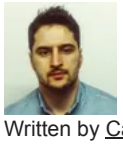
REvil ransomware gang 'acquires' KPOT malware

zdnet.com/article/revil-ransomware-gang-acquires-kpot-malware/

Home Innovation Security

Ransomware gang who claims to have earned $100 million buys the source code of the KPOT information stealer trojan for $6,500.



Written by Catalin Cimpanu, Contributor on Nov. 3, 2020

-
-
-
-
-

Image: Joshua Hoehne

The operators of the REvil ransomware strain have "acquired" the source code of the KPOT trojan in an auction held on a hacker forum last month.

ZDNet Recommends

The best security key

While robust passwords help you secure your valuable online accounts, hardware-based two-factor authentication takes that security to the next level.

Read now

The sale took place after the KPOT malware author decided to auction off the code, desiring to move off to other projects.

The sale was organized as a public auction on a private underground hacking forum for Russian-speaking cyber-criminals, security researcher Pancak3 told ZDNet in an interview last month.

The only bidder was UNKN, a well-known member of the REvil (Sodinokibi) ransomware gang, Pancak3 said.

UNKN paid the initial asking price of $6,500, while other forum members declined to participate, citing the steep asking price.

The REvil operator received the source code of KPOT 2.0, the latest version of the KPOT malware.

First spotted in 2018, KPOT is a classic "information stealer" that can extract and steal passwords from various apps on infected computers. This includes web browsers, instant messengers, email clients, VPNs, RDP services, FTP apps, cryptocurrency wallets, and gaming software, according to a 2019 Proofpoint report.

Pancak3, who first spotted the KPOT auction in mid-October, told ZDNet that he believes the REvil gang bought KPOT to "further develop it" and add it to its considerable arsenal of hacking tools the gang uses during its targeted intrusions inside corporate networks.

Although many other forum members have described the KPOT code as overpriced, UNKN and the REvil gang have money to spare.

The REvil member, who has been operating as the ransomware gang's public figurehead and recruiter for the past two years on hacking forums, has recently given an interview to a Russian YouTube channel, claiming that the REvil gang makes more than $100 million from ransom demands each year [1, 2].

UNKN also claimed the gang fears assassinations more than they fear a law enforcement action.

The FBI's most wanted cybercriminals