SunCrypt ransomware is still alive and kicking in 2022
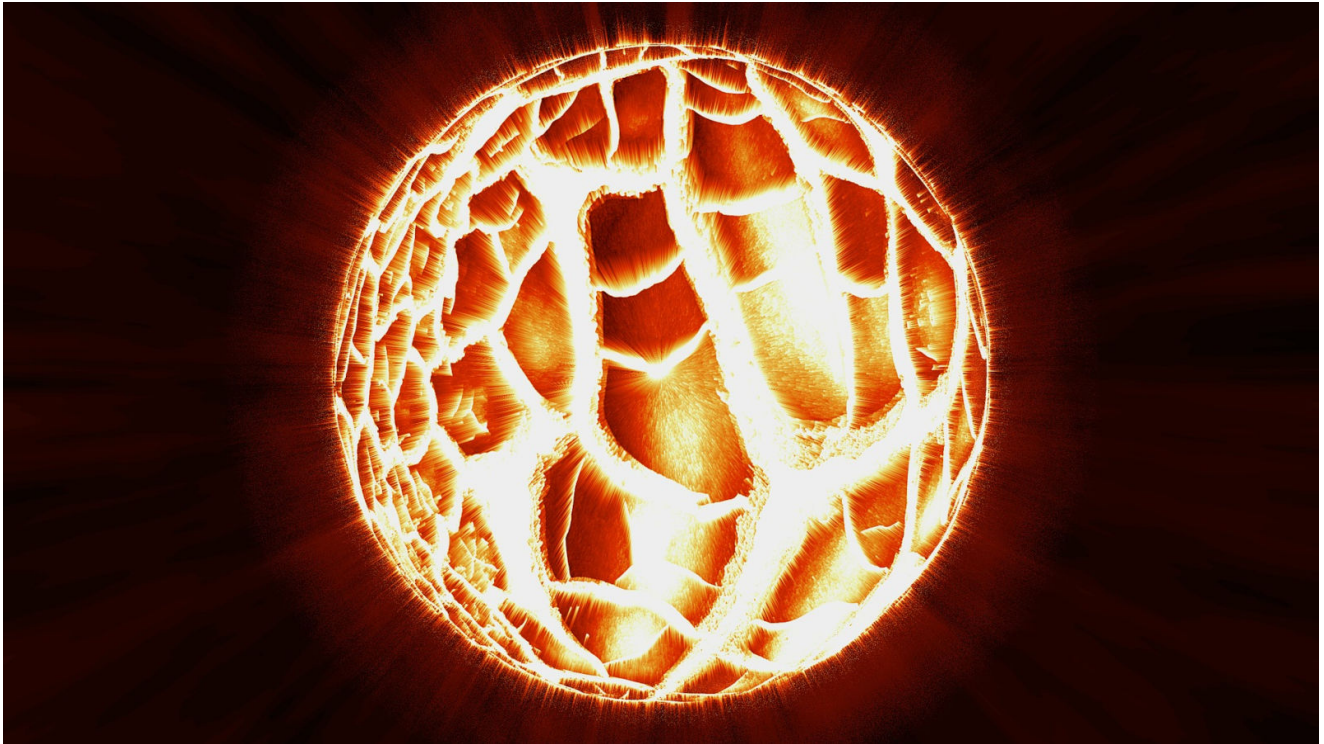
Bill Toulas
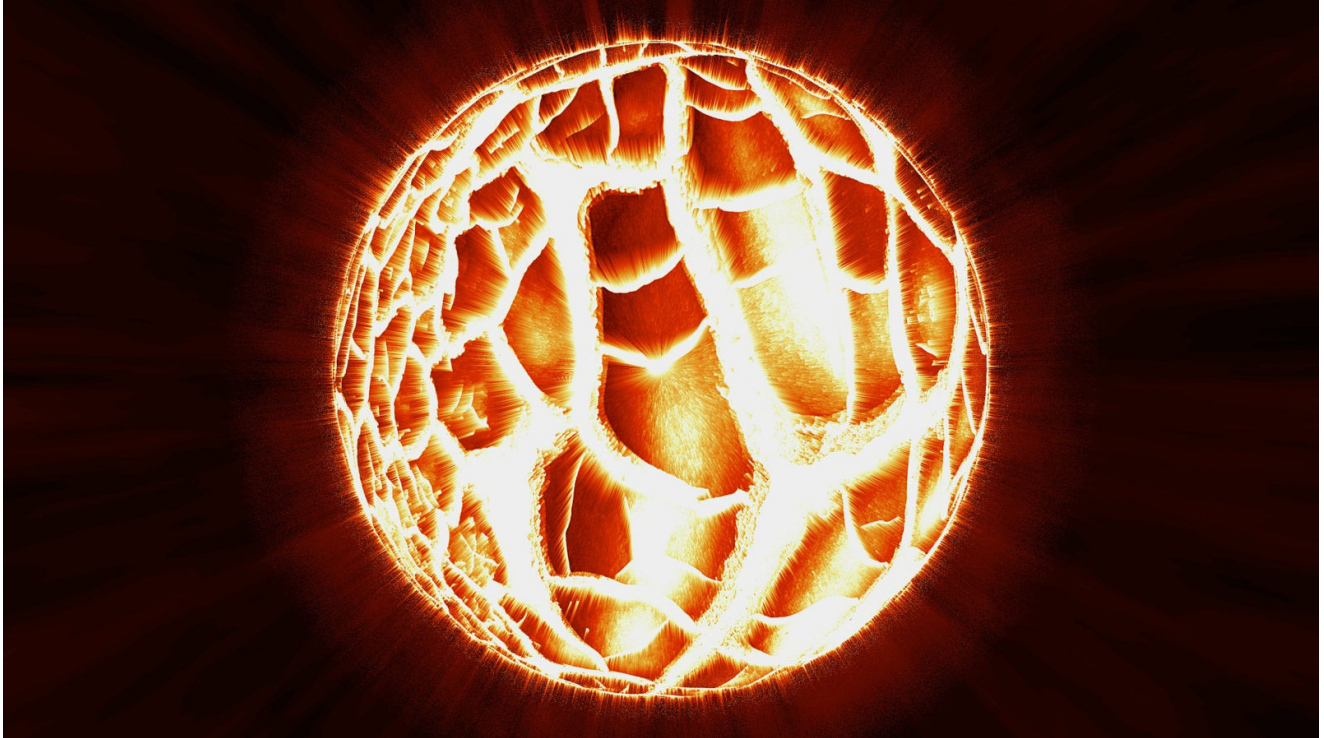
By
Bill Toulas

- March 28, 2022
- 02:35 PM
- 0

SunCrypt, a ransomware as service (RaaS) operation that reached prominence in mid-2020, is reportedly still active, even if barely, as its operators continue to work on giving its strain new capabilities.

SunCrypt was one of the early pioneers of triple extortion, including file encryption, threat to publish stolen data, and DDoS (distributed denial of service) attacks on non-paying victims.

Despite this and the lack of ethic-minded targeting restrictions within the affiliate program, SunCrypt has failed to grow larger than a small private RaaS of a closed circle of affiliates.

According to a report by Minerva Labs, this stagnation hasn't stopped the malware authors from working on a new and better version of their strain, which the analysts analyzed to determine what changed.
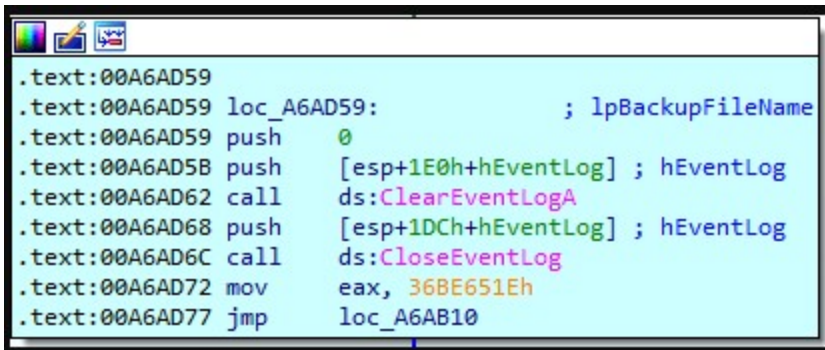
New SunCrypt features

The new capabilities of the 2022 SunCrypt variant include process termination, stopping services, and wiping the machine clean for ransomware execution.

These features have long existed on other ransomware strains, but for SunCrypt, they are very recent additions. As Minerva comments, this makes it seem like it's still in an early development phase.

The process termination includes resource-heavy processes that can block the encryption of open data files, such as WordPad (documents), SQLWriter (databases), and Outlook (emails).

The cleaning feature is activated at the end of the encryption routine, using two API calls to wipe all logs. Although one would be enough, the author probably used two for redundancy. After all the logs are erased, the ransomware deletes itself from the disk using cmd.exe.

API calls that clear the event log *(Minerva)*

One of the important <u>old features</u> retained in the newest version is the use of I/O completion ports for faster encryption through process threading.

Also, SunCrypt continues to encrypt both local volumes and network shares, and still maintains an allowlist for the Windows directory, boot.ini, dll files, the recycle bin, and other items that render a computer inoperable if they're encrypted.

If you get this message, your network was hacked!

After we gained full access to your servers, we first downloaded a large amount of sensitive data and then encrypted all the data stored on them.

That includes personal information on your clients, partners, your personnel, accounting documents, and other crucial files that are necessary for your company to work normally.

We used modern complicated algorithms, so you or any recovery service will not be able to decrypt files without our help, wasting time on these attempts instead of negotiations can be fatal for your company.

Make sure to act within 72 hours or the negotiations will be considered failed!

Inform your superior management about what's going on, invite someone who is authorized to solve financial issues to our private chat. To get there you should download and install TOR browser and follow the link below:

http://sttzxdr7uofos6f5koi644dv2xash7ope5x2yrat6fmhyvywigzc3eqd.onion/chat.html?2e1252bfd6-839caee5d3-d5d0502efe-c2a4b27b62-24dce843c8-017ebce84f-c873e9958a-f2a5b7619e

If you and us succeed the negotiations we will grant you:

- complete confidentiality, we will keep in secret any information regarding to attack, your company will act as if nothing had happened.
- comprehensive information about vulnerabilities of your network and security report.
- software and instructions to decrypt all the data that was encrypted.
- all sensitive downloaded data will be permanently deleted from our cloud storage and we will provide an erasure log.

Our options if you act like nothing's happening, refuse to make a deal or fail the negotiations:

- inform the media and independent journalists about what happened to your servers. To prove it we'll publish a chunk of private data that you should have ciphered if you care about potential breaches. Moreover, your company will inevitably take decent reputational loss which is hard to assess precisely.
- inform your clients, employees, partners by phone, e-mail, sms and social networks that you haven't prevent their data leakage.

Latest ransom note used by SunCrypt *(Minerva)*

Activity and outlook

According to stats from submissions to ID Ransomware, which provides a good idea of ransomware strain activity, SunCrypt is still encrypting victims but appears to have limited activity.

SunCrypt submissions on ID Ransomware

The group may be targeting high-value entities and keeping the ransom payment negotiations private, not drawing law enforcement attention and media coverage.

Minerva mentions Migros as one of SunCrypt's recent victims, which Switzerland's largest supermarket chain employing over 100,000 people.

In summary, SunCrypt is undoubtedly a real threat that hasn't been cracked yet, but whether or not the RaaS will grow into something more significant remains to be seen.

Related Articles:

Clop ransomware gang is back, hits 21 victims in a single month

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New 'Cheers' Linux ransomware targets VMware ESXi servers

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.