What is Storm-1152, alleged top creator of fake Microsoft accounts?

December 15 2023, by Qasim Nauman

Microsoft has seized the websites of Storm-1152, a Vietnam-based group it says is responsible for creating hundreds of millions of fake accounts.

Microsoft has seized the websites of a Vietnam-based group it alleges sold millions of fake accounts to cybercriminals who used them for

ransomware attacks, identity theft and other scams around the world.

The group, identified by Microsoft as Storm-1152, developed sophisticated tools to defeat the US tech giant's security features to set up fraudulent Outlook and Hotmail email accounts in bulk.

Who is in Storm-1152?

Storm-1152 was first detected in 2021. Arkose Labs, the cybersecurity firm that worked with Microsoft against the group, tracked it to Vietnam.

The leaders of the group are three Vietnam-based individuals, Duong Dinh Tu, Linh Van Nguyen and Tai Van Nguyen, Microsoft said in a statement on Wednesday. It is not clear if there are any other members.

AFP has asked the three for a response on email addresses listed in Microsoft's complaint against them in a US federal court last week.

AFP has also contacted Vietnamese authorities for comment.

How did they make millions of accounts so rapidly?

Storm-1152 developed automated software—or "bots"—to create fake accounts.

These bots defeated Microsoft's safeguards, such as the CAPTCHA puzzles users have to solve to prove they are human, the tech giant said in its court filing.

Storm-1152 is "the number one seller and creator of fraudulent Microsoft accounts", creating around 750 million to date, the company said Wednesday.

Microsoft's court filing included a screenshot of a Storm-1152 website that boasts the use of artificial intelligence against CAPTCHA.

The group created accounts "at a scale so large, fast, and efficient that it could have only been carried out through automated, machine-learning technology", Patrice Boffa, chief customer officer at Arkose Labs, said in a statement.

Who needs so many fake email accounts?

Storm-1152 pursued a model called "cybercrime-as-a-service" or CaaS, acting as a provider to other criminal groups, Microsoft and Arkose said.

With tech companies improving their detection and deletion of fake accounts, cyber attackers need huge amounts to carry out their operations.

"Instead of spending time trying to create thousands of fraudulent accounts, cybercriminals can simply purchase them from Storm-1152 and other groups," Microsoft's Amy Hogan-Burney said in a blog post.

Storm-1152 allegedly made millions of dollars from the operation.

What did Storm-1152's customers do with fake accounts?

The group's customers have used fake email accounts for a variety of crimes, according to Microsoft and Arkose Labs.

These include phishing attacks to either steal information or insert malware on devices.

Its customers have also used these accounts to install ransomware and demand payment from victims, according to Microsoft.

The highest-profile customer named in Microsoft's court filing is a group known as Octo Tempest, which has been linked to a wave of cybercrimes in recent years.

Octo Tempest recently launched ransomware attacks against Microsoft customers that "inflicted hundreds of millions of dollars of damage", the company said in its court filing, without naming the victims.

Google and X, formerly known as Twitter, have also been hit by Storm-1152 activities, Microsoft said in the filing.

Was it hard to find Storm-1152?

Unlike many cybercriminals that offer such services on the so-called dark web, hidden away from general users, Storm-1152's websites were on the open web.

It offered its services on at least two websites, according to Microsoft, and even had step-by-step user guides.

Duong Dinh Tu, one of the defendants, also had a YouTube channel with a video demonstration, and the group would edit the code for their anti-CAPTCHA software on GitHub—a Microsoft-owned internet depository for software.

Microsoft said it also hired cybercrime experts to make undercover purchases of accounts and CAPTCHA-beating tools from Storm-1152 websites.

A US court allowed Microsoft to take control of the group's sites in response to the company's complaint last week.

The sites now say, "This Domain has been seized by Microsoft."