# GandCrab ransomware operators put in retirement papers

scmagazine.com/home/security-news/ransomware/gandcrab-ransomware-operators-put-in-retirement-papers/

June 3, 2019

Doug OlenickJune 3, 2019

After operating for about 18 months, the RaaS gang operating under the name GandCrab has announced it has cashed out of the game and has retired.

GandCrab's operators posted a message on a dark web forum indicating the group had made more than $2 billion with its RaaS operation, had laundered the money and was planning a life of leisure, ZD Net reported.

GandCrab uses various exploit kits to deliver a wide variety of malware, including ransomware and cryptocurrency mining malware, and has undergone several upgrades and revisions since it was rolled out in January 2018.

The retirement notice said the group would stop operations within a month and at that time it would delete all its decryptor keys essentially stranding any victims who have not yet paid.

Sherrod DeGrippo, ProofPoint's senior director of threat research and detection, told SC Media she has noticed a steady decline in the volume and frequency of the ransomware over the last few weeks, mainly small campaigns involving Sodinokibi ransomware, but she noted GandCrab's retirement move is something being seen more often.

“This appears to be a case of actors getting out while they are still on top. While malware strains often come and go, we have seen some cybercriminals announce their ‘retirement’ such as the actor behind the Zeus banking Trojan. Interestingly, this actor returned to the scene later with an updated version of the malware,” she said.

DeGrippo noted the GandCrab portal is still active and will likely remain so as affiliates cash out their earnings.

Pierluigi Stella, CTO of Network Box USA, offered several reasons why the GandCrab folks decided to hang up their hats ranging from having a bit more intelligence than other criminals to the possible fact that ransomware may becoming less of a threat due to better defensive methods.

“Are they actually 'giving up' or have they made enough money that they don't need to continue risking being caught?  Hackers usually get caught only when they get greedy and don't know when to stop. This group seems to be smarter - they have made enough money, haven't been caught, and are retiring at the height of their career,” Stella said.

Malwarebytes Malware Intelligence Analyst Marcelo Rivero, called the move a suprise and that "Considering their history of jokes and irony we probably should wait for those 20 days to see what really happens."

Although many companies, municipalities and other types of organizations are frequently victimized, Stella said, “Personally, I am not aware of any of our clients ever actually getting ransomware.  And, disaster recovery procedures now cover ransomware as a possible case of disaster.  Therefore, it is possible that ransomware is becoming less lucrative and this group is getting out while they're still "on top", maybe because they are going to focus on something else, i.e. cryptojacking.”

Others do not believe the GandCrab actors are giving up their day job.

“It is astonishing to read that a cybergang has made so much money they are retiring, and they are publicly announcing it. They are thumbing their noses at all of us. I wouldn’t believe a word of it, though – I would imagine it would be hard to stop, and they will likely resurface soon in another form, helping crooks damage unprotected businesses,” said Dan Tuchler, CMO at SecurityFirst.

Rivero added, "Generally they do not usually retire until they are arrested (there are also the so-called "Exit Scams") or they simply leave the game without prior announcement as in this case."

Doug Olenick

## Related