New action to disrupt world's largest online criminal network

blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/

March 10, 2020

Today, Microsoft and partners across 35 countries took coordinated legal and technical steps to disrupt one of the world's most prolific botnets, called Necurs, which has infected more than nine million computers globally. This disruption is the result of eight years of tracking and planning and will help ensure the criminals behind this network are no longer able to use key elements of its infrastructure to execute cyberattacks.

A botnet is a network of computers that a cybercriminal has infected with malicious software, or malware. Once infected, criminals can control those computers remotely and use them to commit crimes. Microsoft's Digital Crimes Unit, BitSight and others in the security community first observed the Necurs botnet in 2012 and have seen it distribute several forms of malware, including the GameOver Zeus banking trojan.

The Necurs botnet is one of the largest networks in the spam email threat ecosystem, with victims in nearly every country in the world. During a 58-day period in our investigation, for example, we observed that one Necurs-infected computer sent a total of 3.8 million spam

emails to over 40.6 million potential victims.

Necurs is believed to be operated by criminals based in Russia and has also been used for a wide range of crimes including pump-and-dump stock scams, fake pharmaceutical spam email and “Russian dating” scams. It has also been used to attack other computers on the internet, steal credentials for online accounts, and steal people’s personal information and confidential data. Interestingly, it seems the criminals behind Necurs sell or rent access to the infected computer devices to other cybercriminals as part of a botnet-for-hire service. Necurs is also known for distributing financially targeted malware and ransomware, cryptomining, and even has a DDoS (distributed denial of service) capability that has not yet been activated but could be at any moment.

On Thursday, March 5, the U.S. District Court for the Eastern District of New York issued an order enabling Microsoft to take control of U.S.-based infrastructure Necurs uses to distribute malware and infect victim computers. With this legal action and through a collaborative effort involving public-private partnerships around the globe, Microsoft is leading activities that will prevent the criminals behind Necurs from registering new domains to execute attacks in the future.

This was accomplished by analyzing a technique used by Necurs to systematically generate new domains through an algorithm. We were then able to accurately predict over six million unique domains that would be created in the next 25 months. Microsoft reported these domains to their respective registries in countries around the world so the websites can be blocked and thus prevented from becoming part of the Necurs infrastructure. By taking control of existing websites and inhibiting the ability to register new ones, we have significantly disrupted the botnet.

Microsoft is also taking the additional step of partnering with Internet Service Providers (ISPs) and others around the world to rid their customers’ computers of malware associated with the Necurs botnet. This remediation effort is global in scale and involves collaboration with partners in industry, government and law enforcement via the Microsoft Cyber Threat Intelligence Program (CTIP). Through CTIP, Microsoft provides law enforcement, government Computer Emergency Response Teams (CERTs), ISPs and government agencies responsible for the enforcement of cyber laws and the protection of critical infrastructure with better insights into criminal cyber infrastructure located within their jurisdiction, as well as a view of compromised computers and victims impacted by such criminal infrastructure.

For this disruption, we are working with ISPs, domain registries, government CERTs and law enforcement in Mexico, Colombia, Taiwan, India, Japan, France, Spain, Poland and Romania, among others. Each of us has a critical role to play in protecting customers and keeping the internet safe.

To make sure your computer is free of malware, visit support.microsoft.com/botnets.

Tags: botnet, CTIP, cyberattacks, cybercrime, Digital Crimes Unit, Microsoft Cyber Threat Intelligence Program, necurs