Microsoft said on Thursday that a security vulnerability in its Internet Explorer browser was used in cyberattacks that prompted Google to threaten to shut down its operations in China.

Meanwhile, Web security firm MaAfee Inc said the attacks on Google and other companies showed a level of sophistication beyond that of cyber criminals and more typical of a nation-state.

Revealing the attacks on Tuesday, Google said they originated from China and targeted the e-mail accounts of Chinese human rights activists around the world, but did not explicitly accuse the Chinese government of responsibility.

Dmitri Alperovitch, vice president of threat research for McAfee, said that while McAfee had “no proof that the Chinese are behind this particular attack, I think there are indications though that a nation-state is behind it.”

Google said more than 20 other unidentified firms were targeted in the “highly sophisticated” attacks. while other reports have put the number of companies attacked at more than 30.

Google said that following the attacks it had decided to no longer censor its Internet search engine in China and was prepared to close its operations there entirely if it could not reach an agreement with the Chinese authorities.

Only one other company, Adobe, has come forward so far and acknowledged that it was a target of the attacks, which exploited a previously unknown security flaw in Internet Explorer.

“Internet Explorer was one of the vectors used in targeted and sophisticated attacks targeted against Google and other corporate networks,” Mike Reavey, the director of Microsoft’s Security Response Center, said in a blog post on Thursday.

Reavey stressed that Microsoft “has not seen widespread customer impact, rather only targeted and limited attacks exploiting [Internet Explorer 6.]”

Changing security settings to “high” would protect users from the vulnerability, he said.

Microsoft chief executive Steve Ballmer said meanwhile that the US software giant takes cyberattacks “seriously” but has no plans to pull out of China.

“We’ve been quite clear that we’re going to operate in China,” Ballmer told CNBC television. “We’re going to abide by the law.”

“We need to take all cyberattacks seriously, not just this one,” he said.

Alperovitch said the attacks on Google and other companies, which he was not allowed to identify, were unusual in their sophistication.

"We have seen attacks like this before but only in the government space, in the defense-industrial space," Alperovitch said. "We have never seen that level of sophistication, level of planning and reconnaissance and attention to detail in attacks on commercial entities. Primarily the threat to commercial entities is from cyber-crime individuals after financial data. They're typically sloppy."

"This exploit was highly sophisticated," he said. "It used multiple levels of obfuscation and encryption, more so than in any other types of exploits that we have seen previously."

Such sophistication is "typically an attribute of a nation-state type of attack — and that's exactly what we see here," the McAfee researcher said.

Alperovitch said that the attackers used e-mail or some other lure to get employees of a targeted company to click on a link and visit a specially crafted Web site using Internet Explorer.

"Malware would then be downloaded that has the capability to essentially install a 'back door' in the machine," he said. "This allows the attacker to log into the machine and essentially take it over as if they were sitting at the keyboard manipulating that machine."

"What that does is it gives the attacker a beachhead into the organization from which point they can start exploring, identifying valuable pieces of data and other vulnerable services," he said.

Source: Taipei Times 2010/01/16