

**Researchers find Malay-language GE13 document with spyware, says report
Malaysian Insider
May 3, 2013
By Jahabar Sadiq**

KUALA LUMPUR, May 3 — Computer spyware was found recently in a Bahasa Malaysia Microsoft Word document that purportedly discusses Election 2013 candidates, according to IT security researchers Citizen Lab.

In the “For Their Eyes Only” report released on May 1, the University of Toronto’s Citizen Lab said the word document installs FinSpy spyware that masquerades as Mozilla’s Firefox browser on the computers of those who open the file.

“While we cannot make definitive statements about the actors behind the booby-trapped candidate list, the contents of the document suggest that the campaign targets Malay speakers who are interested in Malaysia’s hotly contested 5 May 2013 General Elections,” the report said.

“This strongly suggests that the targets are Malaysians either within Malaysia or abroad,” it added.

The report comes at a time when election watchdogs and opposition parties claim there has been a mass movement of dubious voters and indelible ink that can be washed off in the May 5 polls. The authorities and the caretaker Barisan Nasional (BN) government have denied all claims.

There have also been reports of distributed denial of service (DDoS) attacks on several news portals including The Malaysian Insider while access restrictions have been reported by several websites but denied by the authorities just days before the tightest electoral race in Malaysian history.

The spyware masquerades as Mozilla’s Firefox browser, say the researchers. — Reuters pic “We trust that both domestic and international elections monitoring officials and watchdog groups will investigate to determine whether the integrity of the campaign and electoral process may have been compromised,” said the researchers.

They said the booby-trapped Bahasa document was found after the Malaysian Communications and Multimedia Commission (MCMC) accused The Malaysian Insider of “false reporting” a New York Times article on its earlier research about the spyware.

“After the Malaysian Government’s accusation, we discovered a booby-trapped document that contained a candidate list for the 5 May 2013 Malaysian General Elections,” the report said, adding it was titled “SENARAI CADANGAN CALON PRU KE-13 MENGIKUT NEGERI.”

“When a victim opens this document and sees the list of candidates, their computer is infected with FinSpy,” it added.

Computer experts say when recipients download the infected file, the data on the computer became accessible to an external user as well as the ability to watch and listen to the computer's user through the machine's camera and microphone.

Citizen Lab found that FinSpy "is being used in a number of countries with poor human rights records and has been used to target activists."

FinSpy is owned by the UK's Gamma Group, and media reports say the firm has received a letter from Mozilla asking the company to stop disguising its product as Firefox.

Citizen Lab reports that FinSpy doesn't just make itself look like Firefox; it actually "makes use of Mozilla's trademark and code."

The report, which documents the spread of offensive computer network intrusion capabilities, hacking tools marketed by Western companies, also said that this behaviour has been documented previously in files targeting Bahraini activists.

The country's 13th general election has become a hotly-contested affair with all 222 federal and 505 state seats up for grabs for the first time in history. Several international agencies and regional media are closely watching the May 5 polls ahead of other elections in the region.

Hakcipta © 2013 The Malaysian Insider

Source:

<http://www.themalaysianinsider.com/malaysia/article/researchers-find-malay-language-ge13-document-with-spyware-says-report/>