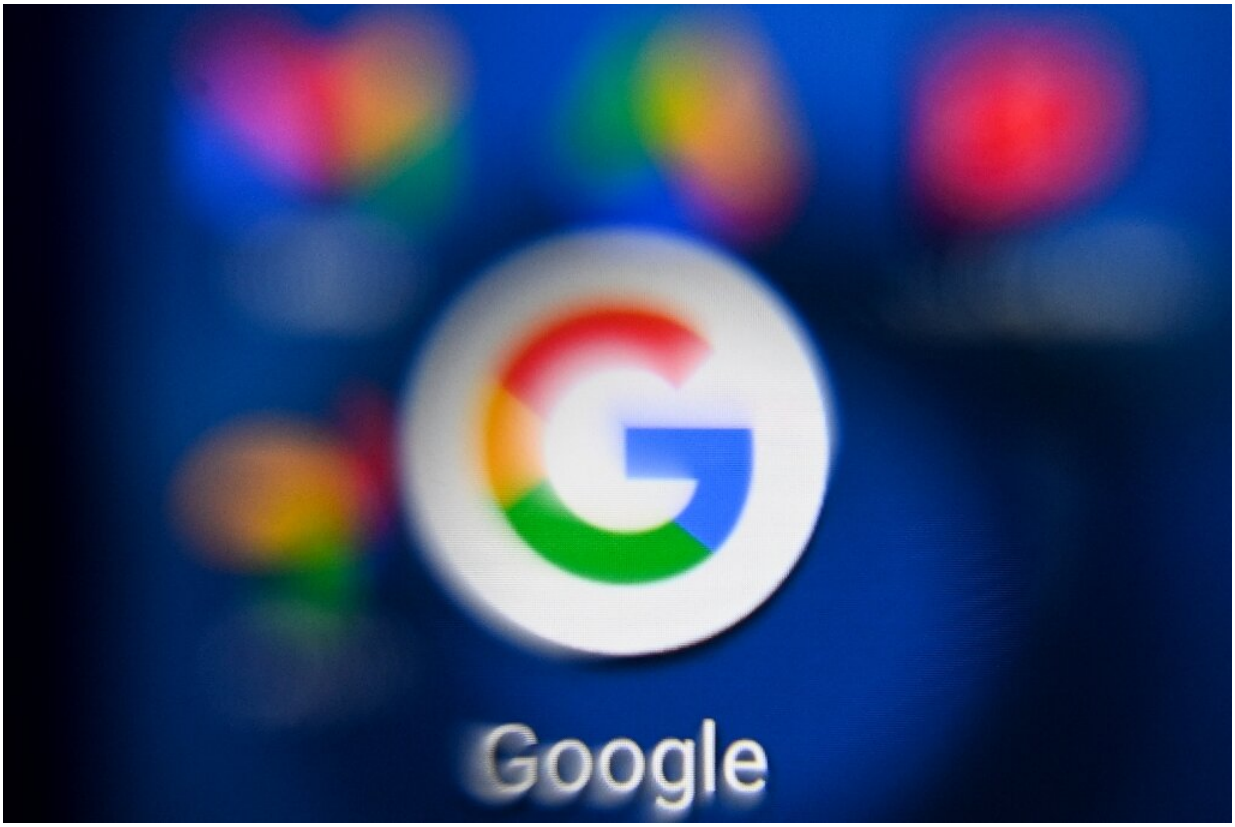
Google disrupts cybercrime web infecting 1 mn devices

December 8 2021



Google takes aim at cybercrime web.

Google said Tuesday it has moved to shut down a network of about one million hijacked electronic devices used worldwide to commit online crimes, while also suing Russia-based hackers the tech giant claimed

were responsible.

The so-called botnet of infected devices, which was also used to surreptitiously mine bitcoin, was cut off at least for now from the people wielding it on the internet.

"The operators of Glupteba are likely to attempt to regain control of the botnet using a backup command and control mechanism," wrote Shane Huntley and Luca Nagy from Google's threat analysis group.

Large technology companies like Google and Microsoft are increasingly pulled into the battle against cybercrime, which is conducted via their products thus giving them unique understanding of and access to the threats.

Google said the network includes about one million Windows-using devices worldwide for crimes that include stealing users' credentials, and has targeted victims from the United States, India, Brazil and southeast Asia.

The company also filed a lawsuit in a New York federal court against Dmitry Starovikov and Alexander Filippov seeking an injunction to block them from wrongdoing on its platforms.

Cybersecurity experts first noticed Glupteba in 2011, which spreads by masquerading as free, downloadable software, videos or movies that people unwittingly download onto their devices.

However, unlike conventional botnets that rely on predetermined channels to ensure their survival, Glupteba is programmed to find a replacement server in order to keep operating even after being attacked, says Google's lawsuit.

Because the botnet web combines the power of some one million devices it possesses unusual power that could be used for large-scale ransomware or other attacks.

To maintain that network, the organization "uses Google advertisements to post job openings for the websites" carrying out the illegal work.

The hackers also used Google's own services to distribute the malware—the internet giant took down some 63 million Google Docs and terminated over 1,100 Google accounts used to spread Glupteba.

The botnets can "recover more quickly from disruptions, making them that much harder to shutdown. We are working closely with industry and government as we combat this type of behavior," Google said in a blog post.