Vice Society spreads its own ransomware

intrinsec.com/vice-society-spreads-its-own-ransomware/

Equipe CTI 14 février 2023

Vice Society is a financially motivated organization encompassing operators and opportunistic intrusion sets known for intrusion, exfiltration and extorsion against a large sample of victims since June 2021. The operator(s) of these alleged intrusion sets offer(s) an active infrastructure as new victims are constantly added to the anonymized dedicated leak site where data of the victims is exposed.

The actors affiliated with Vice Society leverage not only custom Vice Society branded variants but also several ransomware-as-a-service payloads (BlackCat) as well as purchased malware (Zeppelin) for conducting attack campaigns. Sometimes, affiliates do not or cannot encrypt data, thus resorting only to the exposure of exfiltrated data for getting the ransom paid. The overall TTPs are close to those usually encountered by Russian-speaking extorsion groups making headlines in recent years.

We hereby provide threat intel on a variant of a Vice Society locker specimen, dubbed PolyVice by SentinelOne. Slight overall changes were recently observed in terms of file extension and email contact which substantiates that Vice Society affiliates use customizable builders.

Continue reading


INTRINSEC
Innovative by design
Vice Society
CYBER THREAT INTELLIGENCE
Vice Society spreads its own ransomware
TLP: CLEAR
February 2023
Website
www.intrinsec.com
Blog
www.intrinsec.com/blog
Twitter
@Intrinsec