Custom Chinese Malware Found on SonicWall Appliance



Google-owned cybersecurity firm Mandiant reported on Wednesday that it has identified sophisticated malware believed to be of Chinese origin on a SonicWall appliance.

The malware, apparently deployed as part of a Chinese campaign, was analyzed by Mandiant and SonicWall's Product Security and Incident Response Team (PSIRT). The researchers found that the attacker had created a series of bash scripts and a TinyShell variant in the form of an ELF binary.

The custom-built malware allows the attackers to steal credentials – this appears to be its main purpose – and provides shell access. The hackers apparently targeted hashed credentials for all logged-in users.

According to Mandiant, the malware "is well tailored to the system to provide stability and persistence", being able to persist even across firmware upgrades.

The malware was spotted on an unpatched SonicWall Secure Mobile Access (SMA) appliance, but it's unclear how the attackers gained initial access. Mandiant suggested that the hackers may have exploited a known vulnerability that the targeted SonicWall customer neglected to patch.

It's not uncommon for threat actors to target known and even zero-day vulnerabilities in SonicWall appliances in their attacks.

Mandiant believes the malware was likely deployed on the device in 2021, but the attacker managed to maintain access by modifying firmware updates in a way that ensured the malware's persistence.

The security firm is aware of another Chinese threat actor using similar techniques, but it has decided to track the threats separately. The new group is currently tracked by Mandiant as UNC4540.

SonicWall announced this week that it has released an update for SMA 100 series devices (10.2.1.7), which "includes several key security features that protect the operating system from potential attack".

Related: SonicWall Zero-Day Exploited by Ransomware Group Before It Was Patched

Related: Three Zero-Day Flaws in SonicWall Email Security Product Exploited in Attacks

Related: SonicWall Patches SMA Zero-Day Vulnerability Exploited in Attacks

Custom Chinese Malware Found on SonicWall Appliance