The Curious Case of SunCrypt

By Tomas Meskauskas

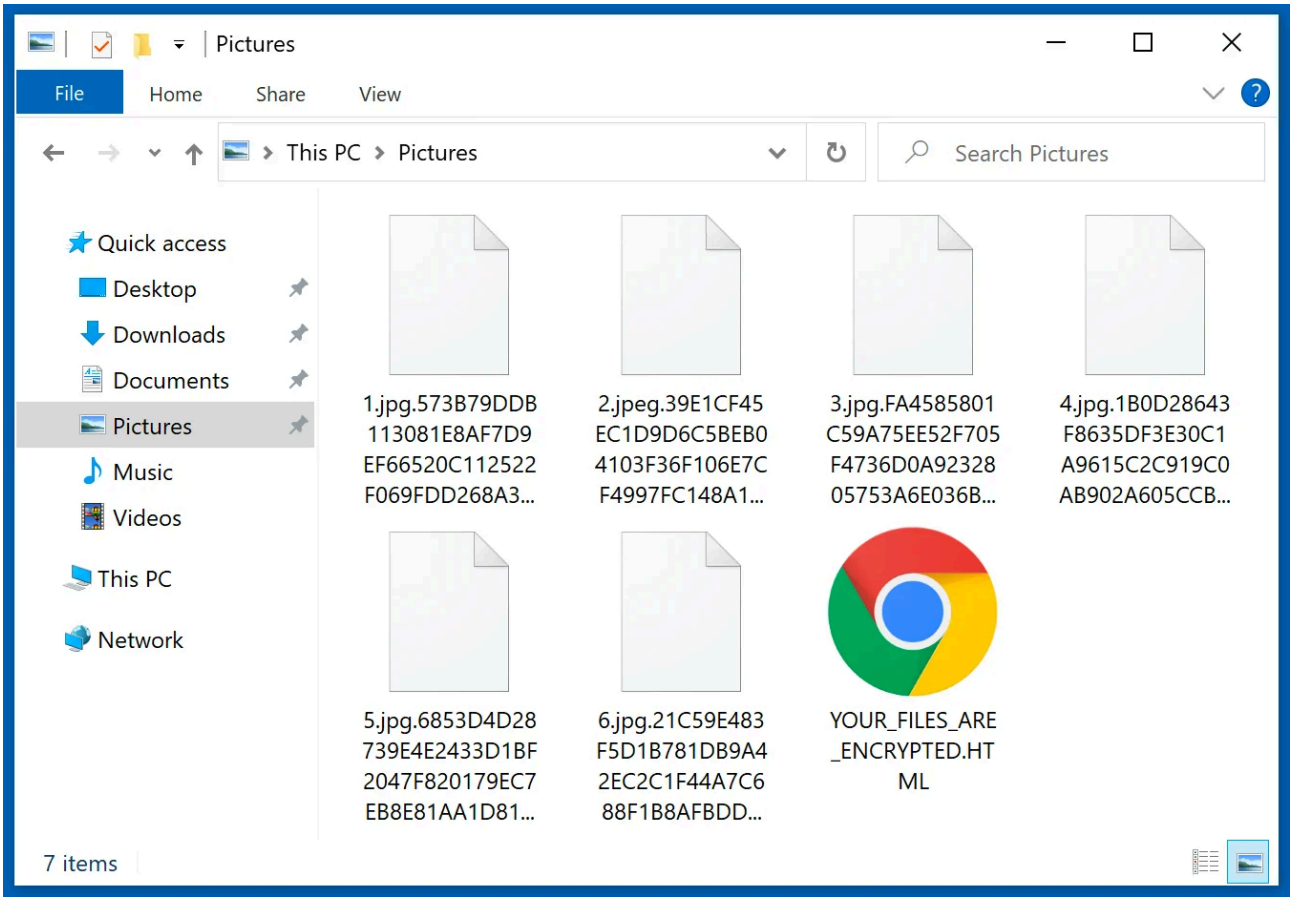
Published: 2020-09-18 · Archived: 2026-04-05 22:54:00 UTC

Toward the end of August, the gang behind the SunCrypt ransomware strain announced they had joined the Maze cartel of ransomware operators, which currently boasts Maze, LockBit and Ragnar Locker. After that announcement, reports began emerging of the first high-profile victim of the gang. However, not all is as it seems with the gang and questions have been raised as to whether they are indeed the newest members of the Maze cartel.

SunCrypt in the Spotlight

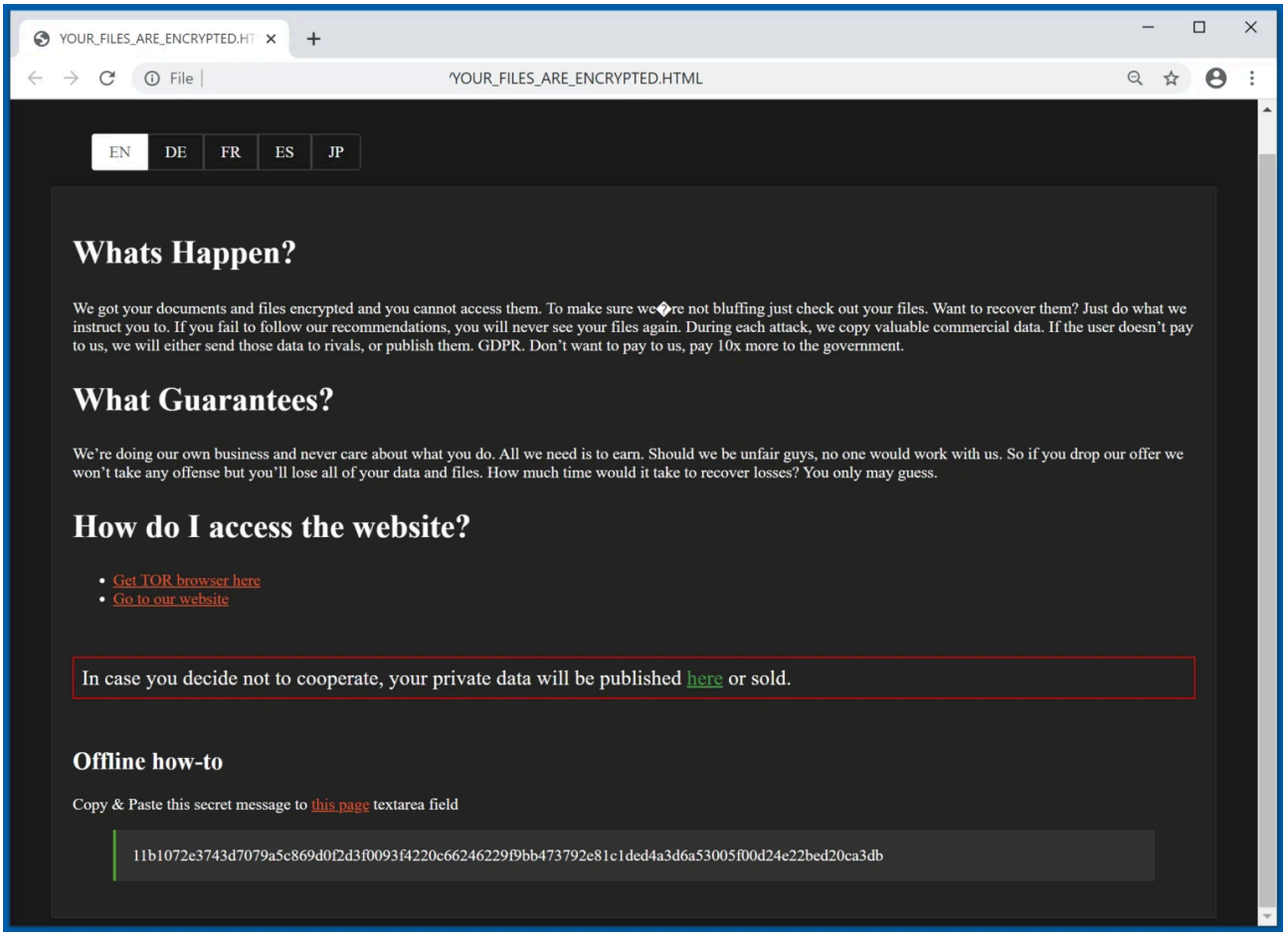
Some reports suggest that group activity of the gang, initially discovered by GrujaRS, can be traced back to October 2019. Fortunately, GrujaRS was recently able to retrieve a sample, shining a light on how the ransomware itself infects and encrypts data. The malware itself is installed from a heavily obfuscated PowerShell script and once executed it will connect to the URL http://91.218.114[.]31. Once the malware has successfully connected with the IP address it begins to send information regarding the victim's machine as well as other data. When it comes time to encrypt data, the encryption module will append a hexadecimal hash to the end of each file name, for example, the file "1.jpg" will be renamed to "1.jpg.F3F2420C68439B451670486B17EF6D1B0188A7982E7A9DBD9327E7F967C15767" once it has been encrypted.

Screenshot of SunCrypt ransomware encrypted files:



Once files are encrypted, a ransom note titled “YOUR_FILES_ARE_ENCRYPTED.HTML” will be dropped and is available in English, German, French, Spanish and Japanese. Given the wide array of languages, it would seem that the gang is not content to target one specific geographical area but has Europe, much of the Americas and Japan in its sights for future campaigns. As has been seen in many other ransomware strains the ransom note contains a TOR link to a website controlled by the attackers. This site has been hardcoded into the note, meaning that all victims will be redirected to a site that contains a chat service to negotiate the ransom amount.

Screenshot of SunCrypt ransom demanding message:



Again SunCrypt plays off the same playbook as other major ransomware families and threatens to leak information if the ransom is not paid in time. To this extent, a special leak website has also been set up to better facilitate this and is similar in approach to the other ransomware families that do the same thing, including Ako, Avaddon, Clop, Conti, CryLock, DoppelPaymer, Maze, MountLocker, Nemty, Nephilim, Netwalker, Pysa/Mespinoza, Ragnar Locker, REvil, Sekhmet, Snatch and Snake.

Distribution

Currently, the ransomware is distributed via a dynamic link library, or DLL. This is not the first nor the last ransomware family to use this method of distribution. Famously, Locky and CryptoMix have been distributed this way. A DLL, simply put, is a code library that can be used by more than one program at the same time. It was intended to allow the creation of more modular code that can be reused, thus promoting better memory efficiency. However, similar to a lot of useful features found within an OS, hackers will look to adopt new tactics to abuse these features. Ransomware strains will typically abuse the DLL protocols to download and install the main ransomware payload. The DLL is typically held within a downloader specifically designed to fetch, download and install the ransomware payload. Locky was seen adopting these tactics as early as 2016. One of the advantages this offers to hackers is it can help evade detection by behavior monitoring heuristics found on many security software packages as standard. The use of DLLs to distribute ransomware is often coupled with another layer of encryption which is also meant to make detection and prevention harder.

While this attack method has been successful in bypassing detection, it is not unpreventable. For those developing programs that use DLL downloads, it is recommended that any code that is written is secure and loads a DLL from a specific path. Further, it is also recommended that only signed DLLs are used or accessed and enabling SafeDllSearchMode to prevent attackers from exploiting the search path should be done where possible. To further protect devices, security firms advise endpoint users to "… ensure that all validated and clean applications are installed in administrator-protected directories. This step restricts write and execute permissions to user folders and implements least-privilege access."

Is SunCrypt In or Out?

As mentioned above, the first time SunCrypt made headlines was when it announced it had joined the Maze cartel. Given that it is well-known that Maze has partnered with both LockBit and Ragnar Locker, this was readily accepted as a distinct possibility by the InfoSec community. At first glance, this appeared to be true, as around the same time frame reports began to emerge that the Conti gang had also joined forces under the Maze cartel umbrella. The evidence for Conti's new partnership rests on the fact that Conti published data about two victims that were on Maze's published victim list. What's more troubling is that some researchers believe Conti may be a replacement for Ryuk, one of the big players in the ransomware game at the moment. This belief is not without grounds, as Conti shares code with Ryuk, drops the same ransom note and utilizes the same infrastructure.

Returning to the question of whether SunCrypt is a member of the group, the group itself stated that it had indeed joined the cartel and made statements to the effect that Maze could not handle all the "work" available and needed help. It can be assumed that this partnership was based on a shared revenue scheme. That being said, Maze has never elaborated on its partnerships to the press so the exact details are unknown.

It was not just the word of SunCrypt that lead researchers and journalists to believe that they had joined the cartel; the IP address mentioned above is one of several IP addresses also used by Maze and its partners. In the past, researchers have noted that the IP address used by SunCrypt has been used by Maze to transmit information during attacks. The shared use of an IP address normally indicates two things: First, the sharing of infrastructure resources and, second, the white-labeling of ransomware resources to other groups so no new attacks are hampered by unintended blacklisting.

All this presents a strong case for the belief that SunCrypt joined the cartel. Here is where things take a turn for the strange. Speaking to Bleeping Computer Maze stated, "We do not have any connections with SunCrypt, it is a lie," and, "We do not know why SunCrypt does it, but we believe it is a PR strategy, to send links to companies in chat that they are working with us as a pressure."

Since Maze's bombshell, SunCrypt stopped responding to requests for information. However, the use of the shared IP address has been confirmed by researchers and has many scratching their heads as to what the scenario is between the two ransomware gangs. More research is needed, given SunCrypt's new arrival as a ransomware threat looking to adopt all the successful tactics of its predecessors. Guessing at this point as to motives and arrangements would likely leave egg on the face of anyone making the guess.

North Carolina School District Struck by SunCrypt

Reports emerged in September that the Haywood County School district in North Carolina had suffered a ransomware incident. No information was provided regarding the ransomware used, but it appeared that the attack began Aug. 17, with the announcement made Aug. 24. The attack rendered most remote learning facilities offline; remote learning facilities becoming available again Aug. 31. Further, the attack led to a data breach. The school district announced,

> "In announcing the ransomware attack on Monday, we wanted everyone to understand a data breach was possible. We have now confirmed a data breach occurred. We are taking every possible step to eliminate any potential harm to staff, students, and affiliates. At this point, the forensic work has not determined the extent of specific data that was stolen. We ask staff, students, and parents to monitor for any suspicious activity."

It was later learned that the school district suffered an attack by the SunCrypt gang. On the gang's data publishing website 5GB of data from the Haywood incident was released due to non-payment by the school district. This is in line with the gang's tactic and the data released contains sensitive information that can be considered personally identifiable. A tactic started by Maze in late 2019 of releasing data to apply more pressure to victims has now almost become an industry standard with many new ransomware families adopting the tactic without question.

While there is little in the way of positives that can be taken from the incident, a silver lining did emerge in that researchers were able to get more information about the malware and how it was deployed. In this instance, as well as some prior, the gang created a PowerShell script named after the intended victim. When executed, the malware encrypts data and drops the ransom note. This can prove a vital bit of information when looking to identify the culprit. To launch the script on all the Windows machines on the network, the gang creates a batch file that is pushed to those machines. The batch file will then run the executable PowerShell script on all the machines it was pushed to. This allows the gang to quietly compromise the network, steal important data and quickly encrypt the Windows machines on the network in one go. The encryption process appends a hexadecimal hash to each file encrypted and drops the same note discovered earlier by researchers. As of it, there are no known weaknesses within the code or the encryption process, so file recovery with a decryption tool is not possible.

A Curious Case

SunCrypt has presented researchers with several perplexing questions, including the mysterious case of the IP address shared by both SunCrypt and Maze. Despite the curiosity the ransomware gang has created, the North Carolina School District incident proves that the gang is not to be underestimated, as they are capable of effectively targeting a network and encrypting multiple devices simultaneously. This ability combined with the gang's willingness to steal and publish sensitive data means that SunCrypt can be classified along with other human-operated ransomware strains as a real danger to organizations.

Recent Articles By Author
