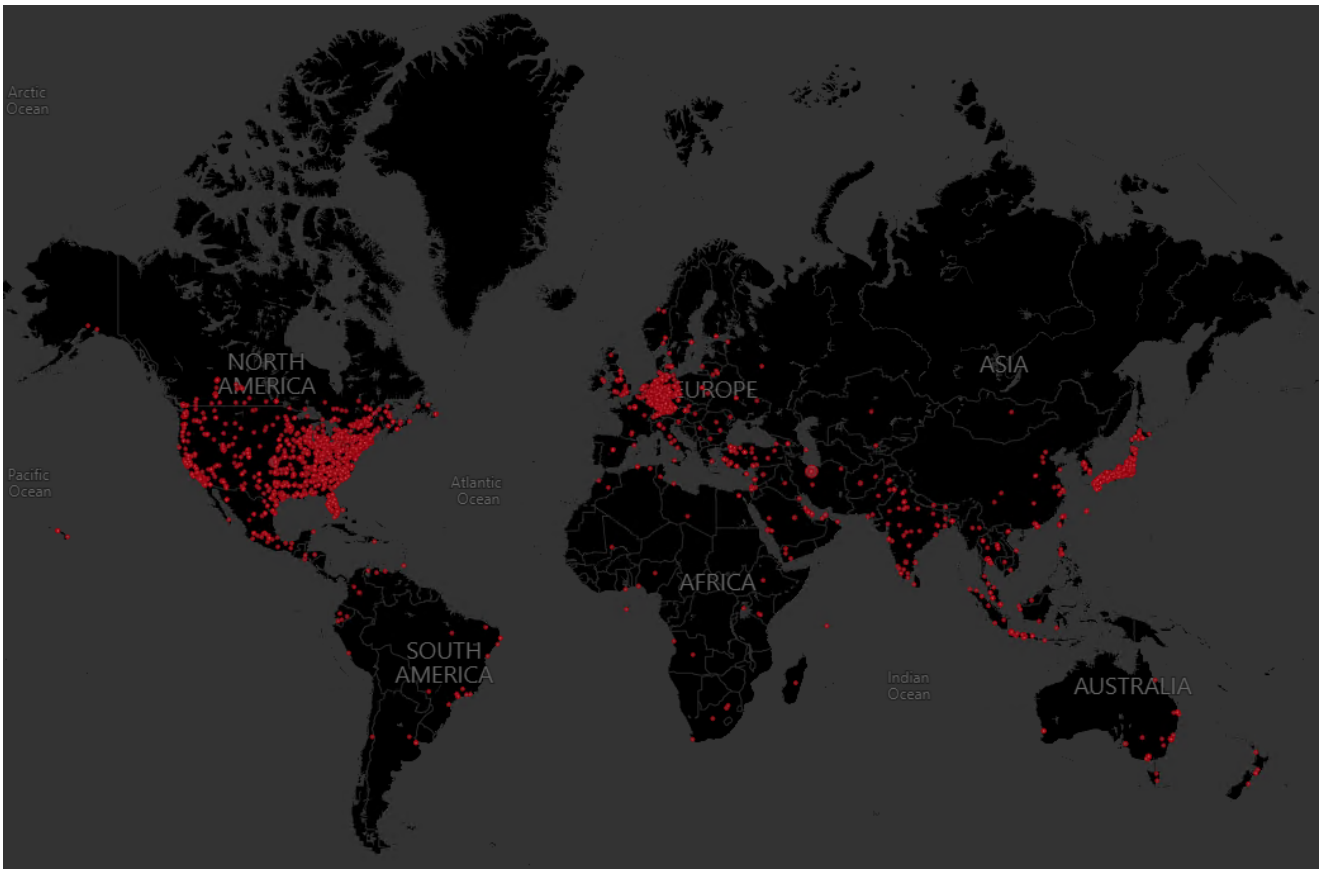
Notorious cybercrime gang's botnet disrupted

blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/

April 13, 2022



Today, we're announcing that Microsoft's Digital Crimes Unit (DCU) has taken legal and technical action to disrupt a criminal botnet called ZLoader. ZLoader is made up of computing devices in businesses, hospitals, schools, and homes around the world and is run by a global internet-based organized crime gang operating malware as a service that is designed to steal and extort money.

We obtained a court order from the United States District Court for the Northern District of Georgia allowing us to take control of 65 domains that the ZLoader gang has been using to grow, control and communicate with its botnet. The domains are now directed to a Microsoft sinkhole where they can no longer be used by the botnet's criminal operators. Zloader contains a domain generation algorithm (DGA) embedded within the malware that creates additional domains as a fallback or backup communication channel for the botnet. In addition to the hardcoded domains, the court order allows us to take control of an additional 319 currently registered DGA domains. We are also working to block the future registration of DGA domains.

During our investigation, we identified one of the perpetrators behind the creation of a component used in the ZLoader botnet to distribute ransomware as Denis Malikov, who lives in the city of Simferopol on the Crimean Peninsula. We chose to name an individual in connection with this case to make clear that cybercriminals will not be allowed to hide behind the anonymity of the internet to commit their crimes. Today's legal action is the result of months of investigation that pre-date the current conflict in the region.

Originally, the primary goal of Zloader was financial theft, stealing account login IDs, passwords and other information to take money from people's accounts. Zloader also included a component that disabled popular security and antivirus software, thereby preventing victims from detecting the ZLoader infection. Over time those behind Zloader began offering malware as a service, a delivery platform to distribute ransomware including Ryuk. Ryuk is well known for targeting health care institutions to extort payment without regard to the patients that they put at risk.

DCU led the investigative effort behind this action in partnership with ESET, Black Lotus Labs (the threat intelligence arm of Lumen), and Palo Alto Networks Unit 42, with additional data and insights to strengthen our legal case from our partners the Financial Services Information Sharing and Analysis Centers (FS-ISAC) and the Health Information Sharing and Analysis Center (H-ISAC), in addition to our Microsoft Threat Intelligence Center and Microsoft Defender team. We also recognize the additional contribution from Avast in supporting our DCU field in Europe.

Our disruption is intended to disable ZLoader's infrastructure and make it more difficult for this organized criminal gang to continue their activities. We expect the defendants to make efforts to revive Zloader's operations. We referred this case to law enforcement, are tracking this activity closely and will continue to work with our partners to monitor the behavior of these cybercriminals. We will work with internet service providers (ISPs) to identify and remediate victims. As always, we're ready to take additional legal and technical action to address Zloader and other botnets.

Tags: cyberattacks, cybercrime, ransomware