REvil-ution - A Persistent Ransomware Operation - CYJAX

By William Thomas

Published: 2021-07-09 · Archived: 2026-04-05 22:39:02 UTC

REvil (short for Ransomware Evil) is a revolutionary ransomware operation. Its predecessor, GandCrab, which was retired in early 2019, pioneered the concept of ransomware-as-a-service (RaaS) for “big game hunting” campaigns (where corporate targets are selected according to their annual turnover). REvil’s operators (also known as GoldSouthfield or PinchySpider) continued where GandCrab left off, and thrived. This success encouraged other ransomware strains to be distributed as a RaaS. REvil is known to have many affiliates, many of which crossover with those of GandCrab. Password spraying, exploiting unpatched systems, and initial access malware families – such as IcedID or Qakbot – and now supply-chain attacks, are all methods of distributing REvil. The tactics, techniques, and procedures (TTPs) of this group continue to evolve and it remains one of the primary threats to large organisations.

On 2 July, reports emerged of a widespread ransomware supply-chain attack on US-based firm Kaseya, a remote management and monitoring (RMM) tool used by multiple managed service providers (MSPs). Kaseya warned customers to immediately shut down their VSA server as REvil ransomware was spreading through its auto-update function. By design, Kaseya's RMM software gives administrators the right to install new software on multiple systems. This mechanism was hijacked by the ransomware operators to launch REvil with high-level privileges. Kaseya has reported that up to 60 MSPs, with as many as 1,500 client organisations, are affected. REvil stated in a post on its darknet leaks site, Happy Blog, that over one million systems had been encrypted, demanding a $70 million ransom in Bitcoin for a universal decryptor.

Fig. 1 – Kaseya appearing on REvil’s Happy Blog darknet leaks site

On the cybercrime forums, the REvil RaaS is represented by a user called UNKN (or Unknown) who recruited the first customer for the ransomware’s affiliate program in July 2019. As the ransomware's reputation grew, by hitting larger targets in the public and private sector and making more money, increasingly talented affiliates were brought on board. UNKN’s interviews with journalists reveal just how successful the group has been. UNKN claims that the group makes a profit of $100 million each year and is aiming to make at least $1 billion.

The REvil development team is said to consist of around ten individuals with as many as 60 affiliates that perform the active deployment of the ransomware. In February 2020, REvil’s data-theft-extortion campaign accelerated with the launch of the Happy Blog. REvil’s notoriety increases the chances of securing a ransom payment. The group’s high-profile leaks are frequently covered by mainstream outlets, which works as further motivation for organisations that initially refuse to pay a ransom to engage with the threat actors.

Fig. 2 – The auction site used to sell stolen data if the ransom is not paid

REvil is at the top of a pyramid of around 30 other ransomware groups that perform Big Game Hunting (BGH) campaigns. As noted above, BGH sees groups target large organisations, from both the private and public sectors, with high annual revenues, so that their victims' are more likely to be able to pay multi-million dollar ransom

demands. These amounts, however, have increased significantly since 2019, peaking at a $50 million demand from Acer (it is unknown if they paid) and securing an $11 million ransom from JBS foods, after originally asking for $22.5 million in Bitcoin. Other significant victims targeted by REvil over the last two years include 20 Texas local administrations, Travelex, SoftwareOne, Quest, GSM Law, Banco Estado, Quanta, FujiFilm, Sol Oriens, Invenergy, and more recently French Connection.

Fig. 3 – Example of the REvil ransom note

Fig. 4 – The REvil decryption site

When it was first discovered in April 2019, REvil was delivered via exploiting vulnerabilities in Oracle WebLogic web servers. Since then, the ransomware has been deployed in a number of ways, including via malicious spam campaigns, exploit kits, and RDP brute-forcing. To escalate privileges, REvil also exploits CVE-2018-8453, a Win32k vulnerability, which is rare among ransomware families. REvil's BGH campaign has been successful in leveraging exploits for unpatched VPN products for initial access. This includes Pulse Connect Secure (vulnerable to CVE-2019-11510) and Citrix ADC gateway (CVE-2019-19781), as well as the BlueGate vulnerabilities affecting the Windows Remote Desktop Gateway (tracked as CVE-2020-0609 and CVE-2020-0610). This is no coincidence: during the COVID-19 pandemic, since March 2020, VPNs and RDP have become widely used, with many forced to work from home and establish remote connections to the office.

In the last six months, there have been several reports of REvil ransomware deployment following an initial IcedID or Qakbot infection. IcedID and Qakbot are reportedly developed by LunarSpider and MallardSpider, respectively. These top-tier malware developers collaborate with affiliates and act as Access-as-a-Service brokers for several ransomware gangs, such as Conti or RansomExx, alongside REvil. Both are currently pushed by the Shathak botnet, operated by a group known as TA551 (also called GoldCabin). IcedID and Qakbot both began life as banking Trojans, used for fraud and hijacking accounts. Infections by either malware family are usually now followed by Cobalt Strike and hands-on-keyboard activity that enables threat actors to move laterally, steal data, and encrypt target networks to hold them to ransom.

The fame and profits achieved by the REvil ransomware gang inevitably attracted other cybercriminal syndicates. C&C servers belonging to the infamous FIN7 group (also called CarbonSpider or Carbanak) was linked by security researchers to REvil's infrastructure, indicating that it was likely FIN7 was an operator and affiliate. This is a burgeoning trend, as cybercriminal APT groups shift from Point-of-Sale malware to ransomware, with the former no longer being as profitable as it once was. This has been accelerated by the closure of Joker's Stash - once the largest darknet market for stolen credit cards. A vacuum was left by its shutting down, making it harder for the carders to cash out after a heist, leading many to turn to RaaS and BGH campaigns.

Most updates about the REvil RaaS project come from the underground Russian-speaking forums. Here, UNKN announces major developments to the RaaS, including technical updates and strategies. It was on the forums that we first learned about the RaaS, the extortion site, affiliate recruitment drives, notifications to NASDAQ, acquisition of the KPOT stealer, the arrival of DDoS attacks, calling victims and the media, and the Linux version of REvil. These updates are posted across multiple darknet forums where UNKN recruits affiliates for the REvil. These adverts are a key part of the REvil operation because the RaaS is ultimately competing with other offerings that may give their affiliates a greater split of the ransom.

Fig. 5 – Example of UNKN's posts to underground cybercrime forums

The most recent update to REvil is the addition of a variant to encrypt Linux systems and VMware ESXi virtual machines. In May, UNKN announced that the group was developing a Linux version of the ransomware and one for network-attached storage (NAS) devices. The Linux version of REvil, which also targets ESXi, has now been discovered in the wild. It is an ELF64 executable file that includes the same configuration options utilised by the more common Windows executable version of REvil. When executed on ESXi servers, it will run the ESXCLI tool to list all running ESXi virtual machines and terminate them. It will then close any open virtual machine disk (VMDK) files so that the ransomware can encrypt them.

The targeting of VMware ESXi servers has proven successful for ransomware operators and will continue to be so while so many remain unsecured. By targeting the management servers this way, ransomware can encrypt multiple virtual machines at once with a single command. Here, REvil is following a trend pioneered by others. Ransomware operations such as Babuk, RansomExx, DarkSide, and Hellokitty have all previously created Linux encryptors to target ESXi virtual machines.

Fig. 6 – Timeline of the REvil ransomware campaign by Cyjax

The REvil campaign continues to evolve. Over 260 victims have been leaked to the Happy Blog (all of which have been recorded by the Cyjax Portal) and countless others will have paid a ransom to prevent a listing. To evade international law enforcement, UNKN stated that the group members never travel and claim to be "absolutely apolitical", which is why they have allegedly "never been contacted by any local intelligence offices" in countries in which they operate.

UNKN also admitted to journalists that the arrests of other ransomware gangs benefit the REvil operation. The closure of Maze ransomware, for example, saw REvil's number of affiliates increase. In May 2021, during the aftermath of the Colonial Pipeline ransomware attack perpetrated by the DarkSide gang, the underground cybercriminal community announced a ban on ransomware on multiple forums. This has significantly affected REvil's ability to advertise as a semi-public RaaS offering. However, UNKN stated that REvil will be moving to a closed affiliate program that can only be contacted directly. This is not the end of the REvil RaaS, although it will undoubtedly have impacted their ability to recruit affiliates.

REvil's latest campaign against Kaseya and its MSP customers is by far the group's most devastating to date. It was always likely that one of the many well-resourced ransomware gangs would launch a widespread supply-chain attack. At the end of 2020, we saw two similar disruptive incidents: Cl0p ransomware exploiting Accellion FTA servers and the SolarWinds SUNBURST campaign. Targeting vulnerable software or distributing Trojanised updates makes for a highly effective attack campaign, especially against IT service providers. Compromising one software update can lead to thousands of victims. REvil has shown itself to be capable of rapid evolution. Expect to hear more from them throughout 2021.
