New action to combat cyber crime

blog.google/technology/safety-security/new-action-combat-cyber-crime/

Royal Hansen

December 7, 2021

Today, we took action to disrupt Glupteba, a sophisticated botnet which targets Windows machines and protects itself using blockchain technology. Botnets are a real threat to Internet users, and require the efforts of industry and law enforcement to deter them. As part of our ongoing work to protect people who use Google services via Windows and other IoT

devices, our Threat Analysis Group took steps to detect and track Glupteba's malicious activity over time. Our research and understanding of this botnet's operations puts us in a unique position to disrupt it and safeguard Internet users around the world.

We're doing this in two ways. First, we are coordinating with industry partners to take technical action.

And second, we are using our resources to launch litigation — the first lawsuit against a blockchain enabled botnet — which we think will set a precedent, create legal liability for the botnet operators, and help deter future activity.

About the Glupteba botnet

A botnet is a network of devices connected to the internet that have been infected with a type of malware that places them under the control of bad actors. They can then use the infected devices for malicious purposes, such as to steal your sensitive information or commit fraud through your home network.

After a thorough investigation, we determined that the Glupteba botnet currently involves approximately one million compromised Windows devices worldwide, and at times, grows at a rate of thousands of new devices per day. Glupteba is notorious for stealing users' credentials and data, mining cryptocurrencies on infected hosts, and setting up proxies to funnel other people's internet traffic through infected machines and routers.

Technical action

We coordinated with industry partners to take technical action. We have now disrupted key command and control infrastructure so those operating Glupteba should no longer have control of their botnet — for now.

However, due to Glupteba's sophisticated architecture and the recent actions that its organizers have taken to maintain the botnet, scale its operations, and conduct widespread criminal activity, we have also decided to take legal action against its operators, which we believe will make it harder for them to take advantage of unsuspecting users. .

Legal Strategy & Disruption

Our litigation was filed against the operators of the botnet, who we believe are based in Russia. We filed the action in the Southern District of New York for computer fraud and abuse, trademark infringement, and other claims. We also filed a temporary restraining order to bolster our technical disruption effort. If successful, this action will create real legal liability for the operators.

Making the Internet Safer

Unfortunately, Glupteba's use of blockchain technology as a resiliency mechanism is notable here and is becoming a more common practice among cyber crime organizations. The decentralized nature of blockchain allows the botnet to 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, so that even if Glupteba returns, the internet will be better protected against it.

Our goal is to bring awareness to these issues to protect our users and the broader ecosystem, and to prevent future malicious activity.

We don't just plug security holes, we work to eliminate entire classes of threats for consumers and businesses whose work depends on the Internet. We have teams of analysts and security experts who are dedicated to identifying and stopping issues like DDoS, phishing campaigns, zero-day vulnerabilities, and hacking against Google, our products, and our users.

Taking proactive actions like this are critical to our security. We understand and recognize the threats the Internet faces, and we are doing our part to address them.