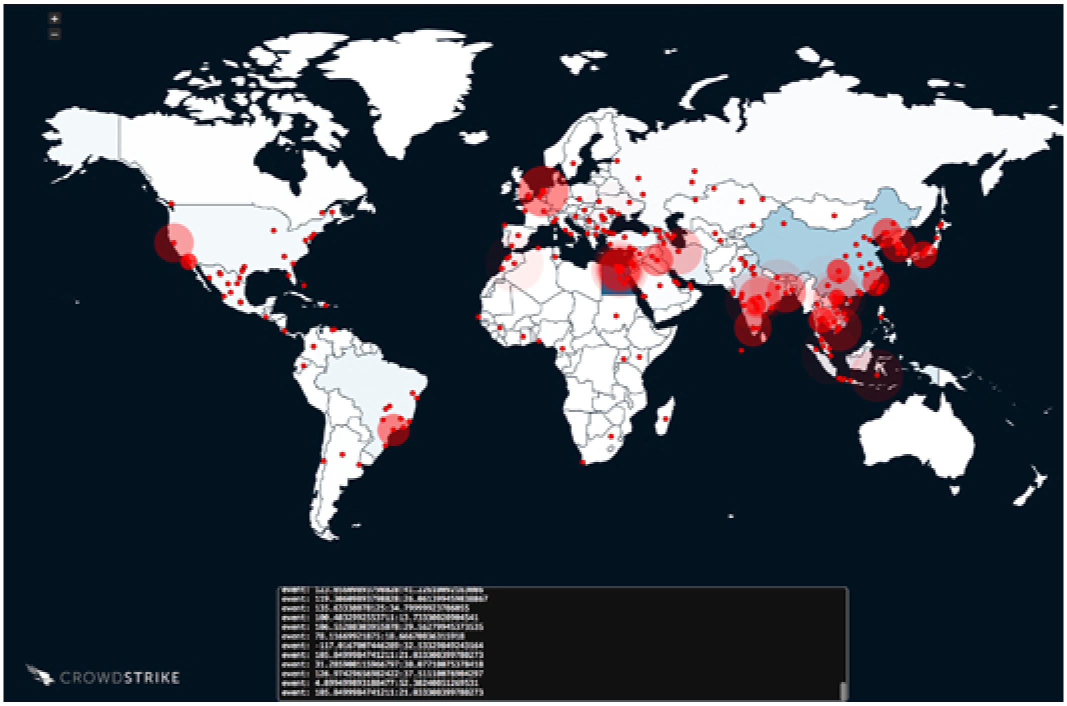
Inside the Takedown of ZOMBIE SPIDER and the Kelihos Botnet

crowdstrike.com/blog/inside-the-takedown-of-zombie-spider-and-the-kelihos-botnet/

April 13, 2017

April 13, 2017

Falcon Intelligence Team Research & Threat Intel



This figure shows a snapshot of systems infected with Kelihos communicating with the sinkhole created to disable it.

The arrest of Russian cybercriminal Pyotr Levashov (aka Peter Severa, or threat actor ZOMBIE SPIDER to CrowdStrike Falcon Intelligence™ subscribers), made global headlines this week and with good reason. For several years, Levashov had been the subject of an international law enforcement operation led by the FBI, which sought to curtail his global criminal activities powered by a peer-to-peer (P2P) botnet known as Kelihos. Levashov was the primary threat actor behind Kelihos, and its predecessors Waledac and Storm.

At the time of Levashov's arrest, the botnet had been operating globally, responsible for perpetrating a wide range of illegal activities including: delivering remote access tools to hijack computers in the Netherlands; distributing banking Trojans in North America, Australia and Europe; engaging in pump-and-dump trading scams (designed to falsely inflate the price of a stock so it can be quickly dumped for profit); spamming victims with advertisements for illegal pharmaceutical sites; delivering ransomware; and conducting massive distributed denial-of-service (DDoS) attacks.

Arresting Levashov was a critical first step in dismantling his incalculably destructive global enterprise – the next step was neutralizing the Kelihos botnet itself. The CrowdStrike Falcon Intelligence team, which had been tracking Levashov as the adversary called ZOMBIE SPIDER, was able to help law enforcement seize control of the Kelihos botnet so that it could no longer be used by criminal actors. To understand that accomplishment, it's important to learn more about Kelihos and how it operates.

The Kelihos Botnet

A botnet is a collection of victim computers infected with malware, connected through a centralized command and control (C2) infrastructure maintained by the criminal hacker. A botnet can be massive – many are comprised of tens of thousands of "zombie" machines – all being used for nefarious purposes. Kelihos was a botnet that employed peer-to-peer (P2P) communications using infected systems that acted as proxies, relaying information between each other and the Kelihos backend servers. This decentralized structure makes P2P botnets harder to disrupt than the more traditional variety. Levashov was able to operate the vast Kelihos network as a service, allowing other criminals to pay for delivering their own spam, banking trojans, ransomware, and even DDoS attacks. His criminal proficiency had even won him a spot on the top 10 list of the world's worst spammers maintained by the anti-spam group Spamhaus.

Here are some key facts about the Kelihos botnet, as compiled by Falcon Intelligence:

- Kelihos is a multi-purpose P2P botnet that emerged in late 2010, shortly after its predecessor (known as Waledac) was dismantled.
- Since its inception, Kelihos has been subject to several takedown operations and each time the botnet has been rebuilt in a new, more robust manner.
- The botnet is primarily used to deliver spam email, but it has a wide assortment of plugins that extend its functionality, including: credential and email address harvesting; launching distributed denial of service (DDoS) attacks; performing click fraud; and fast-flux DNS hosting.
- Previous versions had the ability to mine Bitcoin.
- Kelihos was deliberately designed to be difficult to reverse engineer – its network protocol contains several layers of encryption including RSA, blowfish, and a custom obfuscation algorithm that the malware author refers to as "monkey" functions.
- The fifth and current generation of the botnet has been around since the summer of 2013, with an estimated size of 50,000 to 75,000 infected machines.

The CrowdStrike Falcon Intelligence Team's Role

In order to seize control of the Kelihos botnet, a technique known as "peer list poisoning" was used. The objective of peer list poisoning is to use the criminal's own bot network, what one might consider his strength, against him. The process involved propagating a carefully crafted peer list that prevented the threat actor, in this case ZOMBIE SPIDER, from communicating with infected systems. As a result of the peer list poisoning, the P2P network was transformed into a centralized network, with infected systems only allowed to communicate with a sinkhole established by law enforcement. In effect, this neutralized Kelihos by redirecting communications from infected machines to the sinkhole, rather than the intended C2 infrastructure. Since this technical operation began, Falcon Intelligence has observed 50,541 unique infections communicating with the sinkhole server.

While the arrest of Levashov, and the team's related actions to dismantle Kelihos, are important milestones, we have not seen the last of this breed of criminal enterprises. That's why organizations need to arm themselves with intelligence-driven endpoint security that can address the increasingly sophisticated threats the future is sure to hold.

Learn more about CrowdStrike Falcon Intelligence and CrowdStrike's cyber intelligence subscription offerings.

Related Content

Who is EMBER BEAR?

A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router

PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell