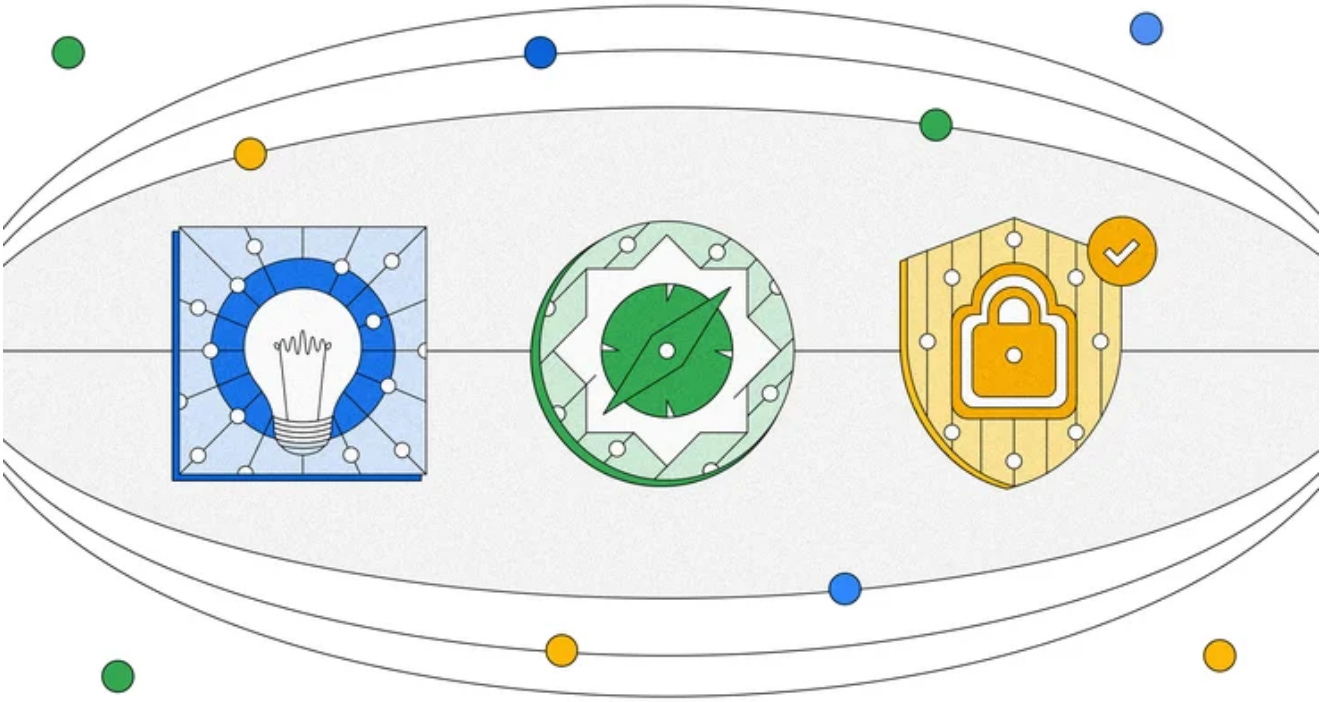
Continuing our work to hold cybercriminal ecosystems accountable

blog.google/technology/safety-security/continuing-our-work-to-hold-cybercriminal-ecosystems-accountable/

Mike Trinh April 26, 2023



Safety & Security

Last year, we shared details about our success in holding operators of the Glupteba botnet responsible for their targeting of online users. We noted that our work was not done and that we would continue raising awareness around issues and working to disrupt groups looking to take advantage of users. Today, we're sharing another milestone in that work.

Yesterday, a federal judge in the Southern District of New York unsealed our civil action against the malware distributors of Cryptbot, which we estimate infected approximately 670,000 computers this past year and targeted users of Google Chrome to steal their data. 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. Cybercriminals often operate like businesses, specializing in a particular function, and partner with other criminal specialists to profit off harm to innocent users. This lawsuit targeting Cryptbot's malware distributors shows our commitment to protecting users from each level of the cybercriminal ecosystem.

About CryptBot

CryptBot is a type of malware often referred to as an “infostealer” because it is designed to identify and steal sensitive information from victims’ computers such as authentication credentials, social media account logins, cryptocurrency wallets, and more. CryptBot then sends the stolen data to be harvested and eventually sold to bad actors to use in data breach campaigns. CryptBot distributors offer maliciously modified versions of many software packages, including Google Earth Pro and Google Chrome. Users download and install these packages, without realizing that doing so infects their machines with malware. Recent CryptBot versions have been designed to specifically target users of Google Chrome, which is where Google’s CyberCrimes Investigations Group (CCIG) and Threat Analysis Group (TAG) teams worked to identify the distributors, investigate and take action.

Legal strategy and disruption

Our litigation was filed against several of CryptBot’s major distributors who we believe are based in Pakistan and operate a worldwide criminal enterprise. The legal complaint is based on a variety of claims, including computer fraud and abuse and trademark infringement. To hamper the spread of CryptBot, the court has granted a temporary restraining order to bolster our ongoing technical disruption efforts against the distributors and their infrastructure. The court order allows us to take down current and future domains that are tied to the distribution of CryptBot. 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.

Dangers of unknown software

To further combat security risks, Cybercrime Support Network recommends additional steps users should take to protect themselves against malware like CryptBot:

- **Download from well-known and trusted sources:** Only download software from the official website or app store and take Chrome Safe Browsing warnings seriously.
- **Read reviews and do your research:** Before downloading any software, do research on the product, and read reviews from others who have already downloaded and used the software.
- **Keep your operating system and software up-to-date:** Make sure to regularly update your device's operating system and software to the latest version. Updates often include security patches and bug fixes that can help protect from threats.

Looking ahead

This litigation is another step forward in holding cybercriminals accountable, by not just targeting those that operate botnets, but also those that profit from malware distribution. With these, and future actions, we look forward to continuing our ongoing commitment to help protect the safety of online users.

POSTED IN:

Safety & Security