Four Members of Notorious Cybercrime Group ‘FIN9’ Charged for Roles in Attacking U.S. Companies

Published: 2024-06-20 · Archived: 2026-04-06 15:32:15 UTC

NEWARK, N.J. – An indictment was unsealed today charging four Vietnamese nationals for their involvement in a series of computer intrusions that caused victim companies to collectively suffer more than $71 million in losses, U.S. Attorney Philip R. Sellinger announced.

According to the indictment, Ta Van Tai, aka “Quynh Hoa,” aka “Bich Thuy;” Nguyen Viet Quoc, aka “Tien Nguyen;” Nguyen Trang Xuyen; and Nguyen Van Truong, aka “Chung Nguyen,” were members of a sophisticated international cybercrime group known as “FIN9.” From at least May 2018 through October 2021, the defendants hacked the computer networks of victim companies throughout the United States and used their access to steal or attempt to steal non-public information, employee benefits, and funds. The defendants caused their victims to suffer more than $71 million in losses.

> “The FIN9 defendants were prolific international hackers who, for years, allegedly used phishing campaigns, supply chain attacks and other hacking methods to steal millions from their victims. They did all of this while hiding behind keyboards, VPNs, and fake identities, and even then, the Department of Justice found them. My office remains committed to its pursuit of justice for victims, and cybercriminals everywhere should take notice.”
>
> U.S. Attorney Philip R. Sellinger

“Cyber actors cloak themselves in the virtual world, hiding in a space most people can't see and don't understand,” FBI – Newark Special Agent in Charge James E. Dennehy said. “However smart these hackers believe they are at disguising themselves, these members of the FIN9 group couldn’t conceal their exfiltration of data from their victims’ companies. FBI Newark’s Cyber Task Force and our law enforcement partners use precision and innovative techniques to expose these people for what they are – simple thieves. We ask any business or company facing a similar attack to reach out to us immediately to protect your systems and to stop these criminals from moving on to the next victim.”

According to documents filed in this case and statements made in court:

Members of FIN9, including the defendants, obtained unauthorized access to the computer networks of victim companies through phishing campaigns or other methods, such as supply chain attacks – a type of cyberattack that seeks to damage an organization by targeting the computer networks of trusted third-party vendors who offer services or software vital to the supply chain. After gaining access to their victims’ networks, FIN9 members, including the defendants, used that access to exfiltrate or attempt to exfiltrate non-public information, employee benefits, and/or funds. For example, the defendants accessed employee benefit rewards programs maintained by their victims and re-directed digital employee benefits, such as gift cards, to accounts controlled by defendants. The defendants also stole gift card information stored on the computer networks of certain victims.

The defendants additionally stole personally identifiable information and credit card information associated with employees and customers of their victim companies. In an effort to hide their own identities, the defendants would, at times, use that information in furtherance of the conspiracy by, for example, registering online accounts at cryptocurrency exchanges or server hosting companies in the names of individuals whose identities were stolen. Tai, Xuyen, and Truong sold stolen gift cards to third parties, including through an account registered with a fake name on a peer-to-peer cryptocurrency marketplace, in order to conceal and disguise the source of the stolen money.

Tai, Quoc, Xuyen, and Truong are charged with one count of conspiracy to commit fraud, extortion, and related activity in connection with computers; one count of conspiracy to commit wire fraud; and two counts of intentional damage to a protected computer. If convicted, they face up to five years in prison for the conspiracy to commit fraud, extortion, and related activity in connection with computers; up to 20 years in prison for the conspiracy to commit wire fraud; and up to 10 years in prison on each count of intentional damage to a protected computer. Tai, Xuyen, and Truong were charged with one count of conspiracy to commit money laundering, which carries a mandatory maximum penalty of 20 years in prison. Tai and Quoc were also charged with one count of aggravated identity theft, which carries a mandatory consecutive term of two years in prison, and one count of conspiracy to commit identity fraud, which carries a maximum penalty of 15 years in prison.

U.S. Attorney Sellinger credited the FBI Newark's Cyber squad, under the direction of Special Agent in Charge James E. Dennehy in Newark. He also thanked the FBI Little Rock Cyber squad, under the direction of Special Agent in Charge Alicia D. Corder.

The government is represented by Assistant U.S. Attorneys Anthony P. Torntore and Vinay S. Limbachia of the U.S. Attorney's Cybercrime Unit in Newark.

The charges and allegations contained in the indictment are merely accusations, and the defendants are presumed innocent unless and until proven guilty.
