

















# SynAck ransomware gang releases decryption keys for old victims

By Catalin Cimpanu

Published: 2022-12-13 · Archived: 2026-04-06 01:08:30 UTC

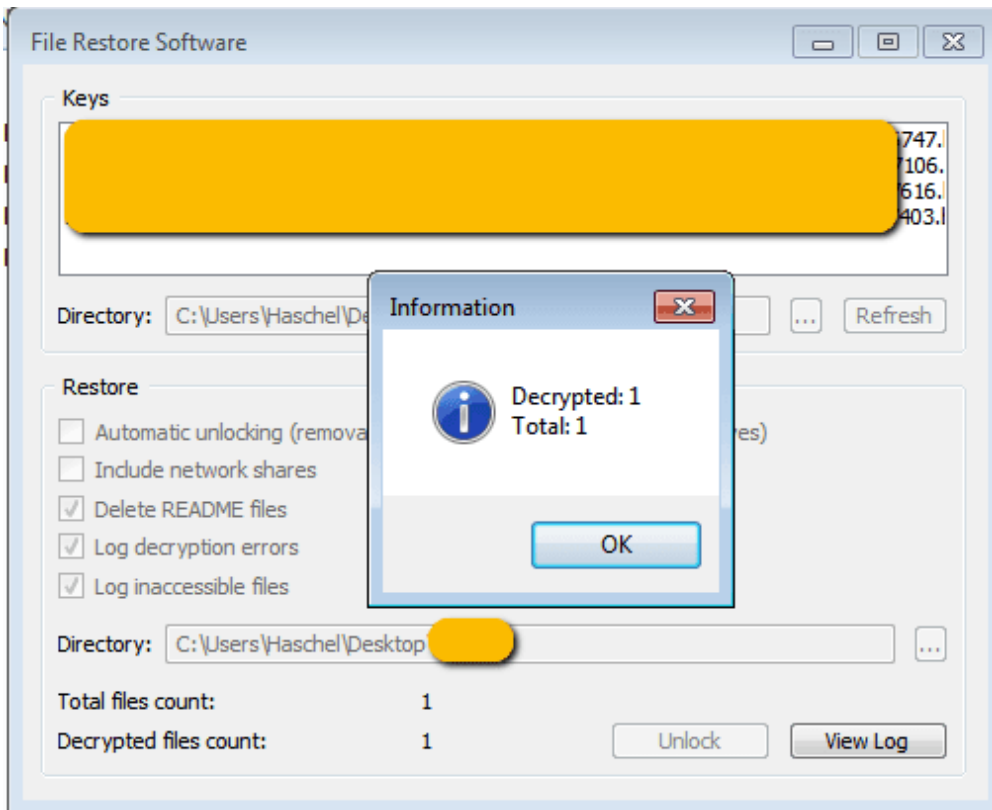
**EXCLUSIVE – The El\_Cometa ransomware gang, formerly known as SynAck, has released today master decryption keys for the victims they infected between July 2017 and early 2021.**

The leaked keys were provided to *The Record* earlier today by an individual who identified themselves as a member of the former SynAck group.

Name	Date modified	Type	Size
▼ Today (16)			
 Manager_x64.exe	13-Aug-21 02:17	Application	75 KB
 Manager_x86.exe	13-Aug-21 02:17	Application	0 KB
 Unlocker_x64.exe	13-Aug-21 02:17	Application	71 KB
 Unlocker_x86.exe	13-Aug-21 02:15	Application	0 KB
 manager_manual.md	13-Aug-21 02:15	MD File	3 KB
 rsa-api-master-1573830815-prv.key	13-Aug-21 02:15	KEY File	2 KB
 rsa-master-0xff003-1570458303-prv.key	13-Aug-21 02:15	KEY File	2 KB
 rsa-master-1550530168-prv.key	13-Aug-21 02:15	KEY File	2 KB
 rsa-master-1564612826-prv.key	13-Aug-21 02:15	KEY File	2 KB
 rsa-master-prv-1548273983.key	13-Aug-21 02:14	KEY File	1 KB
 rsa-master-prv-1549502872.key	13-Aug-21 02:14	KEY File	1 KB
 rsa_OLD-master-prv-1499552138.key	13-Aug-21 02:14	KEY File	1 KB
 rsa_OLD-master-prv-1525990921.key	13-Aug-21 02:14	KEY File	1 KB
 rsa_master-prv-1541701842.key	13-Aug-21 02:14	KEY File	1 KB
 rsa_private.key	13-Aug-21 02:14	KEY File	2 KB
 unlocker_manual.md	13-Aug-21 02:14	MD File	2 KB

The keys have been verified as authentic by [Michael Gillespie](#), a malware analyst at security firm Emsisoft and the creator of the ID-Ransomware service.

Gillespie told *The Record* he was able to use the leaked decryption utilities and private keys to decrypt files from old SynAck attacks.



*The Record* will not be making these keys generally available as the decryption process can be somewhat complicated for non-technical users, and former SynAck victims who may try to decrypt older data might end up damaging files even further.

Instead, Gillespie said that Emsisoft would be developing its own decryption utility that will be safer and easier to use, which they will be releasing within the next few days.

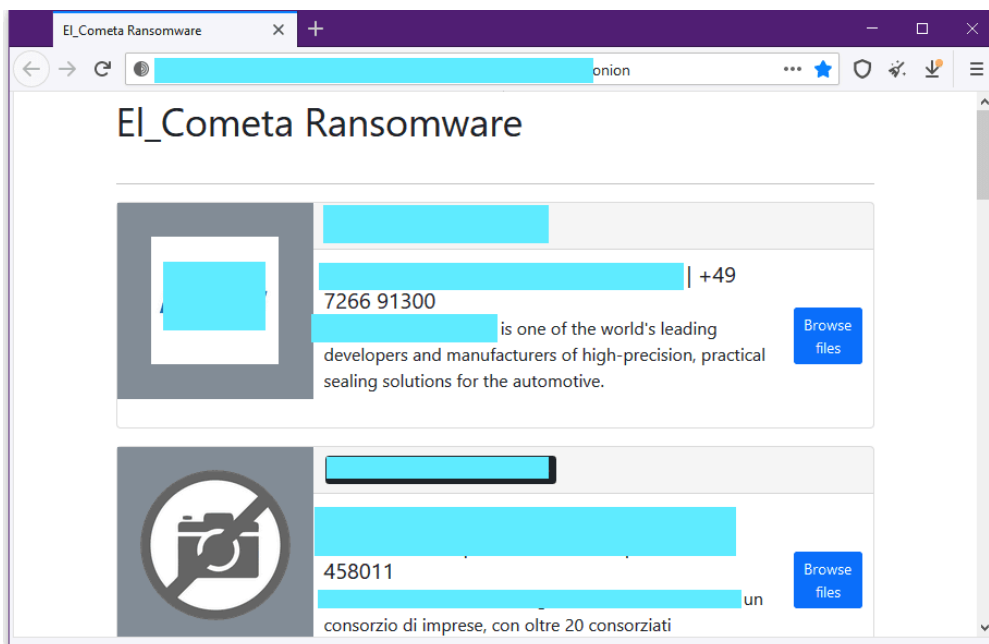
### **Private keys released as group prepares to launch new RaaS**

First spotted in [July 2017](#), the SynAck gang is one of today's oldest ransomware groups still in operation.

While the group had a strong start with somewhat large distribution campaigns, the group also turned heads at the time because of some clever work on its encryption routines and the use of the process doppelganging to evade antivirus detection, [the first ransomware strain to do so](#).

However, as time passed, other ransomware operations grew larger. While the SynAck group continued to infect victims, its statistics were not in the same category as attacks carried out by larger operations like REvil, Netwalker, Ryuk, or BitPaymer.

In an interview today, the SynAck group said they've decided to release master decryption keys for old victims as they've now wound down the old SynAck operation and are focusing on a new one, [which they launched last month and named El Cometa](#).



In addition, the group said that while they previously worked with only two outside "partners" on distributing SynAck, they now plan to considerably increase their operational model.

This will be done by launching a new Ransomware-as-a-Service (RaaS) platform, through which they plan to recruit more partners (also known as "affiliates") to carry out attacks and infect victims with the new El\_Cometa strain.

SynAck now becomes the second ransomware group that released its decryption keys this summer after the Avaddon operation released theirs in June [before shutting down](#).

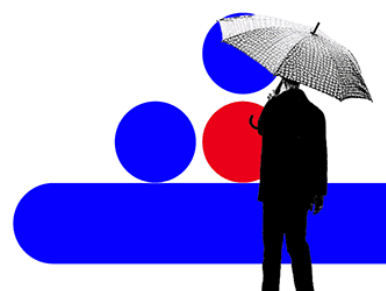
Update on August 20: Emsisoft has released a decrypter for the SynAck ransomware, which is available for download [here](#).

 Recorded Future®

Know what matters.

Act first.

Get started





[Catalin Cimpanu](#)

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

---

Source: <https://therecord.media/synack-ransomware-gang-releases-decryption-keys-for-old-victims/>