

# Zombie Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:44:09 UTC

Description([CrowdStrike](#)) The primary threat actor, who was tracked by CrowdStrike as Zombie Spider, rose to prominence in the criminal underground under the moniker Peter Severa. The individual behind this handle is Peter Yuryevich LEVASHOV who was arrested in Spain when the final version of Kelihos was taken over in April 2017, and who recently pleaded guilty to operating the botnet for criminal purposes.

For several years, pump-and-dump stock scams, dating ruses, credential phishing, money mule recruitment and rogue online pharmacy advertisements were the most common spam themes. In 2017, however, Kelihos was frequently used to spread other malware such as LuminosityLink, Zyklon HTTP, Neutrino, Nymaim, Gozi/ISFB, Panda Zeus, Kronos, and TrickBot. It was also observed spreading ransomware families including Shade, Cerber, and FileCrypt2.

Kelihos has been observed to distribute TrickBot ([Wizard Spider, Gold Blackburn](#)) and Zeus Panda ([Bamboo Spider, TA544](#)).

---

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=2c1d1677-f2d9-44e1-ac9a-4f7f4047e2d5>