Backdoor infecting VPNs used “magic packets” for stealth and security



When threat actors use backdoor malware to gain access to a network, they want to make sure all their hard work can’t be leveraged by competing groups or detected by defenders. One countermeasure is to equip the backdoor with a passive agent that remains dormant until it receives what’s known in the business as a “magic packet.” On Thursday, researchers revealed that a never-before-seen backdoor that quietly took hold of dozens of enterprise VPNs running Juniper Network’s Junos OS has been doing just that.

J-Magic, the tracking name for the backdoor, goes one step further to prevent unauthorized access. After receiving a magic packet hidden in the normal flow of TCP traffic, it relays a challenge to the device that sent it. The challenge comes in the form of a string of text that’s encrypted using the public portion of an RSA key. The initiating party must

then respond with the corresponding plaintext, proving it has access to the secret key.

Open sesame

The lightweight backdoor is also notable because it resided only in memory, a trait that makes detection harder for defenders. The combination prompted researchers at Lumin Technology's Black Lotus Lab to sit up and take notice.

"While this is not the first discovery of magic packet malware, there have only been a handful of campaigns in recent years," the researchers wrote. "The combination of targeting Junos OS routers that serve as a VPN gateway and deploying a passive listening in-memory only agent, makes this an interesting confluence of tradecraft worthy of further observation."

The researchers found J-Magic on VirusTotal and determined that it had run inside the networks of 36 organizations. They still don't know how the backdoor got installed. Here's how the magic packet worked:

The passive agent is deployed to quietly observe all TCP traffic sent to the device. It discreetly analyzes the incoming packets and watches for one of five specific sets of data contained in them. The conditions are obscure enough to blend in with the normal flow of traffic that network defense products won't detect a threat. At the same time, they're unusual enough that they're not likely to be found in normal traffic.

https://arstechnica.com/security/2025/01/backdoor-infecting-vpns-used-magic-packets-for-stealth-and-security/