Google files groundbreaking civil suit to disrupt massive botnet with blockchain backup system

Cybersecurity Law Alert

10 December 2021
By: Edward J. McAndrew

Google has filed a groundbreaking civil suit this week against two Russian hackers who allegedly control the massive Glupteba botnet, which utilizes a blockchain backup mechanism and which has infected more than 1 million Windows computers worldwide. The action illustrates how private entities are increasingly taking legal and technical actions without the aid of law enforcement agencies to disrupt and deter cybercrime.

Created around 2011, Glupteba malware is generally distributed via free download sites and Google's own services. In just the past year, Google took down approximately 63 million Google Docs, more than 1,000 Google accounts and 900 Google Cloud projects that were being used to distribute the malware.

How the malware works

Once implanted, the malware infects a computer and any connected devices and turns them into "bots" in a network that its operators use to execute various cybercrime schemes. Glupteba bots mine cryptocurrencies and steal user credentials, session cookies, personal information and other data. Its operators then offer a menu of "cybercrime-as-a-service" options, including: (1) access to infected bots, Google accounts and live sessions to be used as proxies in cyberattacks; (2) stolen financial information for fraudulent online purchases; (3) pop-up ads on infected devices in aid of

digital ad fraud schemes; and (4) bot computing power for cryptocurrency mining.

Perhaps most concerning, the botnet also could be used to launch ransomware or DDoS attacks. Unlike traditional botnets, Glupteba has a command-and-control backup mechanism that hides C2 server reconnection messages in the public Bitcoin blockchain, making it extremely difficult to disrupt on an ongoing basis.

Aiming to create a disruptive legal mechanism

Google has been working with Internet industry partners to temporarily dislodge network control from the Glupteba operators. The civil action is intended to impose liability and to create a legal mechanism for continuing to disrupt the botnet if and when the operators recover command and control of it.

Filed in the Southern District of New York, Google's complaint for damages and injunctive relief includes claims under RICO, the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the Lanham Act. Although it most certainly will go unanswered, Google's well-pleaded complaint should not go unread . For instance, Google was able to attribute much of the Glupteba activity to the named defendants because they used the same IP addresses to access their Gmail accounts and their C2 servers. That they did not bother to use the very obfuscation techniques they sell to others says much about their utter disregard for the legal repercussions of their global criminal conduct. "Glupteba," by the way, literally translates as "stupid you."

Civil action with a twist

Civil actions to take down botnets have been around for years, but the blockchain aspect adds a new twist. Whether Google's legal strategy succeeds in continuing to disrupt the botnet is worth following closely. Once default judgment and an injunction are entered, Google may be able to wield the injunction against any Internet infrastructure player within the jurisdiction of a US court – or a foreign court that will recognize and enforce the SDNY injunction. In addition, where it can prove attribution to Bitcoin wallets, Google may be able to seize cryptocurrency mined through the botnet or tied to its operators to satisfy whatever damages award it can obtain.

As we have seen with recent law enforcement actions, the most effective tools against international cybercriminals include seizing their infrastructure and ill-gotten financial gains. Divesting them of their weapons and their money may be the best we can do – short of long-term incarceration, when achievable – to alter their criminal behavior. That private actors are increasingly stepping into what has heretofore been the sole domain of law enforcement is a positive – and necessary – development.

In the end, actions like Google's Glupteba takedown may prove to be another game of botnet whack-a-mole, but this time, the hammer is heavier and the prize money could be very real.

AUTHORS

Edward J. McAndrew
Partner
Wilmington | T: +1 302 468 5700
Washington, DC | T: +1 202 799 4000
ed.mcandrew@dlapiper.com