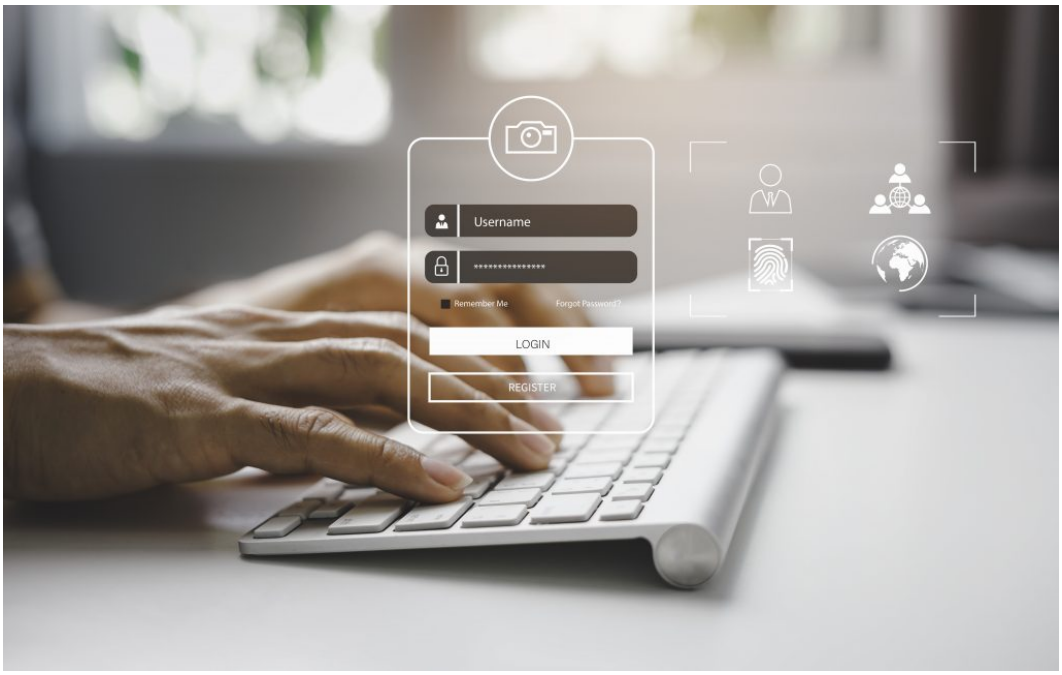
Disrupting the gateway services to cybercrime

blogs.microsoft.com/on-the-issues/2023/12/13/cybercrime-cybersecurity-storm-1152-fraudulent-accounts/

December 13, 2023



At Microsoft, we continue to look for creative ways to protect people online and that includes having no tolerance for those who create fraudulent copies of our products to harm others. Fraudulent online accounts act as the gateway to a host of cybercrime, including mass phishing, identity theft and fraud, and distributed denial of service (DDoS) attacks. That is why today, we, with valuable threat intelligence insights from Arkose Labs, a leading cybersecurity defense and bot management vendor, are going after the number one seller and creator of fraudulent Microsoft accounts, a group we call Storm-1152. We are sending a strong message to those who seek to create, sell or distribute fraudulent Microsoft products for cybercrime: We are watching, taking notice and will act to protect our customers.

Storm-1152 runs illicit websites and social media pages, selling fraudulent Microsoft accounts and tools to bypass identity verification software across well-known technology platforms. These services reduce the time and effort needed for criminals to conduct a host of criminal and abusive behaviors online. To date, Storm-1152 created for sale approximately 750 million fraudulent Microsoft accounts, earning the group millions of dollars in illicit revenue, and costing Microsoft and other companies even more to combat their criminal activity.

With today's action, our goal is to deter criminal behavior. By seeking to slow the speed at which cybercriminals launch their attacks, we aim to raise their cost of doing business while continuing our investigation and protecting our customers and other online users.

How cybercriminals use Storm-1152's services

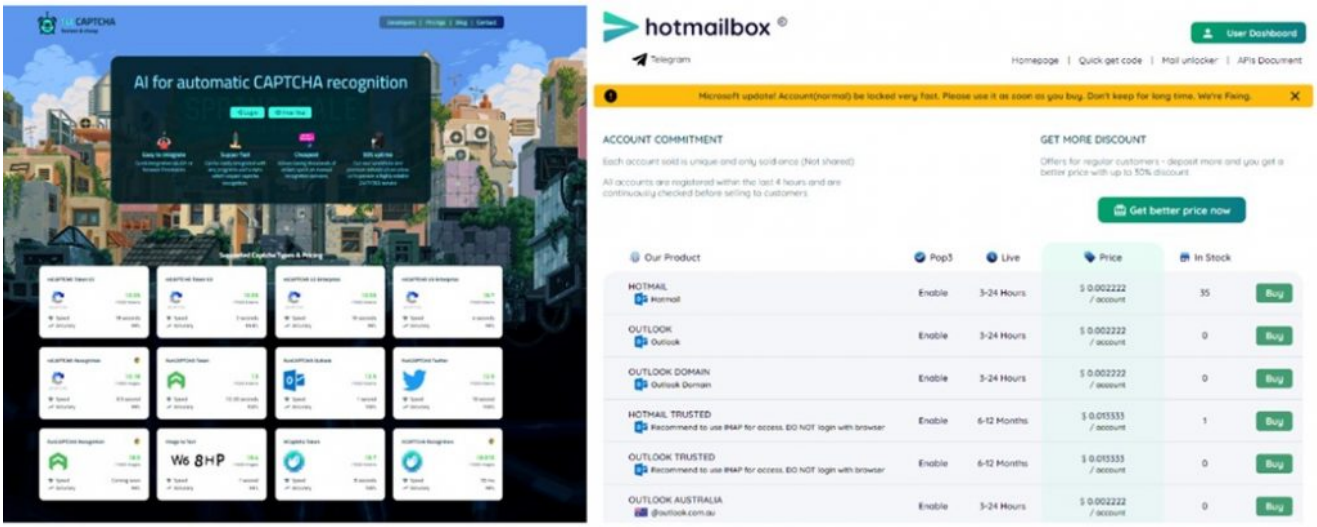
Storm-1152 plays a significant role in the highly specialized cybercrime-as-a-service ecosystem. Cybercriminals need fraudulent accounts to support their largely automated criminal activities. With companies able to quickly identify and shut down fraudulent accounts, criminals require a greater quantity of accounts to circumvent mitigation efforts. Instead of spending time trying to create thousands of fraudulent accounts, cybercriminals can simply purchase them from Storm-1152 and other groups. This allows criminals to focus their efforts on their ultimate goals of phishing, spamming, ransomware, and other types of fraud and abuse. Storm-1152 and groups like them enable scores of cybercriminals to carry out their malicious activities more efficiently and effectively.

Microsoft Threat Intelligence has identified multiple groups engaged in ransomware, data theft and extortion that have used Storm-1152 accounts. For example, Octo Tempest, also known as Scattered Spider, obtained fraudulent Microsoft accounts from Storm-1152. Octo Tempest is a financially motivated cybercrime group that leverages broad social engineering campaigns to compromise organizations across the globe with the goal of financial extortion. Microsoft continues to track multiple other ransomware or extortion threat actors that have purchased fraudulent accounts from Storm-1152 to enhance their attacks, including Storm-0252 and Storm-0455.

Our disruption strategy

On Thursday, December 7, Microsoft obtained a court order from the Southern District of New York to seize U.S.-based infrastructure and take offline websites used by Storm-1152 to harm Microsoft customers. While our case focuses on fraudulent Microsoft accounts, the websites impacted also sold services to bypass security measures on other well-known technology platforms. Today's action therefore has a broader impact, benefiting users beyond Microsoft. Specifically, Microsoft's Digital Crimes Unit disrupted:

- **Hotmailbox.me**, a website selling fraudulent Microsoft Outlook accounts
- **1stCAPTCHA, AnyCAPTCHA, and NoneCAPTCHA**, websites that facilitate the tooling, infrastructure, and selling of the CAPTCHA solve service to bypass the confirmation of use and account setup by a real person. These sites sold identity verification bypass tools for other technology platforms
- **The social media sites** actively used to market these services

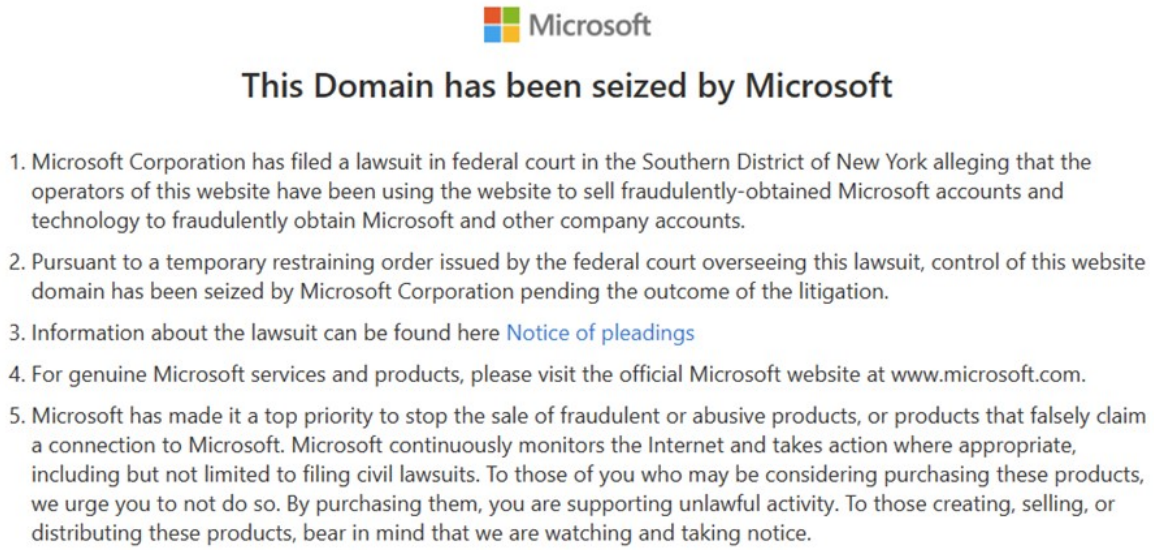


Images of Storm-1152's illicit websites

Microsoft is committed to providing a safe digital experience for every person and organization on the planet. We work closely with Arkose Labs to deploy a next-generation CAPTCHA defense solution. The solution requires every would-be user who wishes to open a Microsoft account to represent that they are a human being (not a bot) and verify the accuracy of that representation by solving various types of challenges.

As founder and CEO of Arkose Labs, Kevin Gosschalk says: "Storm-1152 is a formidable foe established with the sole purpose of making money by empowering adversaries to commit complex attacks. The group is distinguished by the fact that it built its CaaS business in the light of day versus on the dark web. Storm-1152 operated as a typical internet going-concern, providing training for its tools and even offering full customer support. In reality, Storm-1152 was an unlocked gateway to serious fraud."

Storm-1152's activity not only violates Microsoft's terms of services by selling fraudulent accounts, but it also purposely seeks to harm customers of Arkose Labs and deceive victims pretending to be legitimate users in an attempt to bypass security measures.

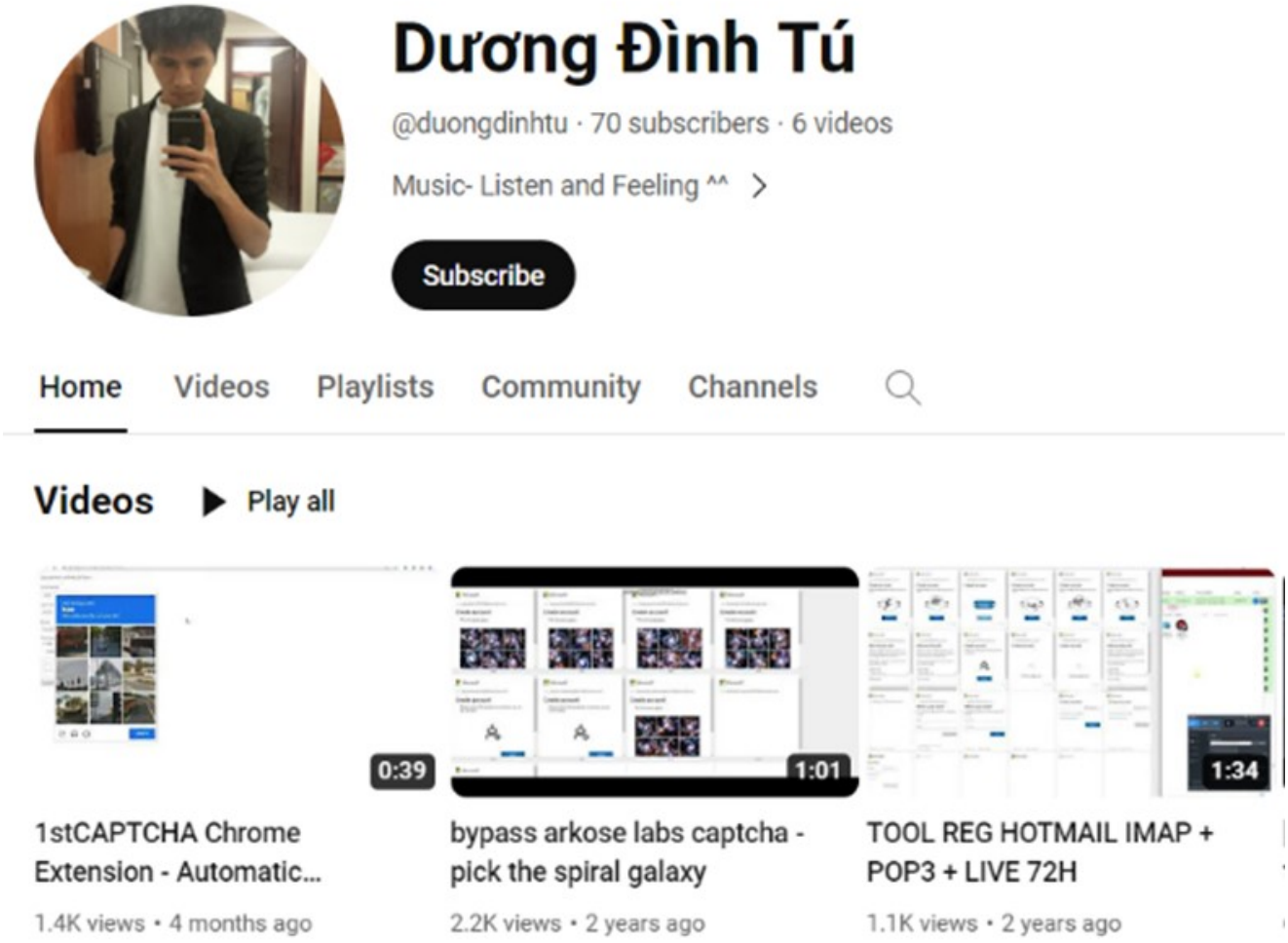


What visitors to hotmailbox.com, 1stCAPTCHA, AnyCAPTCHA, and NoneCAPTCHA will see if they try to access the websites

Identifying the individuals and infrastructure behind Storm-1152

Our analysis of Storm-1152's activity included detection, analysis, telemetry, undercover test purchases, and reverse engineering to pinpoint the malicious infrastructure hosted in the United States. Microsoft Threat Intelligence and Arkose Cyber Threat Intelligence Research unit (ACTIR) provided additional data and insights to strengthen our legal case.

As part of our investigation, we were able to confirm the identity of the actors leading Storm-1152's operations – Duong Dinh Tu, Linh Van Nguyễn (also known as Nguyễn Van Linh), and Tai Van Nguyen – based in Vietnam. Our findings show these individuals operated and wrote the code for the illicit websites, published detailed step-by-step instructions on how to use their products via video tutorials and provided chat services to assist those using their fraudulent services.



Duong Dinh Tu's YouTube channel with "how to videos" to bypass security measures

Microsoft has since submitted a criminal referral to U.S. law enforcement. We are grateful for our partnership with law enforcement who can bring those looking to harm our customers to justice.

Our ongoing commitment to fighting cybercrime

Today's action is a continuation of Microsoft's strategy of taking aim at the broader cybercriminal ecosystem and targeting the tools cybercriminals use to launch their attacks. It builds on our expansion of a legal method used successfully to disrupt malware and nation-state operations. We have also partnered with other organizations across the industry to increase intelligence sharing on fraud and further enhance our artificial intelligence and machine learning algorithms that quickly detect and flag fraudulent accounts.

As we've said before, no disruption is complete in one day. Going after cybercrime requires persistence and ongoing vigilance to disrupt new malicious infrastructure. While today's legal action will impact Storm-1152's operations, we expect other threat actors will adapt their

techniques as a result. Continued public and private sector collaboration, like todays with Arkose Labs and U.S. law enforcement, remain essential if we want to meaningfully dent the impact of cybercrime.

Tags: cyberattacks, cybercrime, cybersecurity, Digital Crimes Unit, MTAC, Storm-1152