EINPRESSWIRE

ESET Research: Infamous IoT botnet Mozi taken down via a kill switch

DUBAI, UNITED ARAB EMIRATES, November 3, 2023 /EINPresswire.com/ -- ESET Research recently observed the sudden demise of one of the most prolific Internet of Things (IoT) botnets, named Mozi, infamous for exploiting vulnerabilities in hundreds of thousands of IoT devices each year. User Datagram Protocol (UDP) observed an unanticipated drop in activity that began in India and was also observed in China a week later. The change was caused by an update to Mozi bots that stripped them of their functionality. A few weeks following these events, ESET researchers were able to identify and analyze the kill switch that caused Mozi's demise.

“The demise of one of the most prolific IoT botnets is a fascinating case of cyber forensics, providing us with intriguing technical information on how such botnets in the wild are created, operated, and dismantled,” says ESET researcher Ivan Bešina, who investigated the disappearance of Mozi.

On September 27, 2023, ESET researchers spotted the control payload (configuration file) inside a UDP message missing the typical content; its new activity was in fact to act as the kill switch responsible for Mozi's takedown. The kill switch stopped the parent process – the original Mozi malware – and disabled certain system services, replaced the original Mozi file with itself, executed certain router/device configuration commands, and disabled access to various ports.

Despite the drastic reduction in functionality, the Mozi bots have maintained persistence, indicating a deliberate and calculated takedown. ESET analysis of the kill switch showed a strong connection between the botnet's original source code and recently used control payloads that were signed by the correct private keys.

“There are two potential instigators for this takedown: the original Mozi botnet creator or Chinese law enforcement, perhaps enlisting or forcing the cooperation of the original actor or actors. The sequential targeting of India and then China suggests that the takedown was carried out deliberately, with one country targeted first and the other a week later," explains Bešina.

For more technical information about the demise of the Mozi botnet, check out the blog post "Who killed Mozi? Finally putting the IoT zombie botnet in its grave" Make sure to follow ESET Research on Twitter (now known as X) for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and X (Twitter).

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here