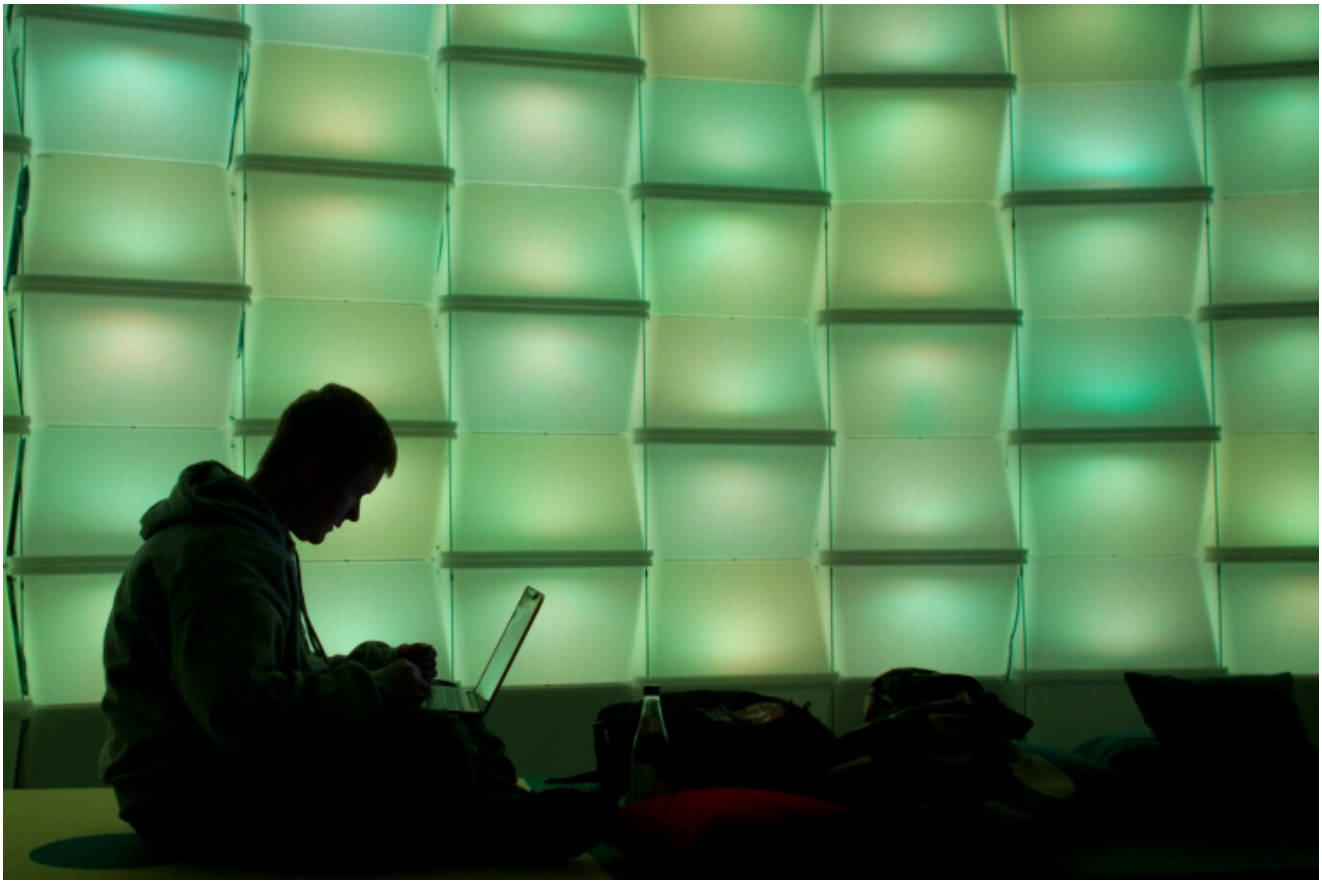
How Vietnam-based hacking operation OceanLotus targets journalists

cpj.org/2021/02/vietnam-based-hacking-oceanlotus-targets-journalists

February 1, 2021



A woman is pictured using a computer at a conference in Berlin, Germany on December 27, 2010. Vietnam-based hacking operation OceanLotus has targeted journalists in Germany. (Reuters/Thomas Peter)

Features & Analysis

By Madeline Earp/Consultant Technology Editor on February 1, 2021 4:52 PM EST

In early 2020, Vietnamese writer Bui Thanh Hieu told Marina Mai, a freelancer based in Berlin, that he was closing his blog to protect his family. In 2009, Hieu was detained for a week for his critical writing on Vietnam's territorial disputes with China, as CPJ documented. In 2013, he fled to Germany, but continued writing about Vietnamese politics on his popular blog *Nguoi Buon Gio* (*The Wind Trader*) and on Facebook, he told Mai in an interview for the Berlin-based daily *taz.* He went on to face hacking attacks, repeated attempts to have Facebook disable his account, and even sought protection from German police following threats related to his work, according to the interview. Eventually, he felt he had no choice but to shut the site.

What Mai didn't know at the time was that her subject had fallen victim to a massive hacking and surveillance operation known as OceanLotus, which experts say targets people who have criticized the Vietnamese state – and which would come to target her as well. Mai, who has not been back to her home country in several years, still writes about Vietnam, as well as the Vietnamese diaspora in Germany, and local issues in Berlin. She told CPJ in an email in late 2020 that she learned she was a target when German journalists informed her of an attempt to install spyware on her computer.

"I didn't think I'd be an interesting person for the Vietnamese secret service, because I only write in German," she told CPJ. "I had to correct this opinion."

Steven Adair, president and co-founder of Volexity, a U.S.-based cybersecurity company that has studied OceanLotus, spoke to CPJ by phone in late 2020 about how the group identifies and targets journalists.The method used in the separateattacks on Mai and Hieu, known as spear phishing, is familiar to many journalists. Mai told CPJ she was targeted via an email that appeared to be legitimate but contained malware; German journalists reported that the same method was used against Hieu in an October 2020 article published by *Die Zeit* newspaper and public service broadcaster BR. (Hieu initially agreed to an interview when CPJ reached him via messaging app in late 2020, but later said he was too busy to respond.)

OceanLotus also creates fictitious news websites and social media profiles to lure its target audience, according to Adair; in December, Facebook said it had traced malicious activity by the same actors to an IT company in Vietnam. Adair shared more insights into the group with CPJ below. His answers have been edited for length and clarity.

Tell us about your work on OceanLotus so far.

In 2017, we released research about a large digital surveillance campaign called OceanLotus or APT32, a cyber-threat actor or group of hackers. There was no attribution to a country, but [Silicon Valley-headquartered cybersecurity firm] FireEye and the EFF [U.S. digital rights group the Electronic Frontier Foundation] had some reporting that clearly showed OceanLotus was out of Vietnam, and was spear phishing dissidents.

Then we happened to come across some weird code on Cambodian government websites that had been compromised. It was profiling visitors, collecting information about them. We eventually uncovered that in over 100 different websites for the Philippine military, Laotian websites, Cambodian media websites – all countries surrounding Vietnam.

We uncovered this huge set of stuff going on, including phishing attacks, and some of the malware we could clearly tie back to OceanLotus. Once they have access to your inbox, they can pretend to be you or anyone that's ever emailed you.

They also [create] fake sites – a lot of them are news websites. None of them are going to leapfrog CNN with millions of views a day, but they have news constantly updating, or they advertise somewhere. Some of the pages never really caught on, but one had over 20,000 [social media] followers. That's a decent number for a completely fraudulent website whose purpose is inarguably to track and target visitors.

The majority [of targets] ended up being human rights defenders like the [Germany-based] VETO! Human Rights Defenders Network, media organizations in the United States, and Vietnamese Catholicism related websites…groups whose mission is offensive to the Vietnamese government. A lot of them were media websites or blogs that expose corruption.

Is it possible to say whether state actors are behind OceanLotus?

We definitely believe it's out of Vietnam, but whether it's a government agency, a contractor working for them, or something else, we don't claim that we know that.

We look at the immense level of effort and resources to maintain all the infrastructure and identify the victims. It's not something anyone's going to do in their spare time.

When you look at the 2017 campaign, they're hacking 120 sites and 90 of them are media and human rights organizations— from our perspective, there's no other explanation.

[Editor's note: CPJ requested comment from the Vietnamese embassy in Berlin via an email address listed on its website, but did not receive a reply. Phone calls to a number on Hanoi's Ministry of Public Security website rang unanswered.]

What are the risks of visiting a malicious website set up by hackers?

These websites have real news on them, and one or two pages out of maybe 5,000 would deliver malware. Theoretically, someone could end up on that [by mistake], but we surmise that they probably deliver links in a targeted fashion through direct messages or email.

Or, if they had designated you as a target and had identified your IP address, then the website would behave differently, either present malware to download or redirect you to a login page to steal your password or the Google OAuth credentials that you use to authorize an application.

There's no vulnerability in a browser that means you could visit a website [from your home] and they would know who you are. But if you're in a corporate office, it may be possible to identify that you're tied to an organization on the target list. With one organization that we worked with, we could visit a site and nothing much happened. But from an IP address tied to that organization, the same website would behave differently.

The main way they can profile you is by looking at what you do. The system can tell that you're Person A who visited this blog. Maybe you visit a second time, maybe you also start showing up on this other news website dedicated to dissidents. They can track language settings, where you came from, enough to say, "That's probably an activist or someone who is interested in activists." It's quite an operation.

One of the websites that we found was compromised related to the Taiwanese steel plant that spilled a bunch of chemicals in the river. The site had been running for several years, saying, "Get this company out of Vietnam." It was actually run by OceanLotus.

[Editor's note: In 2016, a Taiwanese firm that operated a steel plant in Vietnam agreed to pay millions of dollars in damages for a toxic waste spill, according to The Guardian. The incident became a flashpoint for protests and the government cracked down on news coverage, imprisoning at least one journalist as a result, according to CPJ research.]

***Die Zeit* and BR reported that the hackers used a tool called Cobalt Strike. What is that?**

Cobalt Strike is a penetration testing tool. I don't know who their customers are, but it's sold to a lot of companies that use it legitimately. They hire someone to break in and test their security, and that's a toolkit they can use.

I don't suspect that OceanLotus is a customer of Cobalt Strike. We don't know how it happens, but cracked versions get out there. Maybe someone stole it through hacking or after signing up as a customer, but it means multiple people can use an unsupported, illegitimate version without paying for it, and it gives them the capability to take control of a system. That's not because of an irresponsible action from the company, as far as we know — it's not in the same category as companies that are purveying malware to governments.

There's not a specific solution – hackers must be having success with it, or they wouldn't keep using it. But if it's not that tool, it's going to be another. Anti-virus [software] is more likely to pick up something like that, which is a known, older technology and not being updated – though we don't know how many of the kinds of people being targeted have anti-virus.

In the case of OceanLotus, it's interesting that they use it at all. They also have a significant amount of malware developed in-house and a pretty strong capability to attack across different platforms. But they continue to use it, they've been using it for years.

CPJ's Digital Safety Kit, in six languages, has more information on phishing.

Attila Mong, CPJ's EU correspondent, contributed reporting from Berlin.

Madeline Earp is a consultant technology editor for CPJ. She has edited digital security and rights research for projects including five editions of Freedom House's *Freedom on the Net* report, and is a former CPJ Asia researcher.