Technology

Raspberry Pi used to steal data from Nasa lab

24 June 2019

REUTERS

A tiny Raspberry Pi computer has been used to steal data from Nasa's Jet Propulsion Laboratory, the space agency has revealed.

An audit report reveals the gadget was used to take about 500MB of data.

It said two of the files that were taken dealt with the international transfer of restricted military and space technology.

The attacker who used the device to hack the network went undetected for about 10 months.

Remote rover

The malicious hacker won access to the Jet Propulsion Lab internal network via the Raspberry Pi by hijacking its user account.

Although the Pi had been attached to the network by the employee, lax controls over logging meant Nasa administrators did not know it was present, said the report.

This oversight left the vulnerable device unmonitored on the network, allowing the attacker to take control of it and use it to steal data.

- **Nasa to open International Space Station to tourists**
- **Raspberry Pi opens first High Street store in Cambridge**
- **Raspberry Pi scores UK's top engineering award**

The Raspberry Pi is a credit-card sized computer that costs about $30 (£24). It has found a role in many computer education initiatives and is also a popular choice for small-scale computing projects because it is tiny and easy to use.

Once the attacker had won access, they then moved around the internal network by taking advantage of weak internal security controls that should have made it impossible to jump between different departmental systems.

The attacker has not been identified or caught.

The stolen data came from 23 files, but little detail was given about the type of information that went astray.

The audit process revealed several other devices on the JPL network that system administrators did not know about. None of these other devices was believed to be malicious.

"It's extremely hard for large, complex organisations such as Nasa to be perfect in maintaining full visibility and control of all their devices." said Nik Whitfield, head of security company Panaseer. "Typically this is because they depend on manual processes and human beings to continually inventory all devices connected to the network and the specific vulnerabilities they suffer."

When the breach became known about within Nasa, it prompted some parts of the agency, including the Johnson Space Center, to stop using a core gateway that gave employees and contractors access to its other labs and locations.

This was done because it was feared the attacker could exploit their widespread access to get at flight systems controlling currently active spacecraft.

The audit report recommended that Nasa do a better job of monitoring its network and tighten up its hack attack policies.

Based in California, the JPL is Nasa's main location for building and running the agency's collection of robotic spacecraft including its planetary rovers.

Related Topics

Cyber-attacks **United States** **Nasa** **California**

Share this story About sharing

More on this story

European Space Agency probe to intercept a comet
19 June 2019

US detects huge meteor explosion
18 March 2019

Computing in schools in 'steep decline'
8 May 2019

More Videos from the BBC