When Viruses Mutate: Did SunCrypt Evolve from QNAPCrypt?

By Joakim Kennedy

Published: 2021-03-02 · Archived: 2026-04-05 18:49:40 UTC

Dov Lerner from Cybersixgill contributed to this report

Intro

Programmers frequently reuse code, as recycling something that is already written and functional is much more efficient than writing from scratch. Malware authors are no different; functions and modules from one malware can be reused in the next. Because of this, code reuse analysis can connect different malware to the same author.

When performing code reuse analysis, it is important to ensure that the code is unique to the specific developer and not common code that, for example, is part of an open-source library since open-source code can be used by many and cannot be tied to a specific author. If this is handled correctly, code reuse is a very powerful method for attributing malware to a specific malware author.

There is a constant churn of new actors and malware families. However, sometimes a seemingly new threat actor is just a “rebranding” or a new group formed by known actors. For example, in May 2019, the GandCrab group announced that they were retiring from their ransomware activity. Not long after, researchers connected a new ransomware called REvil (also known as Sodinokibi) to the then defunct GandCrab ransomware. REvil shared unique code similarities with GandCrab. This suggested that when GandCrab was closing down, the malware authors switched to develop a new ransomware using some of the code from GandCrab in a new collaboration with other threat actors.

This report uses both dark web research and malware analysis to investigate the connection between the affiliate ransomware service known as SunCrypt and the QNAPCrypt ransomware, the latter of which was used against QNAP and Synology devices back in 2019. While the two ransomware are operated by distinct different threat actors on the dark web, there are strong technical connections in code reuse and techniques, linking the two ransomware to the same author. Just because a malware is a derivative of another malware does not mean it will be deployed in exactly the same way. A new operator may use different targets, tactics, techniques and procedures (TTPs), which can include new evasion techniques. Defenders must remain vigilant.

Technical Connection

SunCrypt is a Ransomware as a Service (RaaS) that uses a closed affiliate program on the dark web. The history of this RaaS can be traced back to circa October 2019. In October 2019, a new ransomware was found in-the-wild (5657abdb9d99cd5aec433099f8d6f53d). The new ransomware was written in Go and targeted Windows machines. This version of SunCrypt was not reported in many attacks and it wasn’t until mid-2020 when a new version of the ransomware written in C/C++ was discovered, that attacks started to increase. It is an interesting shift of retooling from Go to C/C++ when other groups are instead retooling from C/C++ to Go.

While the RaaS didn't appear until October 2019, these ransomware share connections with another ransomware, called QNAPCrypt (also known as eCh0raix), that was used to target Network Attached Storage (NAS) devices back in July 2019. Both families share identical code logic for the file encryption, which we can conclude with high certainty has been compiled from the same source code.

SunCrypt 2020 and SunCrypt 2019

The SunCrypt variant that was released in 2020 is written in C. Due to this, it does not have any shared code with the earlier version from 2019. The functionality of SunCrypt has been well-documented and some of the behaviors are similar between the two variants. For example, both variants are designed to encrypt and steal data. This, together with the name, is not enough to link the two variants together. Instead, we have to look at other data points.

After the ransomware has stolen and encrypted the files on the infected machine, the user is presented with a ransom note. The ransom note for the 2020 variant is shown in Figure 1 below. The note can be read in English, German, French, Spanish or Japanese. It has an input box that when the user enters the unique ID, sends the user to a chat interface.

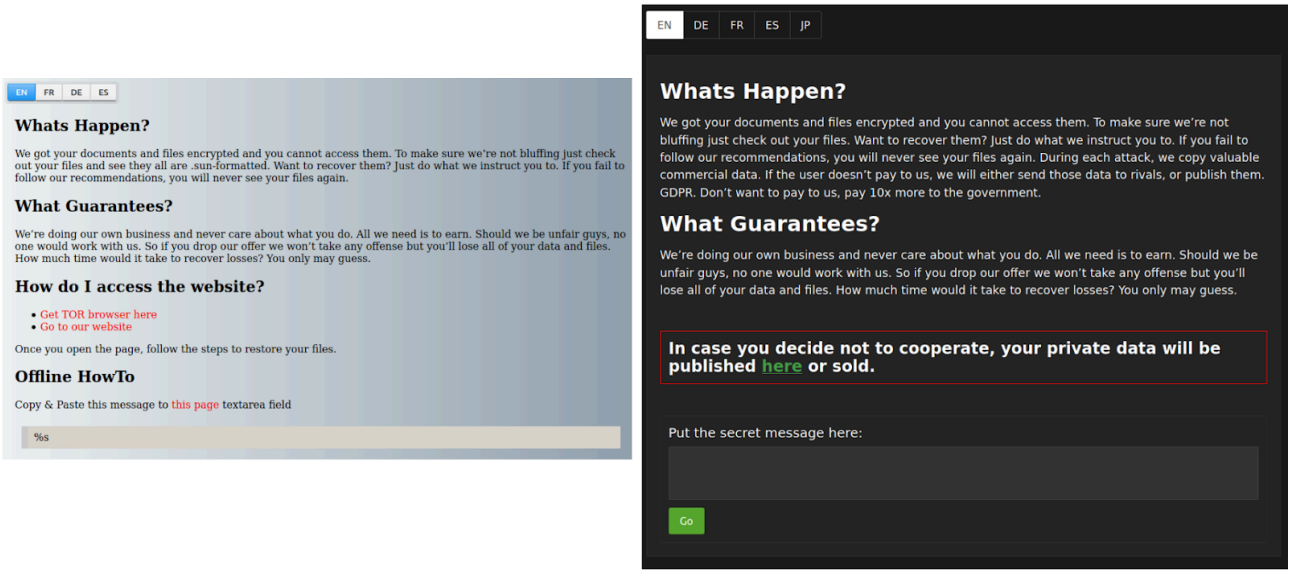


Figure 1: Ransom note pages for SunCrypt. Left is showing the original ransom note and right is showing the current ransom note used. Both share the same typos and structure. The current ransom note provides a link to the leak site while the original note does not.

The ransom note for the 2019 variant is very similar. It has essentially the same text. The background color is different. The major difference is that the 2019 version does not include the text of leaking the stolen data if the ransom is not paid, as can be seen in Figure 1.

Connection to QNAPCrypt

The 2021 variant is potentially a beta release of the RaaS. The version included in the PDB path is "0.1" as can be seen in Figure 2. The figure is showing a partial output of redress, a tool used to analyze Go binaries. As part of

the output, we can see a file called “aes.go” with two functions. Note that one of the functions has a typo in the name, “EncEAS” instead of “EncAES.” A similar file has been found being part of another malware family, QNAPCrypt. This typo was included in two samples of version 2 of QNAPCrypt (8dd59345cc034317630b2ac2ee19b362 and 516291d10b370c7be3863335cf5d57eb). An output generated by redress from one of the QNAPCrypt samples is shown in Figure 3. After searching both our data set of malware and a retro hunt on VirusTotal, only these three samples have the two function names. From this, we can conclude that the typo is unique and potentially shared code between the two ransomware families.

```
Package main: _/home/service00/sun-0.1/src
File: aes.go
        EncEAS Lines: 84 to 172 (88)
        EncFile Lines: 172 to 175 (3)
```

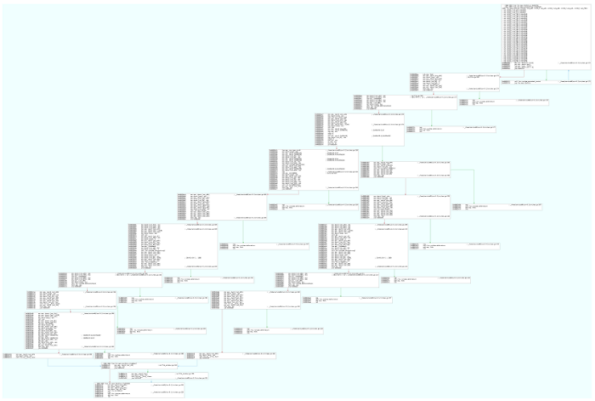
Figure 2: Partial output of redress for SunCrypt 2019 variant. One of the functions has the typo EAS instead of AES.

```
Package main: _/home/ubn/Documents
File: file.go
        EncEAS Lines: 13 to 100 (87)
        EncFile Lines: 100 to 103 (3)
File: main.go
        init0 Lines: 27 to 42 (15)
        main Lines: 42 to 93 (51)
        mainfunc1 Lines: 73 to 82 (9)
        randSeq Lines: 93 to 102 (9)
        writemessage Lines: 102 to 106 (4)
        chDir Lines: 106 to 117 (11)
        check Lines: 117 to 144 (27)
        locale Lines: 144 to 149 (5)
File: rsa.go
        makesecret Lines: 29 to 73 (44)
```

Figure 3: Output from redress for a version of QNAPCrypt with the same typo.

A deeper analysis of the function confirms that they are derived from the same source. A flow graph of “EncFile” is shown in Figure 4 and a flow graph for “EncEAS” is shown in Figure 5.

SunCrypt



QNAPCrypt

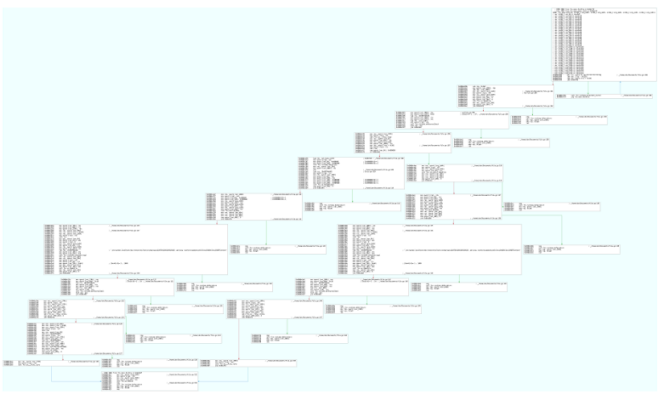


Figure 4: Flow graphs for EncFile function. The flow is identical.

The samples are compiled for different operating systems and architectures using different versions of the Go compiler which results in a slight difference in the generated assembly code. The function opens a file handler to the file to be encrypted. It uses the "Stat" function provided by Go's standard library to determine the file size. Based on the size, the flow splits into two different branches.

For SunCrypt, if the file is larger than 100 MB it goes down one branch while QNAPCrypt uses a cutoff of 10 MB. Files smaller than the cutoff size goes down to the second branch. In the large file branch, the SunCrypt reads in the first 100 MB using the "ReadAtLeast" function that is part of the standard library "io" package. QNAPCrypt does the same but in the first 10 MB instead.

For the smaller files, both families use the "ReadFile" function from the "io" package. The read-in data is passed to the "EncEAS" function that encrypts the data. The content is finally written to disk as a new file with an extension appended while the original file is removed. Except for the size cutoff, the function logic in the two families is identical.

The "EncEAS" function encrypts the data using AES in Cipher Feedback (CFB) mode. A comparison between the flow graphs is shown in Figure 5 below. As with the "EncFile" function, the "EncEAS" function has an identical logic and it can be confirmed that it was compiled from a very similar source code.

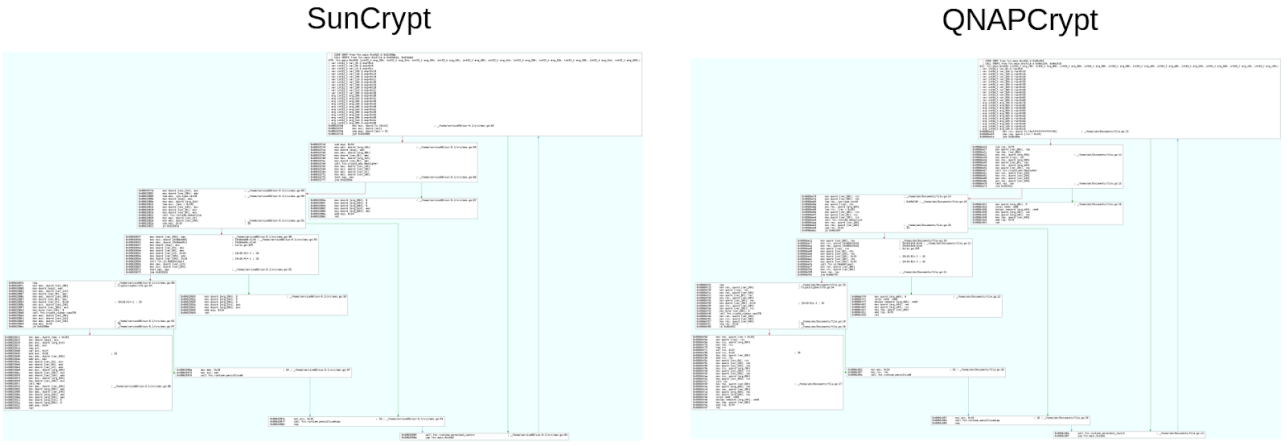


Figure 5: Flow graph comparison between SunCrypt and QNAPCrypt's "EncEAS" function.

Other Similarities

In addition to the shared code between the two malware families for the functionality responsible for the file encryption, the two families also have other similarities. The similarities on their own do not indicate a connection, but the collection of all of them does. The presentation of them is to strengthen the connection indicated by the shared code. Figure 6 is showing functions in QNAPCrypt that share similarities with functions in SunCrypt.

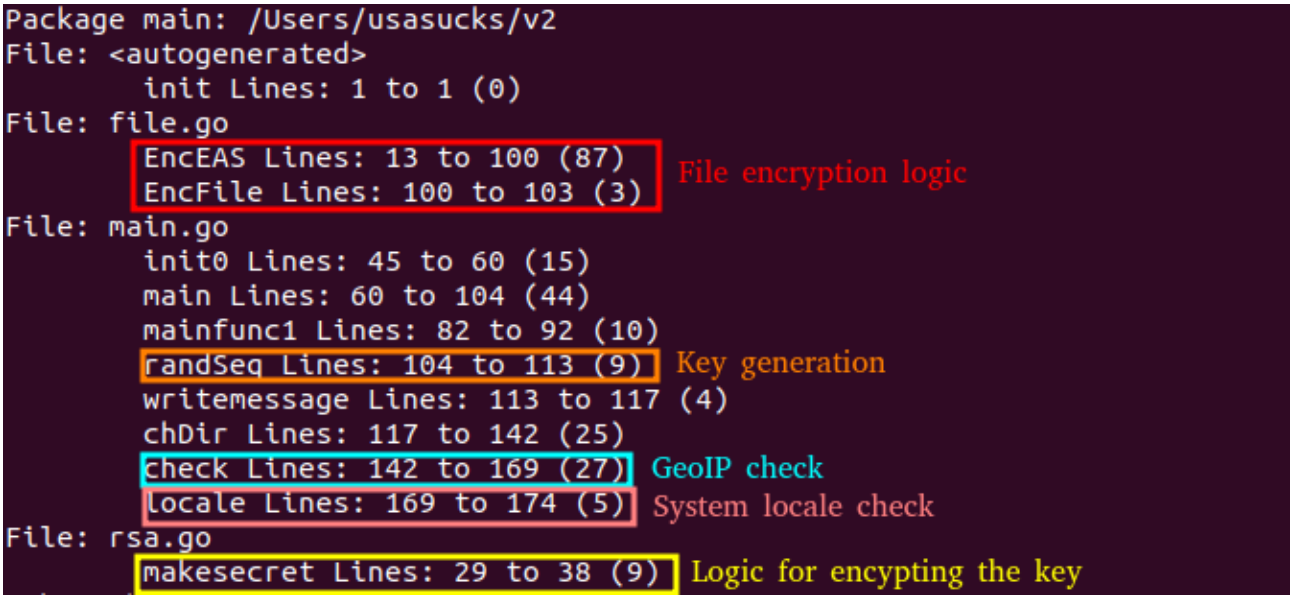


Figure 6: Functions with similarities between QNAPCrypt and SunCrypt. File encryption logic is identical while the key generation and the encryption of the key is very similar. Both malware use the locale of the machine and GeoIP to determine the location of the machine.

Both ransomware are designed to not run on some of the Commonwealth of Independent States (CIS). QNAPCrypt will not perform any encryption of files if it believes it is running on a Belarusian, Russian or Ukrainian machine. SunCrypt does the same, but also includes Kyrgyzstan and Syria in the list.

The way the ransomware tries to determine this is very similar, both use two sources for this information. One of the sources is the locale of the machine. As QNAPCrypt is targeting Linux machines and SunCrypt targets Windows machines, the way of obtaining this information is different. The second source is via geolocation based on the external IP address of the machine. Both ransomware reaches out to an external service to get this information, “ip-api.com” for SunCrypt and “ipapi.co” for QNAPCrypt. While the families use different services, they both use the locale on the machine and the geoip information to determine if the machine is located in a disallowed country.

As discussed in the section covering the file encryption code, the files are encrypted with AES in CFB mode. Both ransomware generates a unique 32 characters “password.” The logic for generating this code is very similar. A comparison of the logic is shown in Figure 7. The characters in the password are randomly selected from a list of valid characters that includes all the English upper and lower characters and the numbers 0 through 9. The list is identical between the malware. The rand implementation provided the math package in the standard library is used, which means the randomness is not cryptographic. The randomness is seeded with the current time. The main difference is that SunCrypt resets the seed every time the function responsible for generating the “password” is called, while QNAPCrypt sets the seed during the initialization. SunCrypt also uses the function to generate a victim identifier.

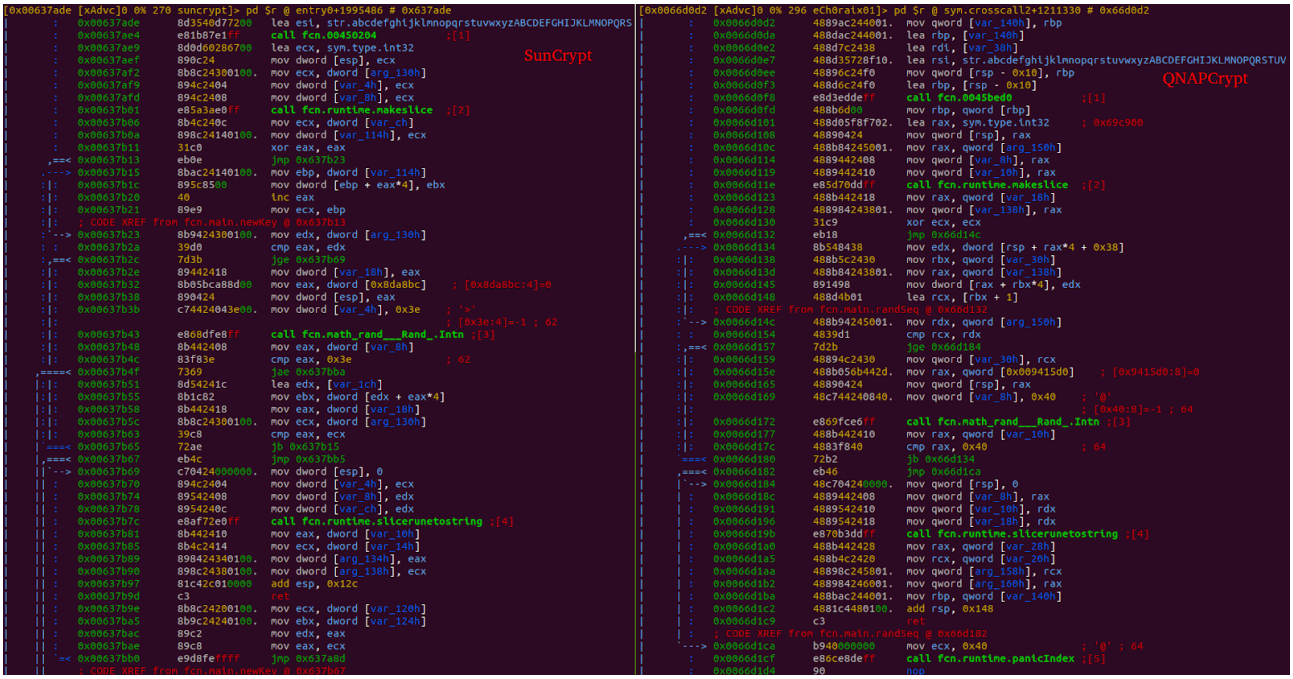


Figure 7: Generation of the encryption password. The function loops 32 times and uses “rand.Intn” to pick a random character from the list of valid characters. When the loop is done, the byte slice of characters is converted to a string.

The encryption password is encrypted with a public RSA key included in the binary. The logic for this code is similar as can be seen in Figure 8. The code uses the “EncryptPKCS1v15” function that is part of the “crypto/rsa” package.

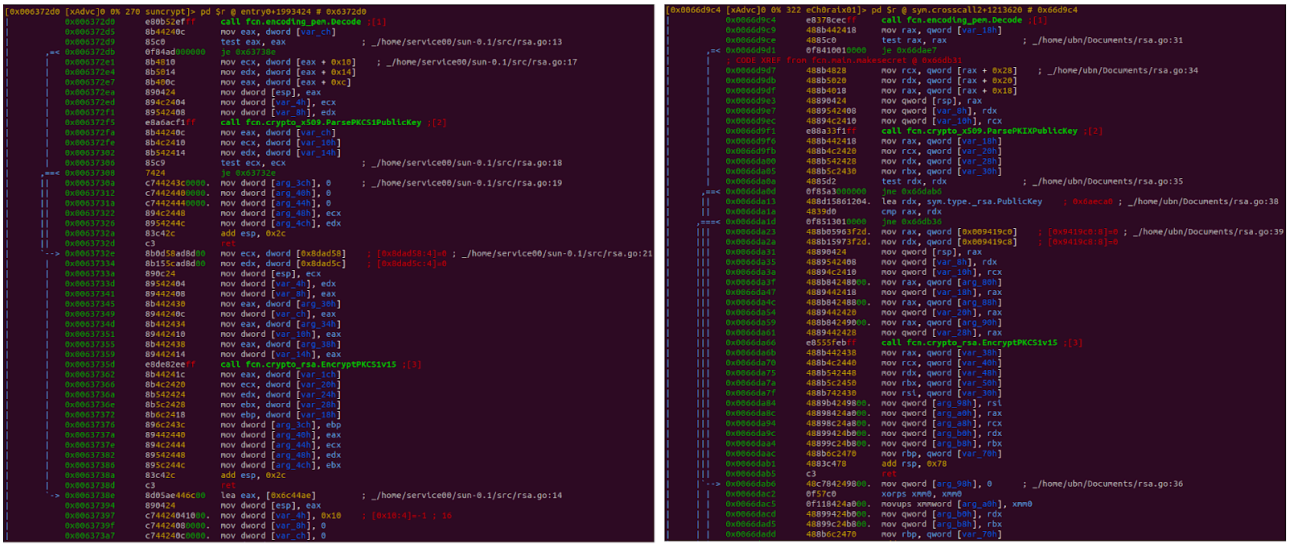


Figure 8: Encrypting of the password using the included public key in the binary.

Both ransomware families have command and control (C2) infrastructure hosted as Tor hidden services. The first version of QNAPCrypt reached out to the C2 to fetch information for the ransom note, including the Bitcoin wallet used for the campaign. SunCrypt sends campaign information and uploads stolen files to the C2 server. To access the hidden service, both families use a public available SocksV5 proxy. QNAPCrypt connects directly to an IP address (192.99.206[.]61) while the proxy used by SunCrypt is accessed via the domain vie8hoos[.]xyz.

The file types encrypted by the ransomware are also similar. Both families have a list of file extensions that they use to determine if the file should be encrypted. In total, SunCrypt has a list of 589 file extensions. If we compare the SunCrypt list to the list used by the first version of QNAPCrypt we can see that SunCrypt's list has added four new entries and removed 19 entries. The lists are not sorted in any way so the extract lists appear exactly in the same order as they appeared in the malware. The code snippet below shows the "diff" between the two lists.

```
$ diff suncrypt_ext.lst qnap_ext_20190705.lst
460d459
< .mp4
562, 564d560
< .java
< .swift
< .go
589a586, 604
> .gcode
> .ngc
> .sldprt
> .sldasm
> .x_t
> .step
> .fits
> .cat
> .ctlg
> .fit
> .rsn
> .eml
> .vhdx
> .cfg
> .plist
```

> .bckup

> .far

> .tbz

> .abf

If we compare SunCrypt's list to the list used by the second version of QNAPCrypt from August the same year, the overlap is even bigger. The "diff" output is shown in the snippet below. The difference is that SunCrypt has added three entries and removed two. This results in a string similarity of 0.991 which is a strong similarity.

$ diff suncrypt-files.lst qnap_ext_20190801.lst

562, 564d561

< .java

< .swift

< .go

589a587, 588

> .gcode

> .ngc

Dark Web Activity

Not long after the public reports on QNAPCrypt/eCh0raix, a new forum user named eCh0raix became active and started promoting the ransomware. Later, a SunCrypt user account promoted a new ransomware affiliate service. While both actors operated on the same popular Russian-language dark web forum, this is where the similarities end.

eCh0raix

The actor behind eCh0raix first posted on August 31, 2019, announcing an affiliate program for a ransomware targeting Linux, Figure 9. This includes a diagram showing how the program works.

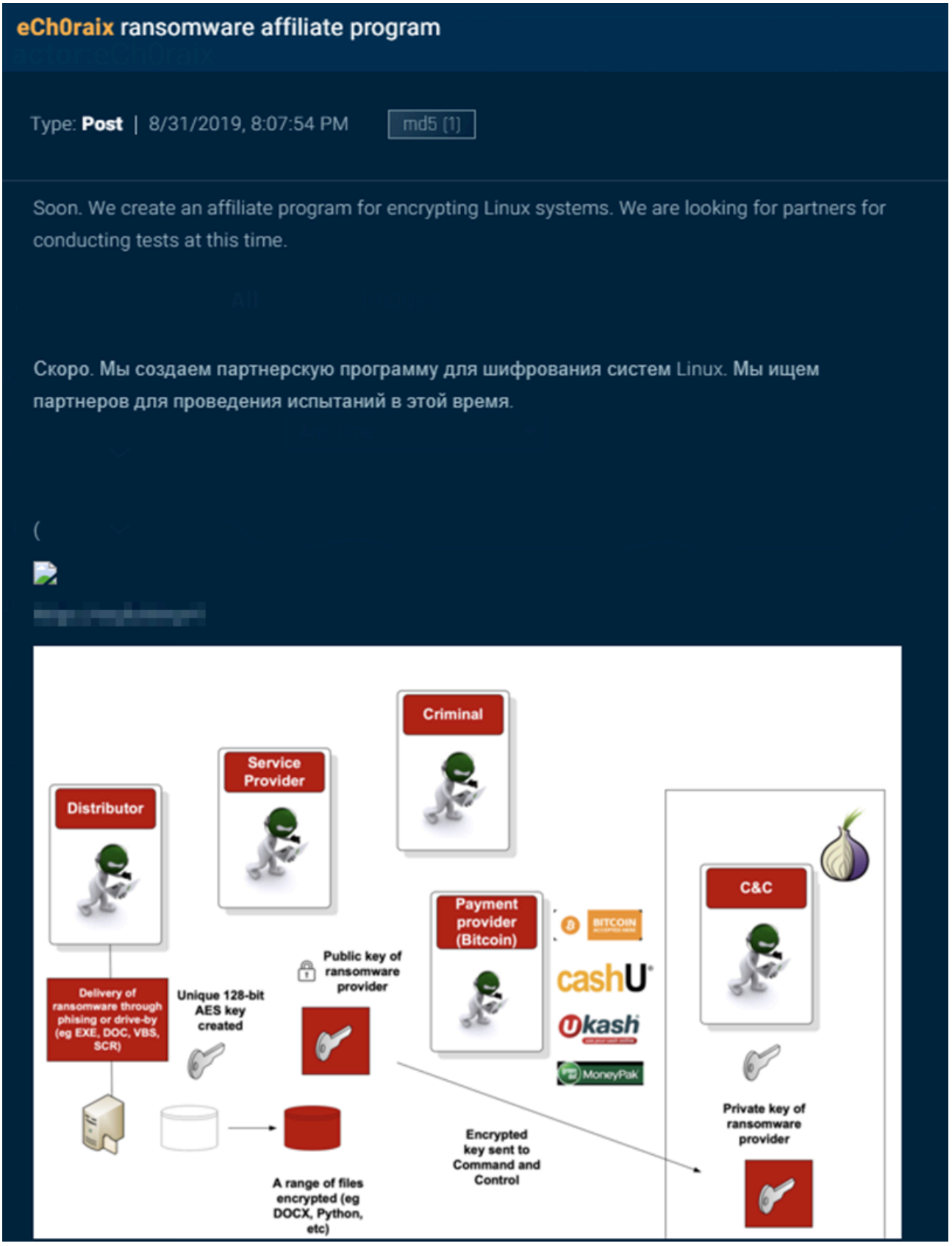


Figure 9: Announcement post made by the eCh0raix actor on the dark web.

In the post (Figure 10), eCh0raix cites research by threat researchers (from Anomali and Trend Micro), a marketing technique often used by RaaS providers in order to bolster credibility.

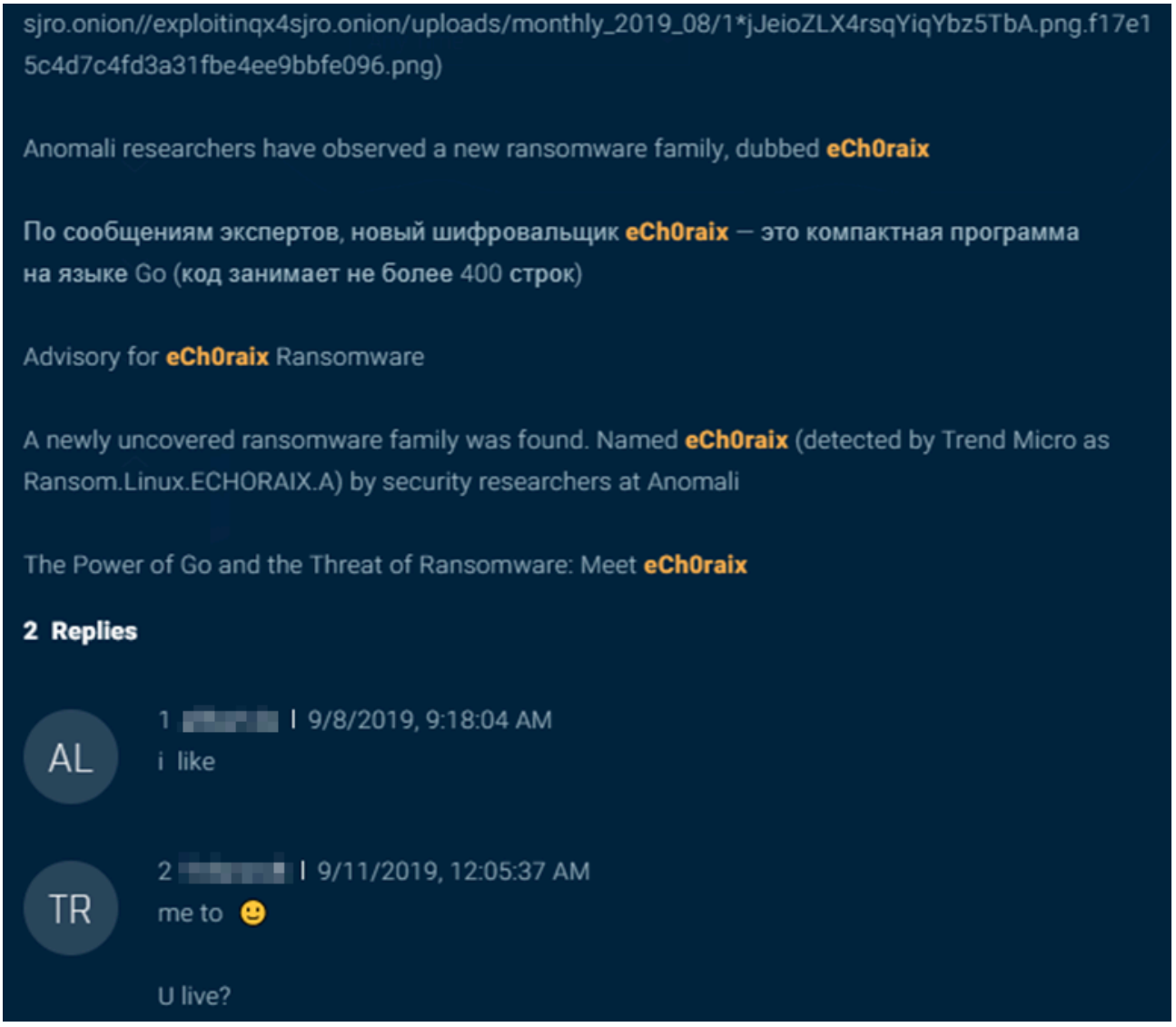


Figure 10: The threat actor referring to public research on his ransomware.

From this initial post until June 20, 2020, the actor posted 27 new threads on the forum and another 77 replies to existing threads. They were quite gregarious, jumping into threads and sharing expertise and advice. While the actor did not give any updates on eCh0raix ransomware, all of the posts concluded with a signature that included the citation from the threat researchers.

The actor's catalogue of posts dealt with a broad variety of topics. On December 25, 2019, eCh0raix offered a second service called DirBuster (Figure 11), for scanning domains, subdomains, pages, and scripts, which appears to have been rebranded as Masscan a few months later:

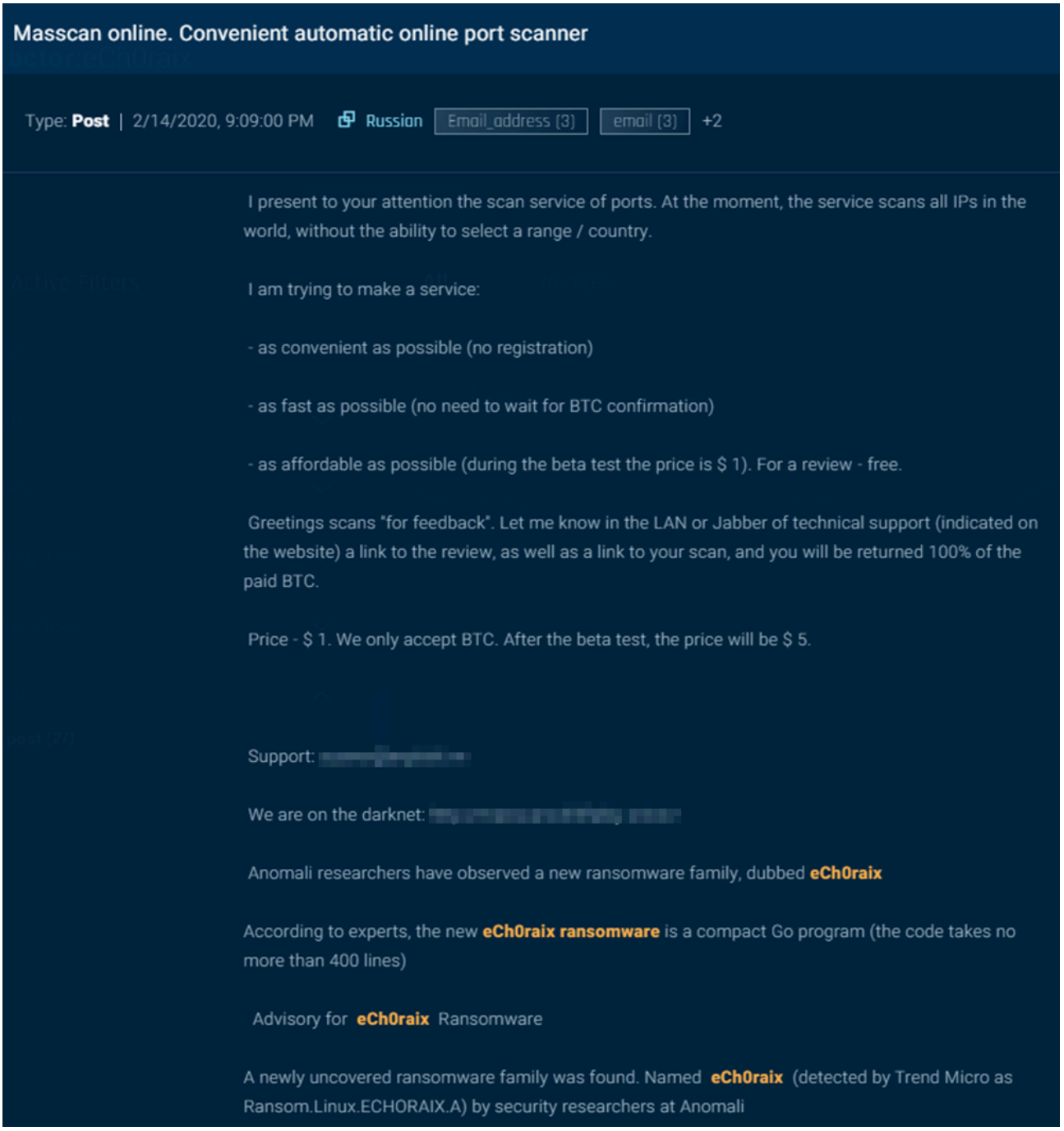


Figure 11: Forum post by the threat actor announcing port scanning service called Masscan.

The actor was also interested in virtualization, network access, and databases. They posted a lengthy account of hacking a Magento site, sold SSH root access/web shell access to a Costa Rican ad network and to an American IT company, and a database dump from a Canadian cannabis store.

In his final post (Figure 12) on the forum, the actor was looking to purchase a Shodan account from which to export IP addresses. Like every post before it, this post concluded with the same announcement of eCh0raix ransomware that had been used ten months prior.

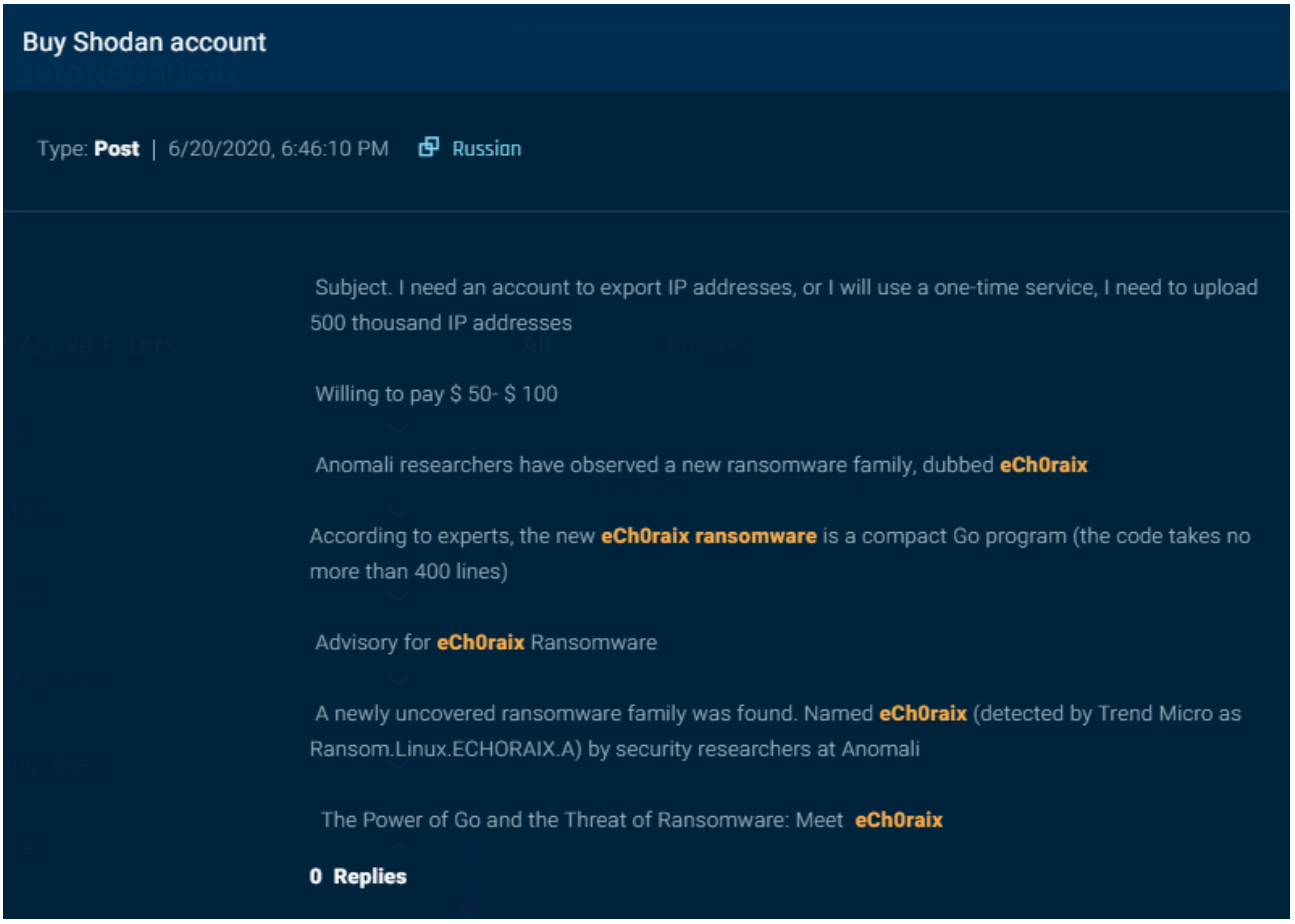


Figure 12: Final post by the threat actor.

Since this was posted on June 20, 2020, without any reason or indication the account has been inactive.

SunCrypt

On August 12, 2020, the actor behind SunCrypt posted on the same forum for the first time. In a post titled *[PARTNERSHIP PROGRAM] SunCrypt Ransomware* (Figure 13), the actor posted characteristics of the ransomware and issued a call for five affiliates to spread the ransomware. The actor noted that once the affiliate program was full, “we will go into private again.”

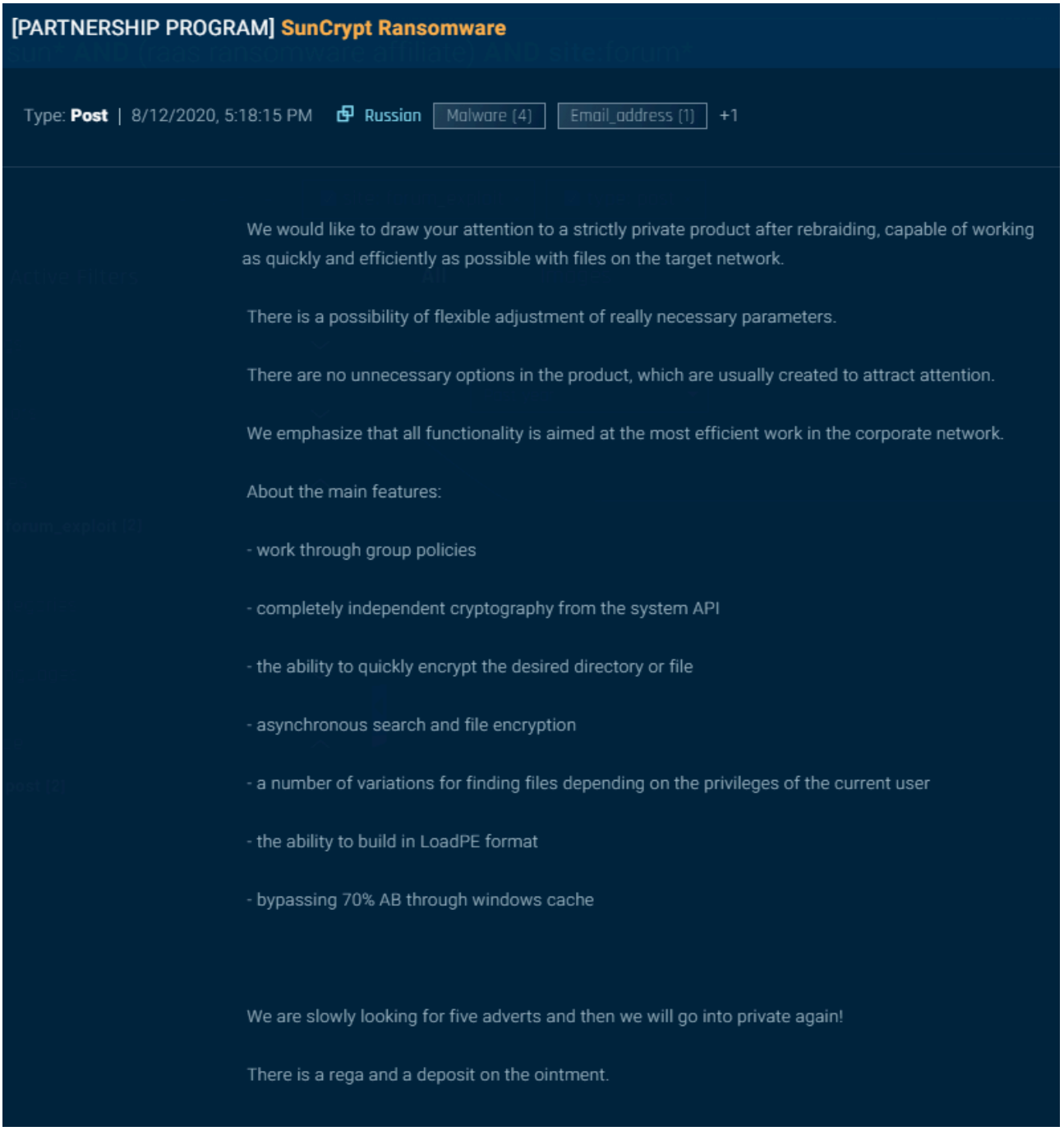


Figure 13: Forum post announcing the SunCrypt partnership program.

The actor posted 11 more times, all on this single thread and having to do with searching for affiliates or answering technical questions about the ransomware. On August 29, the actor announced that the affiliate program was full. Then on September 3, they announced that a position was vacated.

On September 19, an actor posted on the thread (Figure 14), “Even hospitals are scammed by these scum,” and cited a Bleeping Computer article about a SunCrypt attack against University Hospital New Jersey (UHNJ).

Figure 14: Another threat actor posts in the SunCrypt thread about how the ransomware has been used in attacks against hospitals.

SunCrypt wrote defensively (Figure 15), “how can I see you are the most honest here…. Mother Teresa” a stretched take on “Let he who is without attacking a hospital with ransomware cast the first stone.”

The actor continued, blaming the hospital attack on a new affiliate, who was reportedly punished, since “we don’t do hospitals, government agencies, airports, and so on.”

Figure 15: The actor behind SunCrypt response to the hospital attack allegation.

Later that day, another actor posted a lengthy technical analysis of the ransomware. The SunCrypt actor angrily responded, “Tell me, why are you posting this here?” and requested that the moderator erase the post (Figure 16).

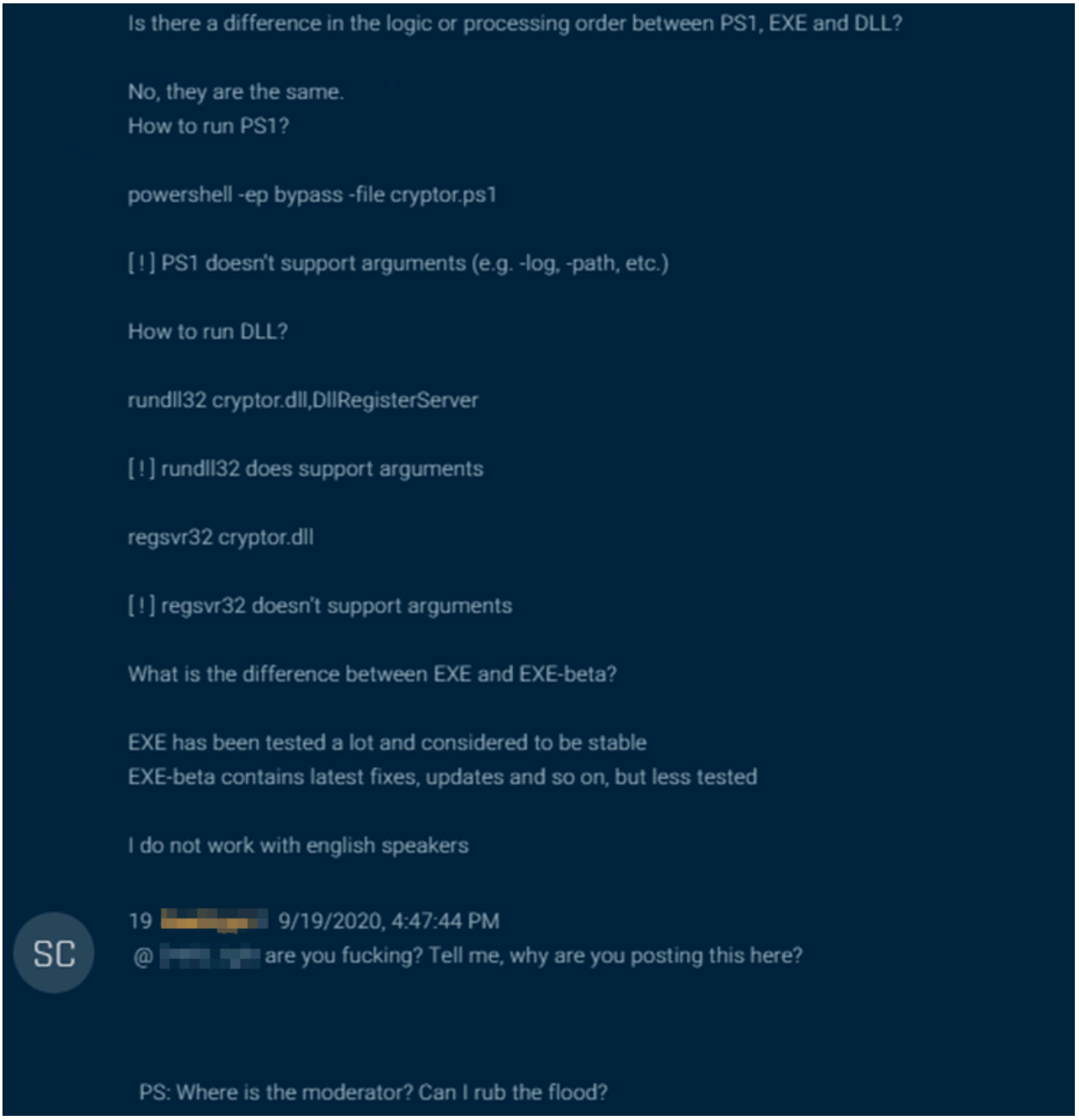


Figure 16: The threat actor's angry response to a technical analysis of the ransomware.

As of the date of this publication, the actor has not posted again. It is unclear why.

SunCrypt's dedicated leak site (DLS) soon wound down. Starting on August 1, there were 15 posts of data from targeted organizations. After September 19, there were only three more over the next 10 days. Even though new samples of SunCrypt ransomware had surfaced in VirusTotal, it appears that SunCrypt's public campaign on dark web forums and management of a DLS went dark.

It is unclear why the forum thread went silent and why the DLS site suspended operations, but the timing indicates that it was related to the hospital attack. SunCrypt's operators may have been afraid that unwanted notoriety would attract law enforcement actions or security researchers, so they decided to keep a lower profile until the attention subsided.

Suddenly, on February 16, SunCrypt's DLS listed a new victim: PRP Diagnostic Imaging. It appears that SunCrypt has returned to the business of public ransomware breaches.

It is notable that PRP provides "an extensive range of diagnostic [medical] imaging services," such as MRIs, ultrasounds, and mammograms. Thus, while attacking a hospital may have forced the actor to suspend operations for several months, SunCrypt has returned and continues to target healthcare providers. These, despite the actor's protest that "we don't do hospitals."

Comparing the Actors

Despite the code similarities between the two ransomwares, the actors behind them exhibited very different behaviors. The eCh0raix actor mentioned his ransomware in passing, but it was hardly their only focus. They launched other initiatives, shared advice, and participated in unrelated conversations in the forum.

Meanwhile, the SunCrypt actor was solely focused on a single purpose: advertising the ransomware in order to recruit affiliates. During his five weeks of activity, they were active in one thread only. SunCrypt operated a DLS site, indicating a more sophisticated operation, while eCh0raix did not.

Considering these behavioral differences, it is our assessment that the eCh0raix and SunCrypt accounts are operated by different individuals/groups. Perhaps the eCh0raix actor, overwhelmed by their many initiatives, decided that they did not have the resources to operate it and sold it to an affiliate. Maybe they were approached by a stranger asking to procure the source code. While we may never know the full story, it appears that the eCh0raix ransomware was transferred to and upgraded by the SunCrypt operators.

Conclusion

With technical analysis, it is possible to link the currently active version of SunCrypt back to QNAPCrypt, a ransomware that was used to target NAS devices back in the Summer of 2019. While the technical based evidence strongly provides a link between QNAPCrypt and the earlier version of SunCrypt, it is clear that both ransomware are operated by different individuals. Based on the available data, it is not possible to connect the activity between the two actors on the forum. This suggests that when new malware services derived from older services appear, they may not always be operated by the same people.

With this in mind, security officials should note that just because one malware family is an iteration of another, it does not mean that the new family will be deployed in exactly the same way. If a malware is exchanged, whether to an affiliate or over the dark web, then the new operators may choose different procedures, attack vectors, and targets. They might invest considerably in the new malware, adding features and evasion techniques. Defenders must remain vigilant.

Track SunCrypt, QNAPCrypt and other ransomware families in Intezer Analyze to get the latest samples detected by code reuse.
