# Alleged REvil member spills details on group's ransomware operations

intel471.com/blog/revil-ransomware-interview-russian-osint-100-million

An alleged member of one of the most notorious ransomware gangs in the world divulged numerous details about its operation, including that it allegedly takes in more than $100 million per year from its attacks.

The figure was revealed during an interview with an alleged representative of the REvil group that was released on Oct. 23, 2020. The interview, conducted by a Russian cybersecurity researcher and posted on the YouTube channel RussianOSINT, covered the group's prior attacks, how it splits its profits, and various tactics, techniques and procedures (TTPs) the group uses to conduct its attacks.

REvil has been one of the most active ransomware gangs in recent memory, claiming responsibility for such attacks as those on U.K.-based financial service provider Travelex, U.S.-based entertainment and media law firm Grubman Shire Meiselas & Sacks and 23 local governments in Texas.

The representative interviewed told host Sergey RedHunt that the malware was created from the source code of a separate, defunct ransomware-as-a-service (RaaS) where core REvil members previously were affiliates. When that RaaS variant was shut down, the actors behind REvil purchased the source code and developed their own ransomware. He also claimed that REvil has 10 developers that keep it running.

While the group carries out attacks on its own, it has found the RaaS model brings back more money. Affiliates are responsible for gaining access to target networks, downloading valuable files and deploying the actual ransomware, while the REvil gang handles victim negotiations and blackmailing, ransom collection and distribution. This model has apparently led to skyrocketing profits: according to the REvil representative, one affiliate's earnings rose from about US $20,000 to US $30,000 per target with another RaaS offering to about US $7 million to $8 million per target in only six months after joining forces with REvil.

One of the most common ways the group gains access to organizations is through remote desktop protocol (RDP) vulnerabilities, such as the BlueGate vulnerability, which allows remote code execution by an authorized user. The representative admittedly preferred to use information stealers to obtain remote access credentials, which are then used to secure an initial foothold in company networks. In the case of the Travelex and Grubman Shire

Meiselas & Sacks attacks, the representative said networks were compromised by exploiting outdated Citrix and Pulse Secure remote access software, with the actors allegedly gaining access to an entire network in "about three minutes."

The representative claimed that most desirable targets for attacks were agriculture companies, insurance companies, internet service providers, law firms and manufacturers. He also claimed that most victims pay the ransom to avoid having their data dumped online rather than just to decrypt the files. According to the representative, there were only 12 cases when the gang could not decrypt files, due to them being corrupted by victims looking to recover them by using third-party or antivirus software. The REvil team allegedly did not take ransom payments in these cases.

REvil has also allegedly taken precautions against attempts by cybersecurity researchers or law enforcement to infiltrate the group or take down its infrastructure. The gang has introduced additional protection measures and vetted new affiliates by asking general political and social questions related to former Commonwealth of Independent States (CIS) countries that only native Russian speakers typically could answer. Russian-speaking infiltrators usually were vetted by asking specific technical questions about attack techniques. The gang is also aware that cybersecurity experts and vendors often tried to penetrate the group's resources, allegedly identifying attempts to exploit cross-site scripting (XSS) vulnerabilities. All the attacks allegedly were unsuccessful.

The interview supports a number of trends Intel 471 has been tracking among prominent RaaS crews, including affiliate payout structures, the relationship between ransomware gangs and information stealers, the growing push to expose private information if ransoms are not paid, and other ties to popular forums in the criminal underground.

Intel 471 will soon be releasing a three-part series that examines the impact of gangs like REvil amid the onslaught of RaaS-based attacks over the past year. The series will cover the explosion in the affiliate model, the relationship between actors selling access to enterprises and how it portends ransomware attacks, and what happens inside businesses when an attack occurs.

You can watch the full interview with the alleged REvil representative below.