Spy agencies ban Lenovo PCs on security concerns

PUBLISHED: 26 Jul 2013 PRINT EDITION: 27 Jul 2013

Since acquiring IBM’s PC division, Lenovo has traded top spots with HP in terms of global market share, however their computers have been banned from the “secret” and ‘‘top secret” networks of the intelligence and defence services of Australia, the US, Britain, Canada, and New Zealand due to security concerns. **Photo: Bloomberg**

Christopher Joye, Paul Smith and John Kerin

Computers manufactured by the world’s biggest personal computer maker, Lenovo, have been banned from the “secret” and ‘‘top secret” networks of the intelligence and defence services of Australia, the US, Britain, Canada, and New Zealand, because of concerns they are vulnerable to being hacked.

Multiple intelligence and defence sources in Britain and Australia confirmed there is a written ban on computers made by the Chinese company being used in “classified” networks.

The ban was introduced in the mid-2000s after intensive laboratory testing of its equipment allegedly documented “back-door” hardware and “firmware” vulnerabilities in Lenovo chips. A Department of Defence spokesman confirmed Lenovo products have never been accredited for Australia’s secret or top secret networks.

The classified ban highlights concerns about security threats posed by “malicious circuits” and insecure firmware in chips produced in China by companies with close government ties. Firmware is the interface between a computer’s hardware and its operating system.

Lenovo, which is headquartered in Beijing, acquired IBM’s PC business in 2005.

IBM continues to sell servers and mainframes that are accredited for secret and top-secret networks. A Defence spokesman said Lenovo had never sought accreditation.

The Chinese Academy of Sciences, a government entity, owns 38 per cent of Legend Holdings, which in turn owns 34 per cent of Lenovo and is its largest shareholder.

Malicious modifications to Lenovo’s circuitry

AFR Weekend has been told British intelligence agencies’ laboratories took a lead role in the research into

Lenovo’s products.

Members of the British and Australian defence and intelligence communities say that malicious modifications to Lenovo’s circuitry – beyond more typical vulnerabilities or “zero-days” in its software – were discovered that could allow people to remotely access devices without the users’ knowledge. The alleged presence of these hardware “back doors” remains highly classified.

In a statement, Lenovo said it was unaware of the ban. The company said its “products have been found time and time again to be reliable and secure by our enterprise and public sector customers and we always welcome their engagement to ensure we are meeting their security needs”.

Lenovo remains a significant supplier of computers for “unclassified” government networks across western nations, including Australia and New Zealand’s defence departments.

A technology expert at the Washington-based Brookings Institution, Professor John Villasenor, said the globalisation of the semi-conductor market has “made it not only possible but inevitable that chips that have been intentionally and maliciously altered to contain hidden ‘Trojan’ circuitry will be inserted into the supply chain.

“These Trojan circuits can then be triggered months or years later to launch attacks,” he said.

Hardware back doors can be very hard to detect

IT security industry analyst at tech research firm IBRS, James Turner, said hardware back doors are very hard to detect if well designed.

They were often created to look like a minor design or manufacturing fault, he said. To avoid detection, they are left latent until activated by a remote transmission.

“Most organisations do not have the resources to detect this style of infiltration. It takes a highly specialised laboratory to run a battery of tests to truly put hardware and software through its paces,” Mr Turner said. “The fact that Lenovo kit is barred from classified networks is significant, and something the private sector should look at closely.”

Professor Villasenor said malicious circuitry known as “kill-switches” can be used to stop devices working and to establish back doors. French defence contractors reportedly installed kill-switches into chips that can be remotely tripped if their products fall into the wrong hands.

AFR Weekend has been told the electronic eavesdropping arms of the “five eyes” western intelligence alliance, including the National Security Agency in the US, GCHQ in the UK, and the Defence Signals Directorate in Australia, have physically connected parts of their secret and top secret computer networks to allow direct communications between them. This means that security bans on the use of products within the secret networks are normally implemented across all five nations. Two commonly used suppliers are Dell and Hewlett-Packard.

The ban on Lenovo computers also applies to Britain’s domestic and foreign security services, MI5 and MI6, and their domestic equivalents: the Australian Security Intelligence Organisation and the Australian Secret Intelligence Service.

Not connected with foreign counterparts

In contrast to the other agencies, ASIO’s top secret network, called “TSNet”, is compartmentalised and not connected with foreign counterparts because of its counter-intelligence role.

All these secret-level defence and intelligence networks are “air-gapped”, which means they are physically separated from the internet to minimise security risks. ASIO, ASIS, and DSD are colloquially known as Channel 10, The Other DFAT and The Factory. An academic expert on computer hardware implants, Professor Farinaz Koushanfar at Rice University’s Adaptive Computing and Embedded Systems Lab, said the NSA was “incredibly concerned about state-sponsored malicious circuitry and the counterfeit circuitry found on a widespread basis in

US defence systems”.

“I’ve personally met with people inside the NSA who have told me that they’ve been working on numerous real-world cases of malicious implants for years,” she said.

“But these are all highly classified programs.”

Australia’s defence department runs three networks managed by the Chief Information Officer Group: the Defence Restricted Network; the Defence Secret Network; and the Top Secret Network.

The DRN is not classified and is linked to the internet via secure gateways. The DSN and TSN are air-gapped and off limits to Lenovo devices. An official with clearance to access all three networks can switch between them using a diode, called the Interactive Link, connected to a single computer. Previously officials used multiple desktops connected to individual networks.

Anti-China trade sentiment

In 2006 it was disclosed that the US State Department had decided not to use 16,000 new Lenovo computers on classified networks because of security concerns.

The change in procurement policy was attributed to anti-China trade sentiment after Lenovo’s acquisition of IBM’s PC business.

Some experts argue that blocking specific companies from classified networks is not a panacea for security threats given the global nature of supply chains.

Many western vendors have semiconductor fabrication plants, or “foundries”, based in China, which exposes them to the risk of interference.

Huawei Technologies made the same argument in response to the Australian government’s decision to exclude it from the National Broadband Network. Huawei says a better approach would be to evaluate all products in a single forum overseen by security agencies.

The Lenovo revelations follow allegations in The Australian Financial Review last week by the former head of the CIA and NSA, Michael Hayden, that Huawei spies for the Chinese government. Huawei officials and China’s Australian embassy strenuously denied these claims.

READ NEXT:

- **Hacking the hardware**
- **Lenovo shares jump after surge in earnings**
- **Huawei spies for China, says ex-CIA head**
- **China denies Huawei spied for state**
- **Interview with former CIA, NSA chief Michael Hayden**

The Australian Financial Review