”, “outlook”, “thunderbird”, “oracle”, “excel”, “onenote”, “virtualboxvm”
added service stop
“DbxSvc”, “OracleXETNSListener”, “OracleServiceXE”, “AcrSch2Svc”, “AcronisAgent”, “Apache2.4”, “SQLW
if you want expand this lists — admin jabber is nemty@thesecure.biz
- 09.24.2019 05:35:24 update 1.5
FastFlux
- 09.27.2019 09:05:57 CLEANING
OLD BOTS WERE DELETED BECAUSE USELESS
- 10.02.2019 15:28:23 1.6 ransomware update
```

```
changed encryption algorithm
added our own key generator (not pseudo keys)
- 10.10.2019 08:25:03 update builds
if there is no internet, it won't get an IP and as a result the panel will not detect the IP string a
so update the builds, all bots that have no Internet or haven't received an IP will be from IP Austra
```
