Lined up in the sights of Vietnamese hackers

By BR Data

Archived: 2026-04-05 23:46:22 UTC

08.10.2020 00:10

There is no safe place

A group of Vietnamese hackers has been systematically spying on dissidents for years, including in Germany. The victims feel left alone by authorities as an investigation by BR and Zeit Online is able to show.

Die deutsche Version dieses Artikels finden Sie hier.

Bui Thanh Hieu had already paid the attendance fee of 200 euros when he heard a warning. He intended to give a speech at a conference near Stuttgart. However, then, he was given the following hint: The Vietnamese secret service might have infiltrated the event. Bui Thanh Hieu is one of the best known bloggers from Vietnam. Most people in Germany know Vietnam as a holiday destination with beautiful beaches and great food. Bui documents the other side: the one-party state that intimidates everyone voicing criticism. A state that tolerates corruption and arbitrariness of authorities.

For a population that knows of press freedom only by hearsay, he filmed police beating up protestors with batons. Due to his work, he was detained by the security forces “probably a dozen times”, as he said. In 2013 he fled to Germany, and ever since Bui Thanh Hieu has been living and working in Berlin. He has hundreds of thousands of followers on Facebook, where he calls himself “the wind trader”. Of course he wants to return home one day, “but there I would have to go back to prison”, he explained in an interview. He added that his parents were called upon by the police and insulted that they had not properly educated their child.

Hundreds of thousands of people fled the country after the end of the Vietnam War from the hunger and the terror of the communist regime. Since 2002, the members of an association of Vietnamese people living in exile have met every year, sometimes in France, sometimes in the USA and, in 2018, near Stuttgart. For four days, they want to discuss a better future for Vietnam. A future, where people with dissenting opinions do not end up in prisons, where sometimes they are tortured.

The hackers send an e-mail – laced with malware

As Bui received the warning, he cancelled his participation. He feared that he might be spied on and that the arm of the Vietnamese state might reach all the way to Germany. What he did not know, however, is that the hackers’ arm had already reached all the way to his mailbox.

Bui is cautious – he had been expecting hackers to target him for some time. But this time, they were well prepared: They apparently knew that he wanted to go to the meeting in Stuttgart – and that they could use that to bait him. Six weeks before the meeting, an invitation arrived in his mailbox. It was sent by the hackers – laced with malware. Bui clicked on the mail.

Spied on and left alone

It is this kind of targetting – meticulously prepared, sent in the right moment, executed in only two clicks – that can become very dangerous for dissidents. Months of research conducted by BR and Zeit Online show that there are numerous persons affected, among them opposition members and human rights activists. Many of these feel left alone in Germany. If they are lucky, information security specialists will contact them and notify them about their website having been hacked. German authorities, on the other hand, usually do not contact them. Research suggests that they are overwhelmed. There are hardly any established procedures to help dissidents in cases of cyber espionage.

Conversations with more than two dozen people – victims, investigators and Germany's top domestic intelligence chief – paint the picture of a group of hackers presumably acting in Vietnam's strategic interest. The research also shows that the hackers make mistakes. Therefore, the team of reporters succeeded in finding out which websites are used for distributing the malware. The hackers have been trying to spy on their victims for years.

The wind trader is concerned for his informants

Only two years later, in the summer of 2020, Bui learned in an interview with the reporters that hackers had sent him the e-mail with the conference invitation. His first concern was about his informants: "If my laptop contained malware, the Government would know who is providing me with this kind of information." This would also include people in the party and state apparatus. These people would be in jeopardy. An information security specialist agreed to scan his computer for malware. The team of reporters had established contact. It was important to Bui that this person had no affiliation to Vietnam, a precautionary measure.


The wind trader Bui Thanh Hieu – © Felix Burchardt for Zeit Online

The wind trader Bui Thanh Hieu – © Felix Burchardt for Zeit Online

Bui arrived at the meeting with a small delegation – as in almost every city in Germany, he also knows people in Berlin who help him. The sun was shining as he got out of the car of a supporter. His backpack read "Take it easy". Bui stuck to it, straightened his flat cap and lighted himself a cigarette. All the while one of his supporters organised someone able to translate the computer jargon into Vietnamese.

As Bui handed over the laptop and password, the expert assured him that no files would be copied, at least not without consultation. He said that he would be ready in approximately an hour. Bui is a man with reduced facial expression. In the course of two meetings, there was only one moment, where his feelings could be read off his face. Namely when he received the answer, whether hackers were spying on his computer.

Digital attacks leave traces behind

It can be difficult to find out who is behind a cyber attack. However, it is not impossible since digital attacks leave traces behind. In principle, these traces can be erased but information security specialists and intelligence services sometimes track the groups for years. And even hackers make mistakes.

In Bui's case the traces lead to a group presumably acting on behalf of the Vietnamese state. Experts have many names for this group: APT 32 and Ocean Lotus are best known. In conversations with a dozen of information security specialists, they all agreed that this is a Vietnamese group spying, in particular, on its own compatriots.

The team of reporters from BR and Zeit Online managed to confirm this statement by means of a technical investigation. The team found hundreds of infected computers hinting at who the hackers might be targeting in particular: Vietnamese citizens. Ocean Lotus has a well-filled digital tool box for placing malware. They also use creative means for retrieving data from the computers spied on.

A broad range of missions

Adam Meyers is Vice President of Intelligence with information security company Crowdstrike and has been monitoring the Vietnamese hacker group for years. "They have been active since 2012, hacking people living in China, Vietnam, Cambodia, the Philippines or Germany," he said. He added that the hackers were targeting the energy, financial, hotel and automotive industries, but also governments, media and human rights groups. "We are not talking about six people sitting in their mom's basement, but about a military unit. We are talking about the premier entity for CNO, computer network operations of a fully functioning nation-state, capable of fulfilling a broad range of missions". According to another IT security specialist – who does not want to be mentioned by name – Ocean Lotus is one of the "five most active groups worldwide".

We are talking about the digital attack group of a fully functioning nation-state,

Adam Meyers, IT-Sicherheitsexperte

There is no clear evidence that the Vietnamese state is giving orders to the group, but there are indications. When asked to comment, the Vietnamese embassy in Berlin vehemently denied that Vietnam is behind the cyber-attacks and rejected any such accusations: "Attacks and threats to cybersecurity must be condemned and severely punished in accordance with law". The embassy added that Vietnam was prepared to cooperate with the international community for preventing future attacks. However, a person who keeps an eye on states and their hackers for the German security authorities told the reporters from BR and Zeit Online: "A group hacking targets on this scale, in a country such as Vietnam – that is not possible without the approval of the state".

For a short moment, Bui Thanh Hieu, the wind trader, was astonished. After searching his computer for traces of hackers the information security specialist gave him an answer that surprised Bui. He listened intently to his translator. Every detail seemed to be important to him. He wanted to know whether he had to warn his contacts – and whether the security specialist had also checked his mailbox. He added that only a few months ago he had again found suspicious e-mails.

The expert did not find any malware. He seemed surprised, as though he had firmly expected to come across traces of the hackers. After all, Bui had emphasized that he had opened the mails and this should have been enough to allow them access to his computer. But there was nothing to be found. Perhaps the hackers had erased

their traces, the expert suspected. He added that he needed some more time for further analyses. Rather days than hours. For the moment, Bui was relieved.

Digital espionage is easy to deny

Bui slipped his virus-free laptop into his backpack and talked about his life in Germany: “I don’t know if it is safe here. In any case, it is a lot safer than in Vietnam. And if it is not safe in Germany, it is not safe anywhere.”

By now he knows that in 2019 alone, he received three e-mails from Ocean Lotus. Three more attempts to spy on his laptop. In these three cases, too, there were no traces left on his laptop. But these cases show that the hackers were reaching out for his secrets. Even if Bui should have been lucky so far, luck alone will not be enough to protect him permanently.

Cyber espionage enables states to spy on what they consider to be troublemakers across national borders. Instead of training agents who get on planes and then recruit people who place bugs in the executive floor unnoticed, it is sufficient to send a few bits through Internet lines. “You can do without the all-round monitoring,” said an information security specialist who hunts down government hackers. “You switch on the microphone on your mobile phone if you want to know what people are talking about.”

Another advantage is that cyber spies can deny their actions much more easily than classic agents. Classic agents cause international scandal if their actions become public, the way it happened in 2017. Ex-politician and businessman Trinh Xuan Thanh was strolling through the park Berliner Tiergarten with his girlfriend when presumably agents of the Vietnamese secret service jumped out of a van and dragged the two inside. With the kidnapping on German grounds, they not only broke international law but also the arm of Thanh’s lover. His smartphone shattered on the asphalt.

Trinh Xuan Thanh had left Vietnam after a power struggle within the party elite. He was hated in Vietnam, even among the population, who saw him as a corrupt politician who roamed the streets of Hanoi in a Lexus with a price tag of 250 000 dollars. Shortly after his kidnapping, he appeared on Vietnamese state television. He was sentenced in Hanoi – to die behind bars.

The price for this operation was probably very high, both financially and diplomatically. The relations between Vietnam and Germany were suspended.

In the digital world, such attacks attract less attention and the level of protection is not particularly high, said Matthias Schulze, who studies hacking incidents for the German think tank “Stiftung Wissenschaft und Politik” (Foundation for Political Science and Politics): “This leaves the door wide open for retrieving information in many places”. The situation is almost inviting states to set up hacking units. “It is worthwhile. The cost-benefit ratio is very good”.

The hackers want to come to Munich – to BMW

The hackers are relying on this, as emerged in spring 2019. Vietnam is currently building up its automotive industry. The engines are coming to Hanoi from BMW in Munich and the hackers to BMW from Hanoi. The attack lasted for months, as a BR investigation showed. But it was noticed before the hackers could intrude into

the networks in Munich and take away sensitive data. The suspicion of industrial espionage is, at least, highly probable. BMW has not made any public statements to this day.

Another technical analysis by BR and Zeit Online reveals how active the hackers are. Ocean Lotus may have made a mistake. Thanks to this, it is possible to see hundreds of websites set up by the hackers to spread their malware.

Berlin – "Capital of spies"

It is an inconspicuous office building in Berlin: drawn curtains, cool temperatures, security guards in well-fitting suits wearing headsets guarding the door. On the conference table, far too large for the interview, in the rooms of the Federal Office for the Protection of the Constitution (BfV), there was the only electronic device that the reporters from BR and Zeit Online did not have to lock up at the entrance. Thomas Haldenwang only wants to speak into microphones that are held to his mouth. Mobile phones and laptops stayed outside.

Germany's supreme security agent talked in a calm manner about intelligence services "which are much more robust than before". For decades, espionage stories were mainly seen in films, but now it is more and more often the reason for "incident-related meetings" in the relevant working group in the Joint Extremism and Terrorism Defence Centre (Gemeinsames Extremismus- und Terrorabwehrzentrum, GETZ).

Haldenwang recently declared Berlin to be "capital of spies". In an interview with BR and Zeit Online, he explained that Germany is an important player in the middle of Europe, and foreign services were therefore very interested in the politics in this country: "Germany is involved in many international relations, and the diaspora from many countries is living here". After the failed coup, Turkey had supporters of the Gülen movement spied on, whereas Iran is trying to intimidate members of the opposition.

We see a clear connection to Vietnam.

Thomas Haldenwang, Präsident des Bundesamtes für Verfassungsschutz

Meanwhile, cyber-attacks have become the "means of choice" for many foreign services, as Haldenwang explained. The Federal Office for the Protection of the Constitution has been observing the hackers of Ocean Lotus since 2014, and the BfV noticed that the hackers are "interested in certain groups of people with a Vietnamese background": "That is another reason why we see a clear connection to Vietnam", Haldenwang said. A clear attribution, especially to Vietnam's intelligence services, could not be made, however.

There is no well-established procedure

Haldenwang described a central problem of counter-espionage. The BfV sent out a warning to the automotive industry when Ocean Lotus was active in Germany. There was a well-established procedure between the authority and the German industry. "The situation is different when dissidents are spied on. If we perceive threats to individuals on this field, we discuss the further procedure with the police". The police are responsible for immediate protection.

However, digital espionage is often a preparatory act. It cannot be told from an e-mail whether it can develop into a real threat. According to Haldenwang, it is part of the task of the BfV to assist the police. However, he said: "No

police authority is able to guard and protect this large group of people around the clock”.

The police do not answer – for months

Vu Quoc Dung is a prime example. Nowadays, he is doubting whether he can rely on the German state. When he learned that he had been targeted by hackers, no one helped him for months. Vu is chairman of the “Veto” network, which campaigns for human rights in Vietnam. He spoke in front of the European Parliament, met with politicians from the Bundestag and also with the German President Frank-Walter Steinmeier.

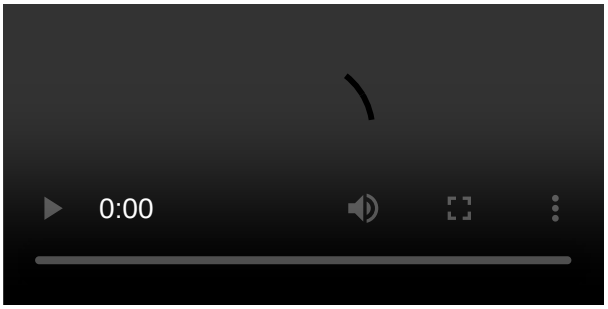
Human rights worker Vu Quoc Dung – © BR

On May 12th, 2020, he received queries from friends about an e-mail containing gossip from the Vietnamese government. They asked whether he had really sent it. The e-mail address was similar to his, and also his signature appeared. However, the e-mail was sent by Ocean Lotus. It was also sent to his nephew and a journalist who reports on the Vietnamese community for the newspaper “taz”. The association “Veto” filed a complaint. Nothing happened for months.

Vu’s nephew learned to recognize e-mails containing viruses at his workplace. “When I receive a message with an attachment from a new e-mail address, I become cautious,” Huy said when reached by phone. Out of curiosity, he wrote an e-mail back. Less than two hours later, the hackers actually replied – as a supposed Uncle Vu – and asked him “what’s up”. “My uncle would never write like that,” said Huy.

Professional hacker software „Cobalt Strike“

If someone where to download the text file sent by the hackers, they would install professional hacker software called “Cobalt Strike”, as Steven Adair, who works for the information security company Volexity, explained. He analyzed the mail that contained malware. Cobalt Strike is the software of a US company. The price tag is at several thousand euros a year. The software framework is so powerful that the US government has to agree to its sale to many countries. The software is used, completely legally, by specialists as soon as they receive the order from a company to test their IT security.



Now you see them, now you don't

It could be argued that the hackers of Ocean Lotus are also testing the IT security of government and corporate networks – albeit unsolicited and illegally. If they are successful, they will exfiltrate the data back to a server they own, said Steven Adair.

The information security specialist already knew Vu Quoc Dung. After all, Adair reached out to the human rights organisation Veto after their website had been hacked in 2017. The homepage was one of more than 100 websites that the hackers had taken over. “The absolute majority of these sites, about 80 to 90, were related to Vietnam,” explained Steven Adair. Sites for Vietnamese Catholics were targeted, sites for local news or a website for a steel company whose plant in Vietnam is responsible for one of the country’s biggest environmental disasters.

Adair analyzed the Veto website and removed the hackers’ tools. “They had created a profile of each visitor to the site,” he explained and estimated that out of 100,000 visitors per day, only ten were likely to be of interest to the hackers. “As soon as they wanted to target a person, the hackers changed the look of the site”. Suddenly, for example, a Google login appeared. This is how the hackers obtained access to these people’s login data and were able to read and send e-mails in their name.

Years later, the hackers of Ocean Lotus are still targeting Vu Quoc Dung, as the e-mails, sent by them, show. It clearly is a case of cyber espionage. “We translated the text of the e-mail – it was written in Vietnamese – into German and explained in detail why we had filed criminal charges,” said Vu. But when reached by BR and Zeit Online, the police authority in charge wrote back that the case had ended up in the fraud department. The police apparently had tried to contact Vu by phone as well as by e-mail. However, as BR and Zeit Online were able to find out, the address to which they sent the e-mail belonged to the hackers. After the press request, the police invited Vu for another interview.

The human rights organisation Veto is trying to protect itself in the meantime, even if this is probably in vain, as Vu explained: “I don’t think that we, as a small organization, have the possibility to defend ourselves against a group of hackers who probably are supported by the state”. In Vu’s opinion, German authorities are the ones responsible: “We would like to see the state or the police trying to protect human rights groups when they become the target of such attacks”.

A task for the Federal Government

This is also the view of Christoph Safferling, Professor of International Criminal Law and International Law at the University of Erlangen-Nuremberg. He said that the protection of these people was a task of the Federal Government, and resulted from the constitution: “If we want to have an unbiased cooperation here in the Federal Republic, we cannot allow foreign secret services to spy on people living in exile”. He added that one had to be aware of the consequences: “These people are not just any foreigners who are here by accident, but they are a part of our society. And they must be able to live here in peace and in freedom”.

That is precisely what the hackers of Ocean Lotus want to prevent – that is what their name stands for. At the very beginning, in 2011, they have given themselves a Vietnamese name. Sinh Tu Lenh. A metaphor for a command over life and death. The name goes back to a talisman that appears in many novels by the Chinese bestselling author Jin Yong. His books and films are popular in Vietnam.

Whoever uses the talisman is able to make people compliant. The victims suffer excruciating pain. Until they obey. Only then is their pain relieved. The malware - that is the talisman of the hackers of Ocean Lotus. Just like the character in the novel, the hackers control their victims: the keyboard, the screen, the files. Until the critics of the regime are obedient.

About the project:

Lined up in the sights of Vietnamese hackers is an investigatoin by Bayerischer Rundfunk (BR Recherche / BR Data) and Zeit Online. Their project, titled "Hackers of Hanoi", is viewable at this link..

Published on October, 8th, 2020

- **Written by:** Hakan Tanriverdi, Ann-Kathrin Wetter, Maximilian Zierer, Kai Biermann (Zeit Online), Thi Do Nguyen (Zeit Online)
- **Digital Design:** Sebastian Bayerl
- **Illustrations:** Christian Sonnberger
- **Contributions by:** Michael Kreil, Steffen Kühne
- **Edited by:** Verena Nierle, Robert Schöffel, Lisa Wreschniok

---