Appears new malware HiatusRAT targeting enterprise routers

A new malware campaign, called Hiatus, is targeting small business routers to steal data and track victims.

New "Hiatus" malware campaign attacks enterprise routers

A new malware campaign, dubbed "Hiatus" is targeting small business routers through the use of HiatiusRAT malware.

On March 6, 2023, research firm Lumen published a blog post discussing this malicious campaign. Lumen's blog post states that "Lumen Black Lotus Labs has identified another never-before-seen campaign involving compromised routers".

HiatusRAT is a type of malware known as a Remote Access Trojan (RAT). The Remote Access Trojan is used by cybercriminals to gain remote access and control over the target device. The latest version of the HiatusRAT malware appears to have been in use since July 2022.

Lumen's blog post also states that "HiatusRAT allows the threat actor to remotely interact with the system, and it uses prebuilt functionality - some of which are highly unusual - to transform the compromised machine into as a secret proxy for the threat agent".

Using the command line utility "tcpdump", HiatusRAT can intercept network traffic passing through the targeted router, allowing data theft. Lumen also speculates that the bad guys involved in this attack aim to establish a secret proxy network through the attack.

HiatusRAT is targeting specific types of routers

HiatusRAT malware is being used to attack old DrayTek Vigor VPN routers, specifically models 2690 and 3900 running i386 architecture. These are high-bandwidth routers used by businesses to support VPNs for remote workers.

These router models are often used by small and medium business owners who are at risk of becoming a specific target in this campaign. Researchers do not currently know how these DrayTek Vigor routers were compromised at the time of writing.

More than 4,000 devices were found to be vulnerable to this malware campaign in mid-February, meaning many businesses are at risk.

Attackers only targeted a few DrayTek routers

Of all the DrayTek 2690 and 3900 routers connected to the Internet today, Lumen reported an infection rate of just 2%.

This shows that attackers are trying to leave a minimal footprint in order to limit exposure and avoid detection. Lumen also suggests in the aforementioned blog post that this tactic is also being used by attackers to "maintain critical points of presence".

HiatusRAT creates big risks for businesses

At the time of this writing, HiatusRAT poses a risk to many small businesses, with thousands of routers still exposed to this malware. Time will tell how many DrayTek routers are successfully targeted in this malicious campaign.