

Google Obtains Court Order to Disrupt CryptBot Distribution

Google this week announced that it has obtained a court order that helped it disrupt the CryptBot information stealer's distribution.

Initially designed to harvest and exfiltrate sensitive information such as credentials, cryptocurrency wallets, and more, CryptBot was also seen distributing banking trojans.

Over the past year alone, the malware infected roughly 670,000 computers, Google estimates.

The malware has been distributed via modified versions of legitimate software, including Google Earth Pro and Chrome, with recent CryptBot versions focusing heavily on the users of the Chrome browser.

According to Google, its investigation into the malware has identified several major CryptBot distributors based in Pakistan, which operate a global criminal enterprise.

To disrupt the operation, Google filed a legal complaint in the Southern District of New York, and a judge has granted the internet giant a temporary restraining order to act against the identified distributors.

"We're targeting the distributors who are paid to spread malware broadly for users to download and install, which subsequently infects machines and steals user data. [...] The legal complaint is based on a variety of claims, including computer fraud and abuse and trademark infringement," Google says.

Armed with the fresh court order, Google can take down current and future domains used to distribute CryptBot, which is expected to impact the infostealer's infection rates.

"This will slow new infections from occurring and decelerate the growth of CryptBot. Lawsuits have the effect of establishing both legal precedent and putting those profiting, and others who are in the same criminal ecosystem, under scrutiny," the internet giant says.

Related: Technical, Legal Action Taken to Prevent Abuse of Cobalt Strike, Microsoft Software

Related: Industry Reactions to Hive Ransomware Takedown: Feedback Friday

Related: Facebook Takes Legal Action Against Data Scrapers

Google Obtains Court Order to Disrupt CryptBot Distribution