Threat actors are using advanced malware to backdoor business-grade routers

reader comments

19 with

Share this story

Researchers have uncovered advanced malware that’s turning business-grade routers into attacker-controlled listening posts that can sniff email and steal files in an ongoing campaign hitting North and South America and Europe.

Besides passively capturing IMAP, SMTP, and POP email, the malware also backdoors routers with a remote access Trojan that allows the attackers to download files and run commands of their choice. The backdoor also enables attackers to funnel data from other servers through the router, turning the device into a covert proxy for concealing the true origin of malicious activity.

Black Lotus Labs

“This type of agent demonstrates that anyone with a router who uses the Internet can potentially be a target—and they can be used as proxy for another campaign—even if the entity that owns the router does not view themselves as an intelligence target,” researchers from security firm Lumen’s Black Lotus Labs wrote. “We suspect that threat actors are going to continue to utilize multiple compromised assets in conjunction with one another to avoid detection.”

The researchers said the campaign, dubbed Hiatus, has been operating since at least last July. So far, it has primarily hit end-of-life DrayTek Vigor models 2960 and 3900 running an i386 architecture. These high-bandwidth routers support virtual private network connections for hundreds of remote workers. To date, roughly 100 routers have been infected, which is about 2 percent of the DrayTek 2960 and 3900 routers exposed to the Internet. The researchers suspect the unknown threat actor behind Hiatus is deliberately keeping its footprint small to maintain the stealth of the operation.

Black Lotus still doesn’t know how devices are getting hacked

in the first place. Once and however that happens, the malware gets installed through a bash script that’s deployed post-exploitation. It downloads and installs the two main binaries.

Advertisement

The first is HiatusRAT. Once installed, it allows a remote threat actor to do things like run commands or new software on the device The RAT also comes with two unusual additional functions built in: (1) “convert the compromised machine into a covert proxy for the threat actor,” and (2) use an included packet-capture binary to “monitor router traffic on ports associated with email and file-transfer communications.”

The researchers suspect the threat actor included a SOCKS 5 software in function 1 was to obfuscate the origin of malicious traffic by proxying it through the infected router. Black Lotus researchers wrote:

> *The HiatusRAT tcp_forward function allows a threat actor to relay their beaconing from a separate infection through a compromised device before hitting an upstream C2 node. Conversely, they can also echo their command to a web shell from upstream infrastructure through the compromised router in the country of the targeted device, then interact with a more passive agent to obscure their true origination source by passing geo-fencing-based security measures.*

Black Lotus Labs

A tcpdump binary enabling packet capture was the engine behind function 2. It gave Hiatus the ability to monitor traffic on ports transmitting email and FTP communications from the adjacent LAN. It was preconfigured to work with the IMAP, POP, and SMTP email protocols.

Black Lotus Labs
Hiatus is mainly targeting DrayTek routers running an i386 architecture. The researchers, however, have uncovered prebuilt binaries compiled for ARM, MIPS64 big endian, and MIPS32 little endian platforms.

The packet-capture ability of the HiatusRAT should serve as a major wake-up call for anyone still sending email that isn’t encrypted. In recent years, email services have improved at automatically configuring accounts to use protocols such as SSL/TLS over port 993 or STARTTLS on port 143. Anyone still sending email in plaintext will likely regret it sooner rather than later.

It’s also a good idea to remember that routers are Internet-connected computers, and as such, they require regular attention to ensure updates and other measures, such as changing all default passwords, are adhered to. For businesses, it may also make sense to use dedicated router

monitoring.

https://arstechnica.com/?p=1922180