Vietnamese hackers trigger software trap after Australian sale of newspaper in Cambodia

By Liam Cochrane

Published: 2018-05-15 · Archived: 2026-04-06 00:51:04 UTC

A Vietnamese state-linked hacking group has used a Cambodian newspaper website to attack a local human rights organisation, according to a leading cyber security firm.

The attack started just days after Australian mining magnate Bill Clough sold the newspaper to Malaysian spin doctor Sivakumar Ganapathy, who specialises in "covert PR".

"Since last Tuesday [May 8], computers in our office were targeted by a malicious piece of code when we visited the Phnom Penh Post website," said Naly Pilorge, director of Licadho — one of Cambodia's leading human rights groups.

"We have taken precautions to defeat the targeted attack," Ms Pilorge told the ABC.

(L-R) West Australian mining magnate and former owner of the Phnom Penh Post, Bill Clough, with then editor-in-chief Kay Kimsong and finance director Heang Tangmeng. *(Supplied: Facebook)*

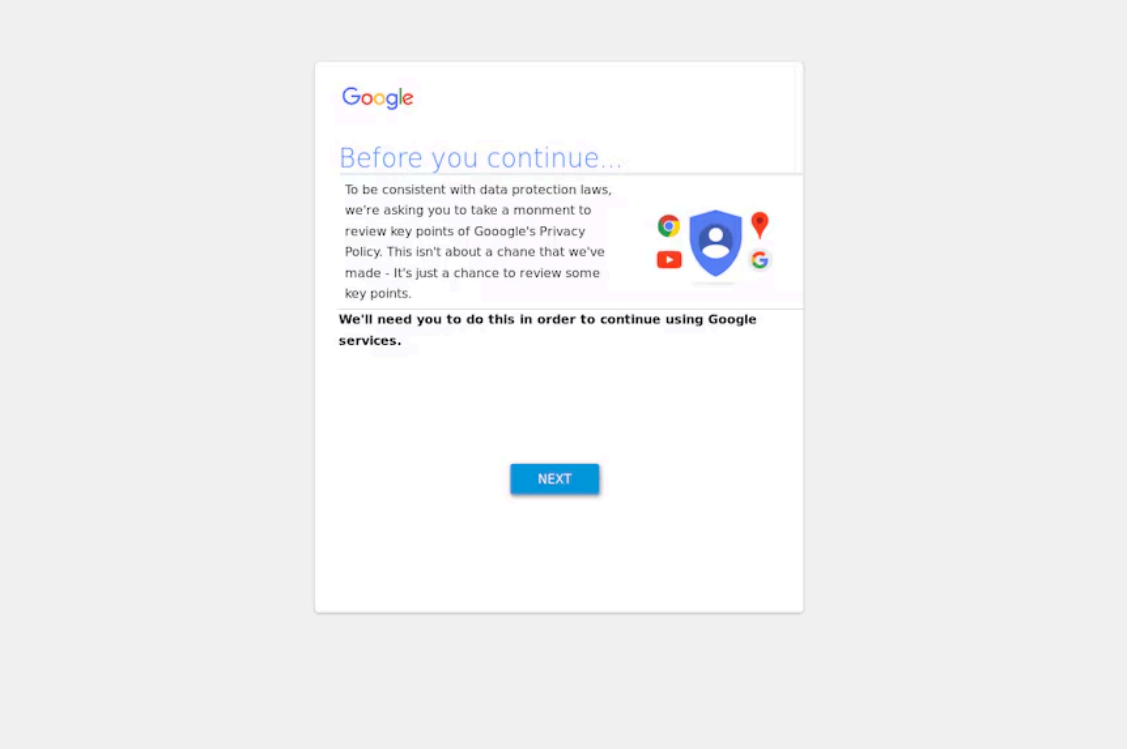
So-called "watering hole" attacks use popular websites to select targets and then direct specific malware attacks at them.

Licadho staff visiting the site are redirected to a fake Google page about privacy and then to a page called GTransfer which asks for permission to "read, send, delete and manage your email" and "view your contacts".

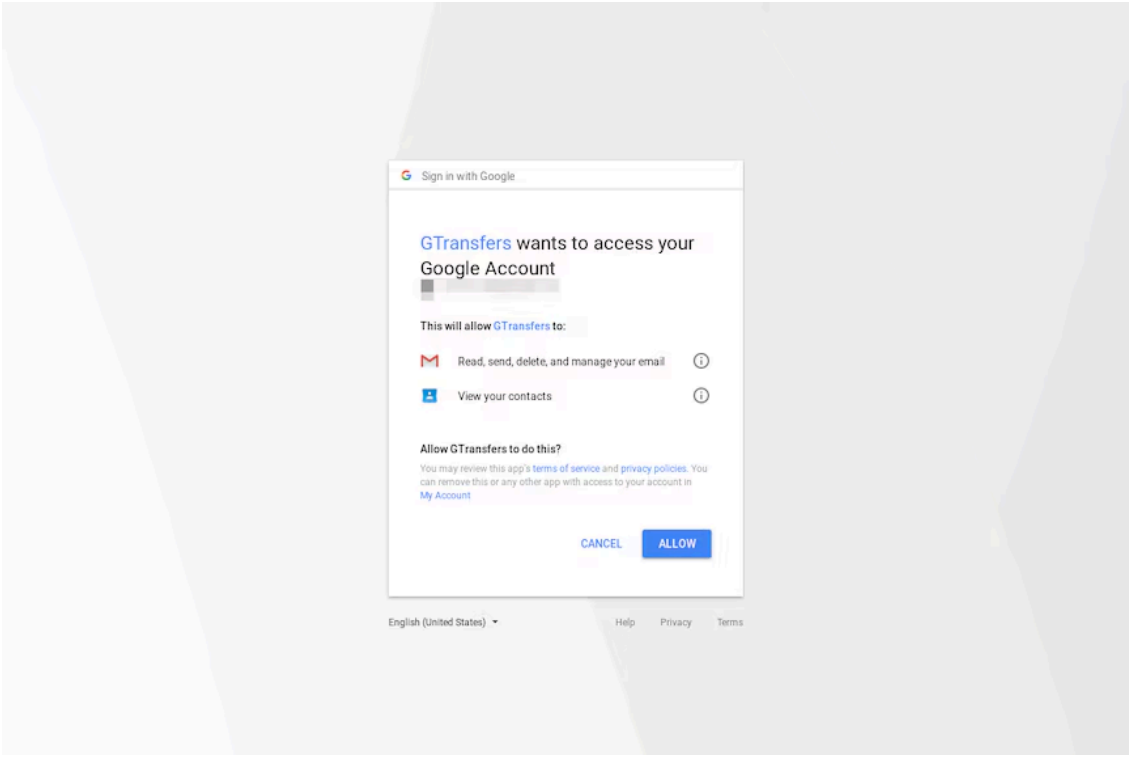
As of Tuesday afternoon, the attack attempts were still happening for Licadho staff.

"In this instance we're pretty confident that this is being carried out by a group we track as APT32," said Ben Wilson, a Canberra-based threat intelligence analyst with cyber security firm FireEye.

"They are what we believe to be a Vietnam-based nation state group that are acting in the interests of Vietnam's political interests," Mr Wilson told the ABC.



First the attack tricks users into providing their Google account data. *(ABC News)*



Then it asks whether you will allow GTransfer access to your Google account. *(ABC News)*

APT32 has targeted foreign governments, as well as Vietnamese dissidents and journalists for at least five years.

Since 2014, FireEye has observed APT32 targeting foreign corporations with a vested interest in Vietnam's manufacturing, consumer products and hospitality sectors.

This particular malware campaign by APT32 is believed to have started in late 2016 and is the first state-linked hacking outfit identified by FireEye that is not Chinese or Russian.

"This kind of selective targeting allows the actors to stay under the radar a bit longer, you're less likely to tip off someone [than] if they're just redirecting all visitors to these websites to a malicious location," said Mr Wilson.

FireEye first detected the Phnom Penh Post had been compromised in November 2017.

Using Wayback Machine — a research tool that allows a snapshot of webpages as they existed on certain dates — it is clear that malicious 'eval()' code used to trigger the targeted attack was added to the Phnom Penh Post website on or around May 8.

Malware attack comes ahead of national election

Calls to six different numbers listed on the Phnom Penh Post website went unanswered on Tuesday.

The ABC has contacted Sivakumar Ganapathy via his company Asia PR, and his lawyer Ly Tayseng, but there was no response at time of publication.

Sivakumar Ganapathy (right) with Philip Mills who heads AsiaPR's presence in Phnom Penh. *(Facebook)*

Negotiations between Bill Clough and Sivakumar Ganapathy over the sale of the newspaper were already underway in November 2017, when early stages of the malware were detected.

The ABC has no evidence the former or current owners of the Post were aware of the malicious software implanted into the paper's website.

A spokesman for the Vietnamese Government had not responded at time of publication, but Hanoi has previously denied similar allegations.

In a New York Times story about cyber-attacks in Asia and Europe, spokeswoman for the Vietnamese Foreign Ministry Le Thi Thu Hang called the findings of a previous FireEye report "groundless".

Vietnam "does not allow cyberattacks on organisations or individuals," she told the New York Times in May 2017.

Australian security researcher Troy Hunt said getting access to email is particularly valuable for hackers.

"It tends to be the skeleton key for all your other accounts, so if someone can get access to your email they usually have the ability to go through and reset passwords on other accounts," said Mr Hunt.

He said there were some obvious warning signs that GTransfer was bogus, including its website having the contact the email "some.email@somewhere.com".

"It certainly looks dodgy," said Mr Hunt.

The malware attack comes in the lead-up to a national election in Cambodia on 29 July.

Hun Sen — who was placed into power by Vietnam in the 1980s and has been Prime Minister for 33 years — has threatened civil war if his Cambodian People's Party is not re-elected.

On Hun Sen's request, courts have outlawed the main opposition party, locked up its leader on treason charges and banned 118 opposition MPs from politics for five years.

The increasingly-authoritarian leader has also attacked the media.

Both the Phnom Penh Post and The Cambodia Daily were hit with multi-million-dollar tax bills.

The Daily was forced to close last year, and the Post's sale earlier this month was immediately followed by editorial interference by the new Malaysian owner and the departure of 14 staff.

Crucially, for Cambodia's mostly-rural population with low literacy, Hun Sen closed down 32 radio frequencies which broadcast independent news.

Disclosure: Liam Cochrane worked at the Phnom Penh Post as a journalist in 2004 and as the managing editor in 2005.
