Trump hacker and friends on a mission to fix the internet

July 16 2021, by Katy Lee

Victor Gevers describes himself and other ethical hackers as a 'volunteer fire brigade' for the internet.

When a massive cyberattack took out everything from Swedish supermarkets to New Zealand kindergartens this month, a group of Dutch ethical hackers breathed a collective sigh of frustration. They had

been so close to stopping it.

If the Dutch Institute for Vulnerability Disclosure (DIVD) sounds obscure, that's in keeping with its discreet presence on the internet.

This volunteer army of unpaid tech geeks have quietly prevented hundreds of cyberattacks since 2019 by finding holes in websites and software that could be exploited by hackers.

"You can see us as a volunteer fire brigade," said DIVD chairman Victor Gevers in an interview from his home in The Hague, a dog yapping at his ankles.

"Your house is on fire, there's flames coming out of it, and then random people with a Dutch accent show up and start putting out the fire."

The bearded hacker declined to give his age, but he has been carrying out these "responsible disclosures" for the best part of two decades.

Most famously, he successfully accessed Donald Trump's Twitter account—not once, but twice.

'Oh God, why him?'

Just before the 2016 US election swept Trump to power, Gevers and two friends decided to make sure the then-candidate wasn't using a password that had previously been leaked online.

Gevers managed to access Trump's Twitter account twice, once using the password 'yourefired' and then the password 'maga2020!'

A huge hack of LinkedIn revealed that the password "yourefired"—Trump's catchphrase from his days on TV show The Apprentice—had been used for an account in his name on the business networking site.

And after trying the same password on Twitter alongside several different email addresses, the Dutch hackers were horrified to see Trump's personal page load up before their eyes.

They rushed to inform Trump's campaign and US authorities, stressing that if they could access his account, so might more malevolent hackers.

But they never heard back.

So when Gevers succeeded in hacking Trump's Twitter again last year—this time, with the password "maga2020!"—his heart sank.

"Honestly, it was like, 'Oh God, why him?'," Gevers recalled. He knew that he would again have to make rigorous efforts to contact Trump, which would likely be ignored—all the while leaving his account open to attack.

That was an alarming prospect. Trump's febrile Twitter presence gave him a megaphone to directly address some 90 million people. And as the violence at the US Capitol showed a few months later, his posts were capable of fuelling an incendiary atmosphere.

"Imagine there was a tweet that said something like, 'start throwing axes at police officers'," Gevers said. "There would be a lot of followers who blindly followed him."

This time, instead of being ignored, Gevers' hack sparked international headlines and a stressful criminal investigation.

The Kaseya ransomware attack forced Swedish supermarket chain Coop to shut hundreds of stores.

While the White House denied it had ever happened, Dutch prosecutors said in December that they were satisfied Gevers had indeed accessed Trump's account.

And fortunately for Gevers, they determined that he "met the criteria that have been developed in case law to go free as an ethical hacker".

Racing against 'the bad guys'

This law makes it easier for ethical hackers to operate in the Netherlands than countries like the US or UK, where forays into people's accounts—even when well-intentioned—run greater legal risks, says Gevers.

He has also founded the GDI, a similar "online fire brigade" working internationally, from India to Portugal.

"We do this volunteering work because we have to leave behind something that is good for the next generation," he said.

During the pandemic, the volunteers have grown increasingly worried about weak spots in VPNs and other tools that allow computers to be managed remotely—tools that are being used more and more, with no end in sight to the working-from-home trend.

Kaseya, the Miami-based IT company targeted in a spectacular cyberattack on July 3, had been in the DIVD's sights for months. Thousands of companies use its software to manage their networks of printers and computers.

Gevers has personally carried out more than 5,000 ethical disclosures, warning organisations that they are vulnerable to hackers.

Fellow DIVD researcher Wietse Boonstra had spotted a major problem with Kaseya's software in April, and the ethical hackers had been frantically helping the company develop a fix.

To their dismay, the Russian-speaking hacking outfit REvil got there first. They exploited the vulnerability to stage a massive ransomware attack, encrypting the data of hundreds of companies and demanding $70 million in bitcoin in exchange for its release.

"It sucks," Gevers said. "I don't mind that the bad guys are faster—what I mind is that there are victims."

The hack hit around 1,500 businesses worldwide and wiped out the cash registers of Swedish supermarket chain Coop. Gevers is still working with those affected.

"If the Red Cross can help victims worldwide, why not us?" Gevers said. "The only thing is that we do it from behind a keyboard."

Citation: Trump hacker and friends on a mission to fix the internet (2021, July 16) retrieved 10 April 2024 from https://techxplore.com/news/2021-07-trump-hacker-friends-mission-internet.html