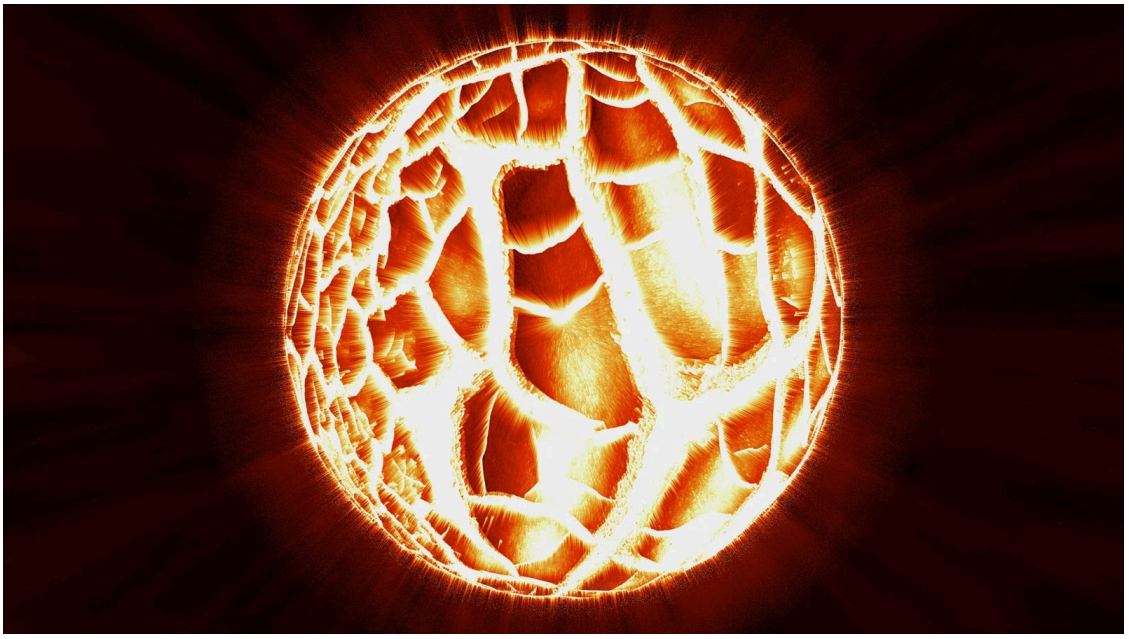
SunCrypt ransomware is still alive and kicking in 2022

By Bill Toulas

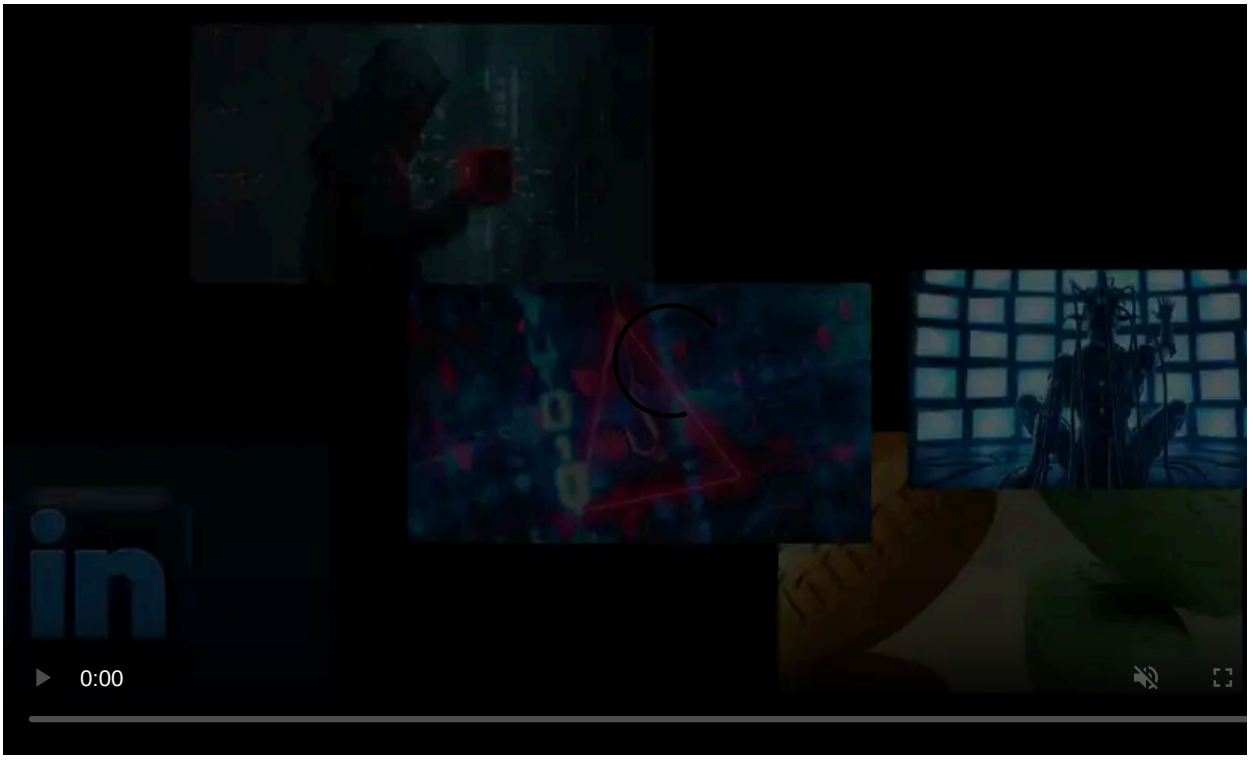
Published: 2022-03-28 · Archived: 2026-04-05 18:03:40 UTC

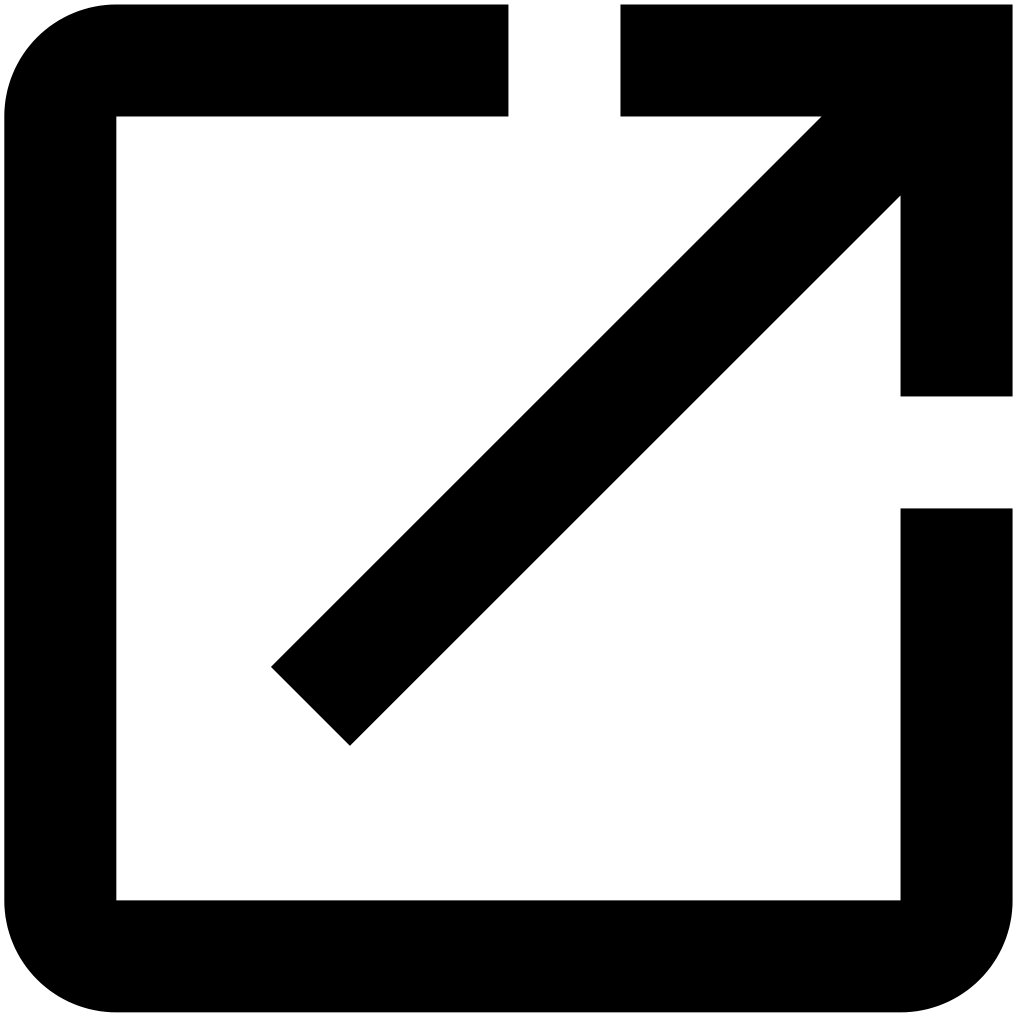


SunCrypt, a ransomware as service (RaaS) operation that reached prominence in mid-2020, is reportedly still active, even if barely, as its operators continue to work on giving its strain new capabilities.

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.


0:00



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.

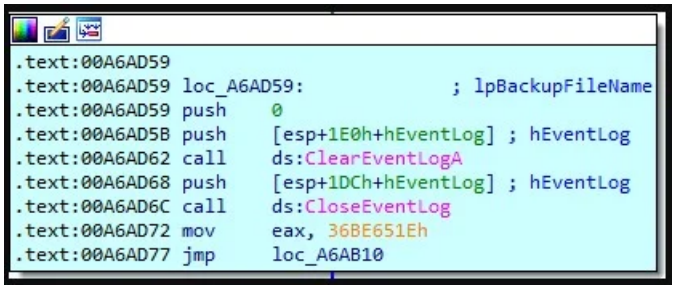
New SunCrypt features

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).

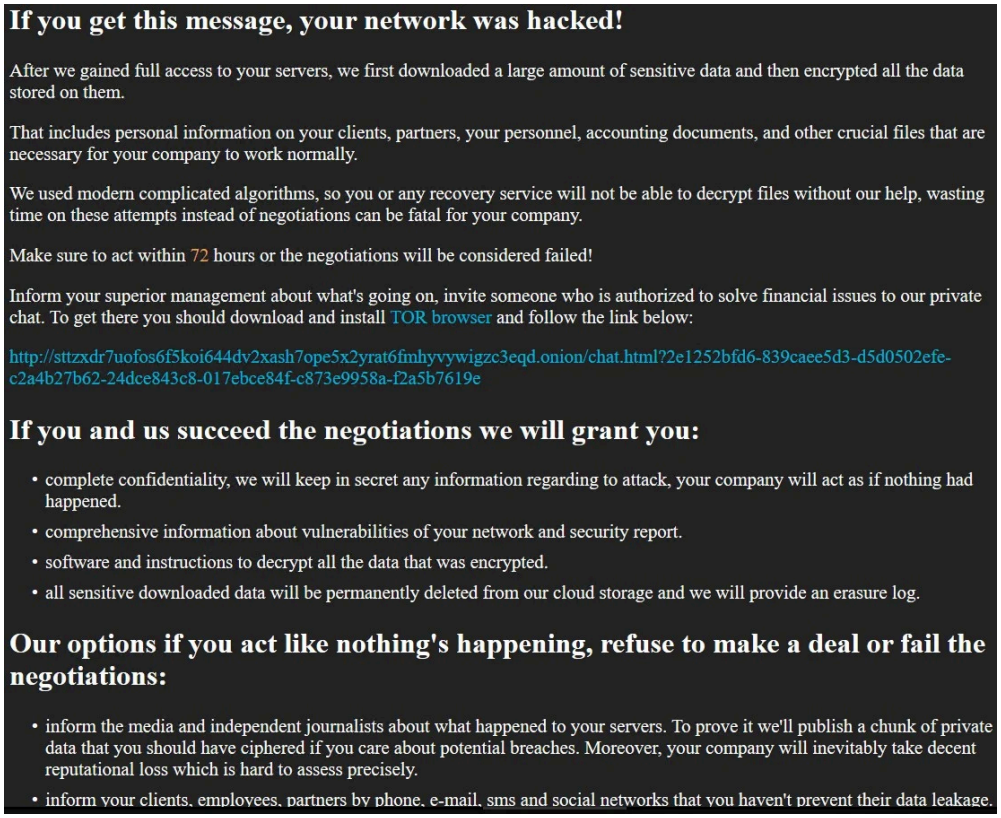
The cleaning feature is activated at the end of the encryption routine, using two API calls to wipe all logs. Although one would be enough, the author probably used two for redundancy. After all the logs are erased, the ransomware deletes itself from the disk using cmd.exe.



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

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

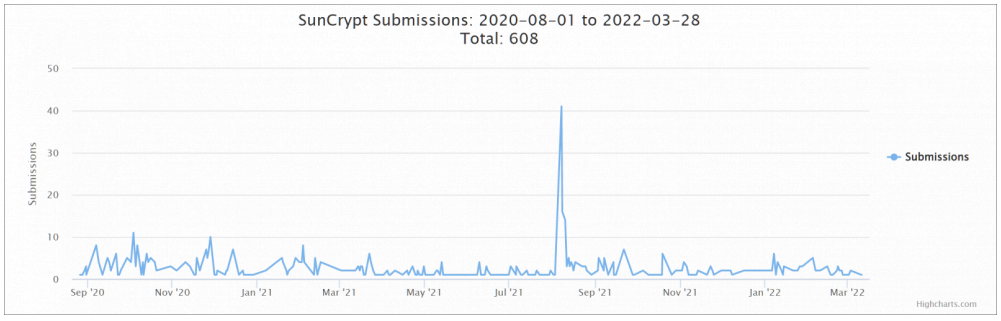
Also, SunCrypt continues to encrypt both local volumes and network shares, and still maintains an allowlist for the Windows directory, boot.ini, dll files, the recycle bin, and other items that render a computer inoperable if they're encrypted.



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.

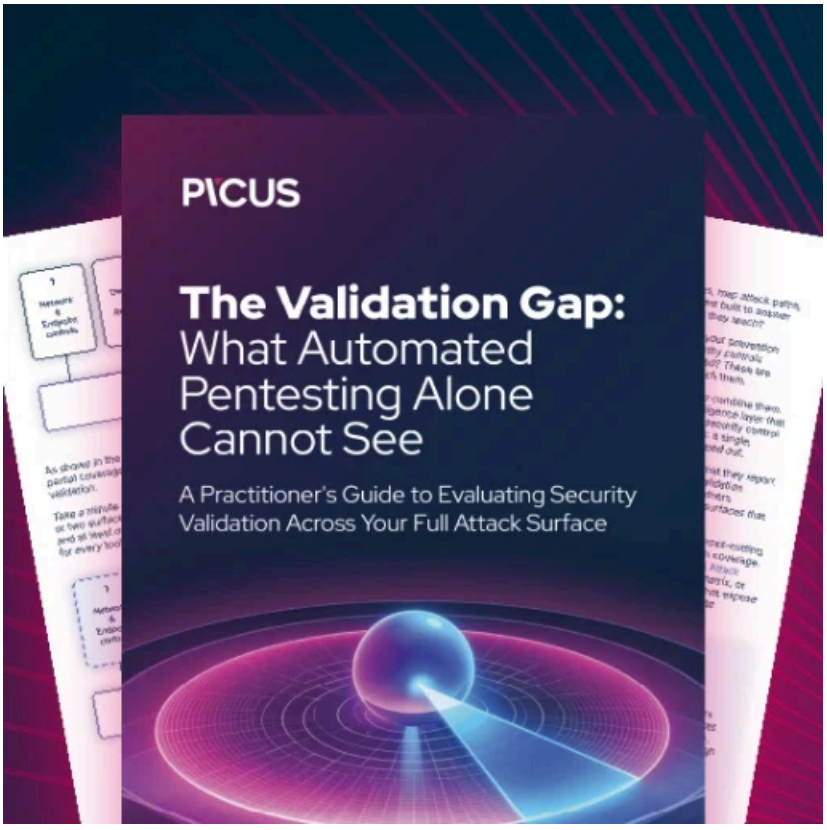


SunCrypt submissions on ID Ransomware

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.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-is-still-alive-and-kicking-in-2022/