Trend Micro Research Discovers Botnet Battle for Home Routers

Report warns of users caught in the middle of new cybercrime turf war

DALLAS, July 15, 2020 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released new research warning consumers of a major new wave of attacks attempting to compromise their home routers for use in IoT botnets. The report urges users to take action to stop their devices from enabling this criminal activity.

There has been a recent spike in attacks targeting and leveraging routers, particularly around Q4 2019. This research indicates increased abuse of these devices will continue as attackers are able to easily monetize these infections in secondary attacks.

"With a large majority of the population currently reliant on home networks for their work and studies, what's happening to your router has never been more important," said Jon Clay, director of global threat communications for Trend Micro. "Cybercriminals know that a vast majority of home routers are insecure with default credentials and have ramped up attacks on a massive scale. For the home user, that's hijacking their bandwidth and slowing down their network. For the businesses being targeted by secondary attacks, these botnets can totally take down a website, as we've seen in past high-profile attacks."

Trend Micro's research revealed an increase from October 2019 onwards in brute force log-in attempts against routers, in which attackers use automated software to try common password combinations. The number of attempts increased nearly tenfold, from around 23 million in September to nearly 249 million attempts in December 2019. As recently as March 2020, Trend Micro recorded almost 194 million brute force logins.

Another indicator that the scale of this threat has increased is devices attempting to open telnet sessions with other IoT devices. Because telnet is unencrypted, it's favored by attackers – or their botnets – as a way to probe for user credentials. At its peak, in mid-March 2020, nearly 16,000 devices attempted to open telnet sessions with other IoT devices in a single week.

This trend is concerning for several reasons. Cybercriminals are competing with each other to compromise as many routers as possible so they can be conscripted into botnets. These are then sold on underground sites either to launch Distributed Denial of Service (DDoS) attacks, or as a way to anonymize other attacks such as click fraud, data theft and account takeover.

Competition is so fierce that criminals are known to uninstall any malware they find on targeted routers, booting off their rivals so they can claim complete control over the device.

For the home user, a compromised router is likely to suffer performance issues. If attacks are subsequently launched from that device, their IP address may also be blacklisted – possibly implicating them in criminal activity and potentially cutting them off from key parts of the internet, and even corporate networks.

As explained in the report, there's a thriving black market in botnet malware and botnets-for-hire. Although any IoT device could be compromised and leveraged in a botnet, routers are of particular interest because they are easily accessible and directly connected to the internet.

Trend Micro makes the following recommendations for home users:

- Make sure you use a strong password. Change it from time to time.
- Make sure the router is running the latest firmware.

- Check logs to find behavior that doesn't make sense for the network.
- Only allow logins to the router from the local network.

To read the complete report, please visit: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/caught-in-the-crossfire-defending-devices-from-battling-botnets.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com.

SOURCE Trend Micro Incorporated

For further information: Media Contact: Erin Johnson, 817-522-7911, media_relations@trendmicro.com

---