Introducing The Most Profitable Ransomware REvil

By Cyber Threat Intelligence

Published: 2021-06-02 · Archived: 2026-04-05 17:55:00 UTC

In March 2021, another REvil's attack was announced. Targeting the computer giant Acer, the actors behind the ransomware asked for 50 million dollars, the highest ransom they have demanded so far. Acer was not the only victim of the notorious ransomware. Debuted in April 2019, REvil has attacked hundreds of high-profile agencies in multiple sectors. In 2020, REvil has earned more than 100 million.[1] In this report, we will introduce the basic profile of REvil and share the techniques they used in operations.

What is REvil

REvil, a.k.a Sodinokibi, is a Ransomware as a Service (RaaS) operation deployed by a Russian cybercrime group named GOLD SOUTHFIELD or Pinchy Spider. The group is believed to be based in Russia, as it does not attack organizations in Post-Soviet States, and refuse to cooperate with English speaking cyber criminals.[2]

REvil was highly possible the successor of GandCrab, another notorious ransomware, because of code similarities and REvil's active operations right after GandCrab's retirement.[3]

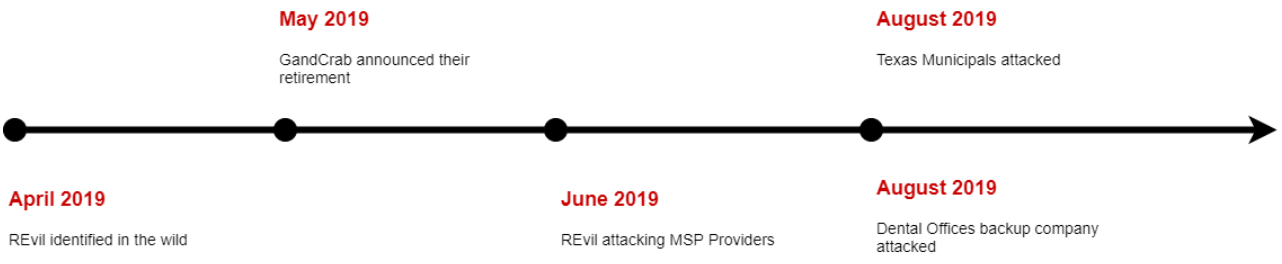


Figure 1: The timeline of REvil's appearance and GandCrab's retirement

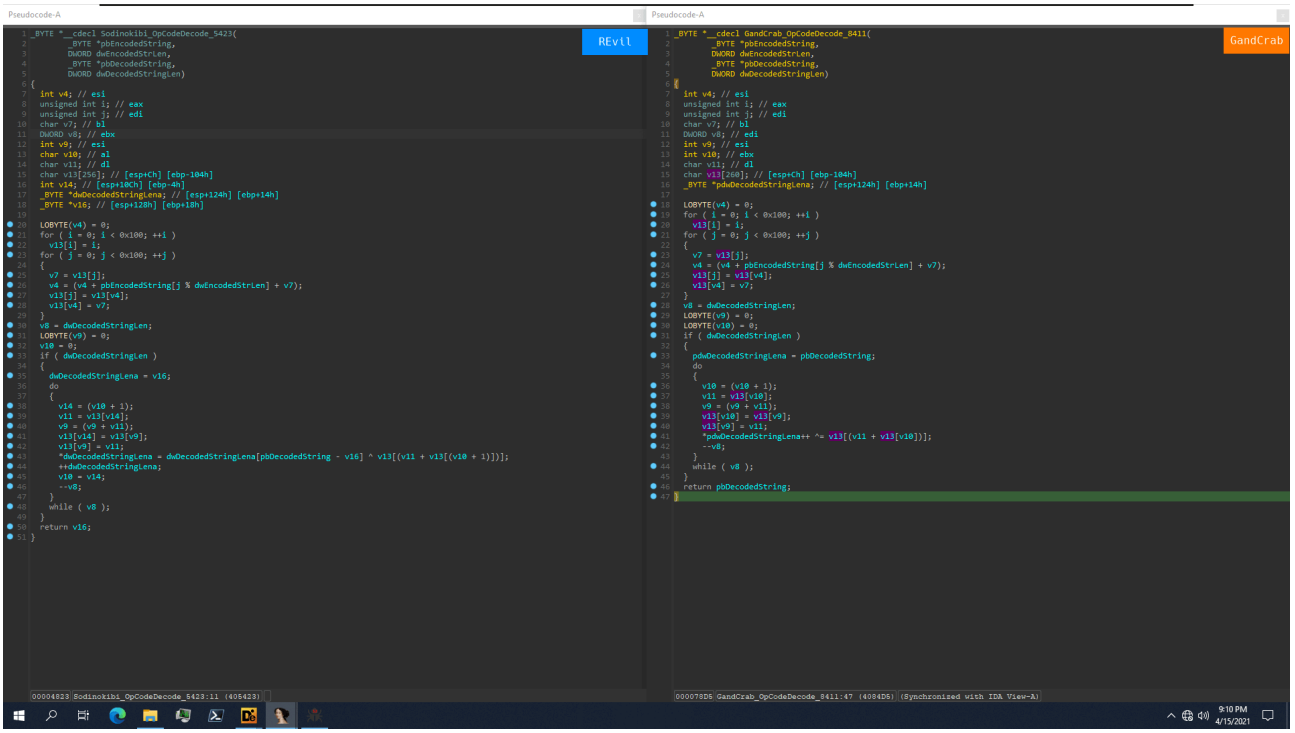


Figure 2: REvil and GandCrab's similarity on string decoding

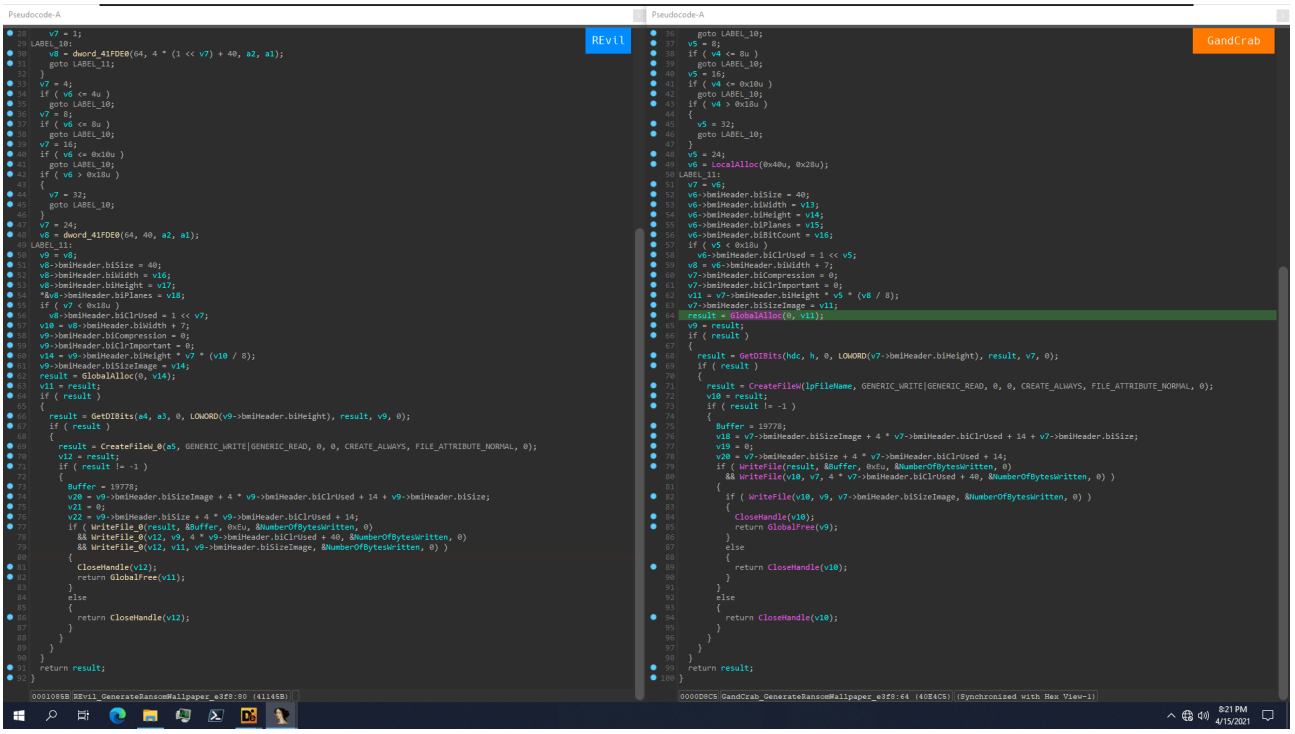


Figure 3: REvil and GandCrab's similarity on building ransom wallpaper

Numerous campaigns attacking multiple sectors were observed all over the world. The REvil actors has attacked local governments, giant law firms, multinational retailers, etc. The highest ransom they have asked was 42 million for the law firm but was now surpassed by the 50 million Acer attack. (References for the events, please see the end of this page.[4])

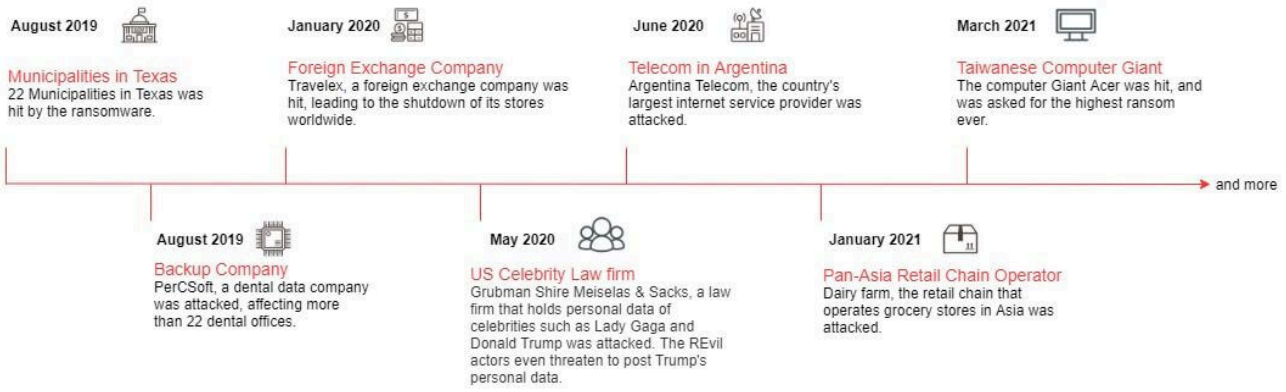
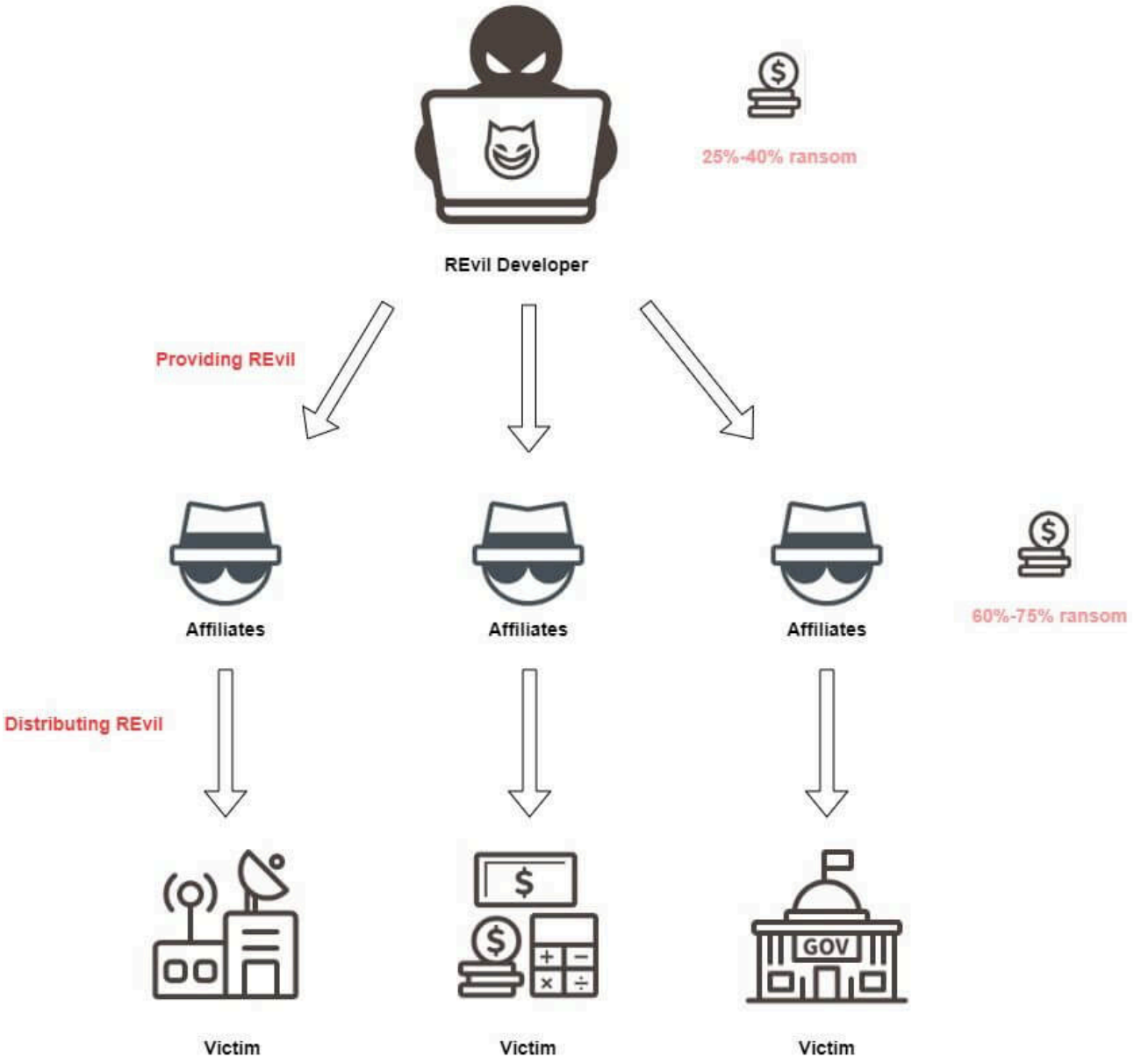


Figure 4: The timeline of REvil's notorious attacks

The Ransomware as a Service model (RaaS)

The actors of REvil adopt the Ransomware as a Service business model. In this model, Ransomware developers are responsible for development and maintenance of the ransomware, while the groups of cyber criminals, named affiliates in this model, are responsible for accessing victims' system to distribute the ransomware. The business model allows cyber criminals who are not capable of developing their own ransomware to buy the service on dark web and deploy ransomware attack.

Through this model, REvil actors provide REvil or the customized version of REvil to their affiliates. After they successfully breached victims' systems, REvil actors will ask for ransom by themselves, providing the ransom payment link. After the collection of money, their affiliates will receive 60% to 75% of the profit. Moreover, the actors also provide other paid services, such as money laundering assistance for the affiliates.



Tactic, Techniques and Procedures

Initial Access

For REvil, different affiliates may use different methods for initial access. The ransomware is now distributed primarily through compromised RDP sessions (65%), phishing (16%), and software vulnerabilities (8%).[5] However, a supply chain attack distributing REvil was also observed.

REvils' actors said in an interview that they used brute force attacks to compromise RDP sessions.[1] As for phishing emails, the cyber criminals have once disguised their email as a new booking from "booking.com". They also exploit vulnerabilities. In fact, REvil's debut was exploiting the Oracle Weblogic vulnerability, CVE-2019-

2725. Moreover, the actors are able to deploy new vulnerabilities after its disclosure. For example, the group used the recent disclosed Microsoft Exchange server vulnerability to access Acer's system.

The most astounding technique they deployed is supply chain attack. Around June 2019, a WINRAR distributor site in Italy was hacked.[6][7] The software downloaded from the site at that time was not the WINRAR installer but the REvil installer. Although no public announcements showing that any company was infected in this attack, the successful replacement shows that their affiliates were able to deploy a supply chain attack.

Apart from their various method on initial access, the cyber criminals also adopted several unique techniques. For example, REvil used Elliptic-curve Diffie-Hellman key exchange to encrypt files, while other ransomware often used RSA, Salsa20 or AES to do so. This method is more efficient as it used shorter key and is difficult to decrypt.

The Effective Methods for Ransom Collection

Nowadays, as ransomware attacks become a serious problem, most companies have learned to back up crucial data in case they are hit by a ransomware. However, ransomware actors develop several new methods to ensure that the victims will pay the ransom, including Double-extortion, VoIP calling, and DDoS attack.

- "Double-extortion"
  The actors disclose or sell the data of the company if the company is not willing to pay ransom. This method was first introduced by Maze, another notorious ransomware, and currently almost all ransomware actors have adopted this method, and so as REvil. Starting from January 2020, the group runs their own site "Happy Blog", where they post data extorted from their victims.

- Voice over Internet Protocol (VoIP) calling
  In February 2021, they announced that they are now offering Voice over Internet Protocol (VoIP) calling and DDoS attack service for their affiliates to make pressure on their victims.[8] They stated that they will call the media or their victims' business partners, telling them about the attack.

Detect and Defense

For prevention, it is always crucial to be aware of spamming emails. Nowadays, spamming emails is still the most popular and effective method to access victims' computers.

In addition, keep an eye on new exploits and updates is also important. Ransomware groups usually are not capable of discovering 0-day exploits by themselves, but they will exploit the disclosed vulnerabilities and attack those who have not updated their system. Thus, keep computers updated and patched systems immediately after the disclosure is essential for preventing ransomware attack.

Furthermore, as the REvil business grows, the actors behind has posted on dark web to recruit more affiliates for their operations. Thus, more attacks from the group is expected. TeamT5 will keep following the ransomware and provide up-to-date information of the notorious ransomware.

To efficiently prevent ransomware attacks, TeamT5 offers a total solution for enterprise protection. Our unique ransomware containment technology is proven to successfully block many types of ransomware, which can detect and stop malicious ransomware immediately. And even restore encrypted files from the backup.

For more information about TeamT5 Ransomware Prevention total solution, please contact: sales@teamt5.org

References
