New malware hides as legit nginx process on e-commerce servers

Ecommerce servers are being targeted with remote access malware that hides on Nginx servers in a way that makes it virtually invisible to security solutions.

The threat received the name NginRAT, a combination of the application it targets and the remote access capabilities it provides and is being used in server-side attacks to steal payment card data from online stores.

Testing Phone-Sized Faraday Bags

Back in the not-so-distant past, if you were patient and knowledgeable enough, you could reverse engineer the behavior of almost any electronic device simply by inspecting it carefully and understanding the circuitry. But those days are rapidly ending. Today, virtually every aspect of complex electronic hardware is controlled by microprocessors and software, and while that's generally good news for functionality, it's also bad news for security (and for having any chance of being sure what, exactly, your gadgets are doing, for that matter). For devices like smartphones, software runs almost every aspect of the user interface, including how and when it's powered on and off, and, for that matter, what being "off" actually means.

Complex software is, to put it mildly, hard to get right (for details, see almost any other posting on this or any other security blog). Especially for gadgets that are rich with microphones, cameras, location and environmental sensors, and communication links (such as, you know, smartphones), errors and security vulnerabilities in the software that controls them can have serious privacy implications.
The difficulty of reliably turning software-based devices completely off is no longer merely a hypothetical issue. Some vendors have even recognized it as a marketable feature. For example, certain Apple iPhones will continue to transmit "Find My Device" tracking beacons even after they've ostensibly been powered off. Misbehaving or malicious software could enable similar behavior even on devices that don't "officially" support it, creating the potential for malware that turns your phone into a permanently on surreptitious tracking device, no matter whether you think you've turned it off. Compounding these risks are the non-removable batteries used in many of the latest smartphones.

- **Netgear router vulnerabilities affecting SME products fixed ? The Register** [4]

  Two arbitrary code execution vulnerabilities affecting a number of Netgear routers aimed at small businesses have been patched following research by Immersive Labs.

  The vulns rely on authenticated access to affected devices so aren't an immediate threat. They do, however, allow someone with remote access to the router to pwn the device's underlying OS, threatening the security of data passing through the router.

  Helpfully, Netgear itself publishes default login credentials for "most" of its products on its website. If you haven't been into your Netgear router's admin panel and changed these default creds, you're at increased risk.

- **Netgear vulnerabilities could put small business routers at risk** [5]

  Netgear has released a set of updated firmware for multiple devices to resolve a number of security vulnerabilities responsibly disclosed by researchers at Immersive Labs. These could lead to unauthorized access to devices or modification of the internal filesystem that can be abused to affect traffic passing through the device.

**Security**

Source URL: [http://www.tuxmachines.org/node/158703](http://www.tuxmachines.org/node/158703)

Links: