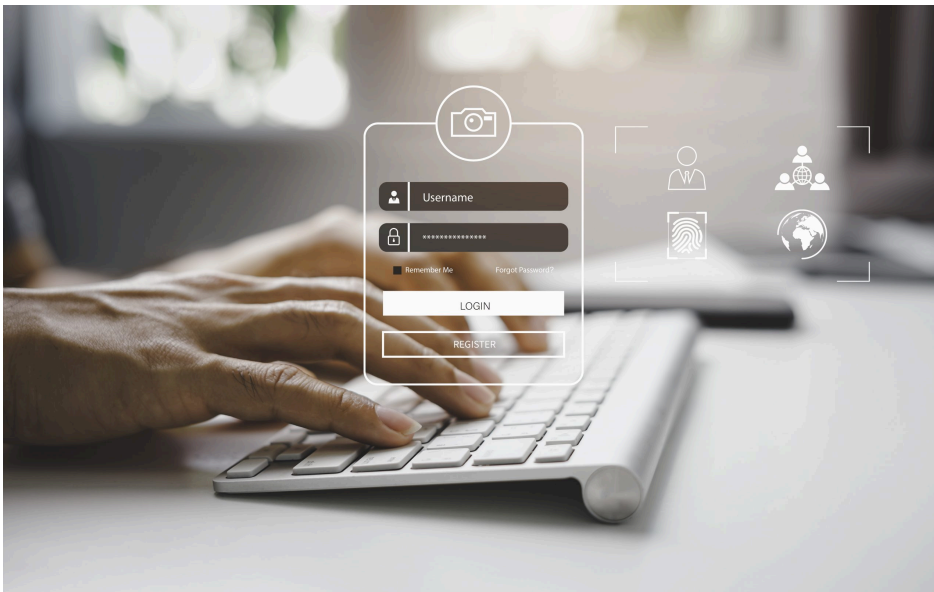


Disrupting the gateway services to cybercrime

[Topics](#)
[Cloud Principles](#)
[Press Tools](#)

Dec 13, 2023 | [Amy Hogan-Burney](#) - General Manager,
Associate General Counsel, Cybersecurity Policy & Protection



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.

Dec 7, 2023 | [Clint Watts](#)

**Russian influence and
cyber operations adapt
for long haul and
exploit war fatigue** >

Nov 7, 2023 | Brad Smith,
Microsoft Vice Chair and
President, and Teresa Hutson,
Corporate Vice President,
Technology for Fundamental
Rights

**Microsoft announces
new steps to help
protect elections** >

Nov 2, 2023 | [Brad Smith](#)

**A new world of security:
Microsoft's Secure
Future Initiative** >

Related Blogs

Dec 11, 2023 | [Brad Smith](#)

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

AFL-CIO and Microsoft announce new tech-labor partnership on AI and the future of the workforce >

Dec 5, 2023 | [Jon Palmer](#)

38 VC firms and investors advocate for a thriving innovation ecosystem >

Nov 29, 2023 | [Chris Barry](#)

AI in Canada: meeting the opportunity >

More Cybersecurity Stories

Standing up for democratic values and protecting stability of cyberspace: Principles to limit the threats posed by cyber mercenaries >

April 11, 2023

Digital Crimes Unit: Leading the fight against cybercrime >

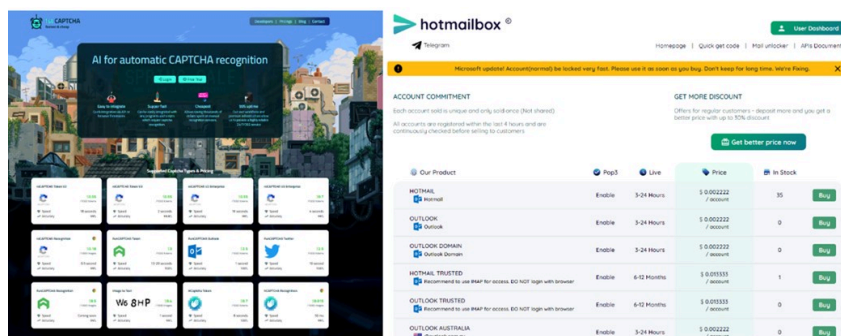
May 3, 2022

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

Keeping your vote safe and secure: A story from inside the 2020 election >

June 22, 2021



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.



This Domain has been seized by Microsoft

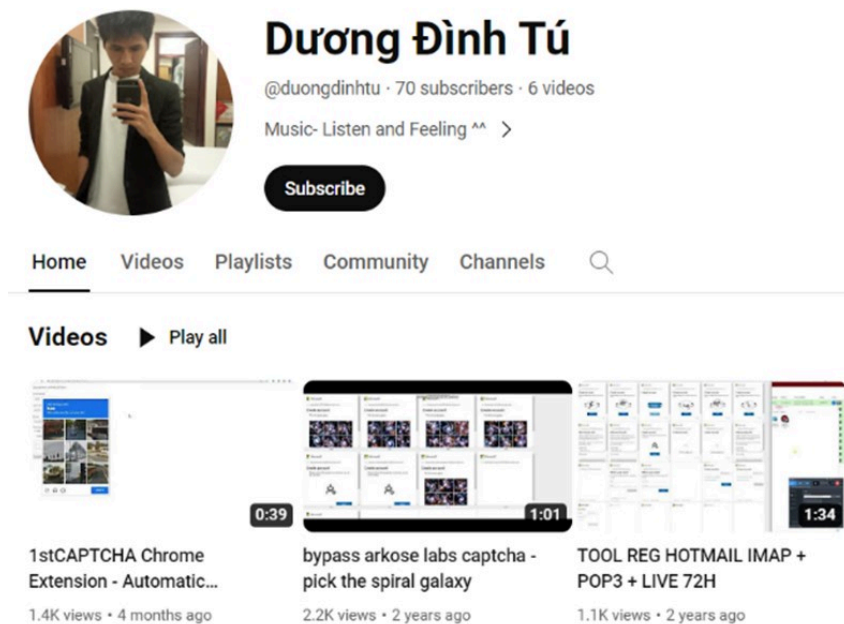
1. Microsoft Corporation has filed a lawsuit in federal court in the Southern District of New York alleging that the operators of this website have been using the website to sell fraudulently-obtained Microsoft accounts and technology to fraudulently obtain Microsoft and other company accounts.
2. Pursuant to a temporary restraining order issued by the federal court overseeing this lawsuit, control of this website domain has been seized by Microsoft Corporation pending the outcome of the litigation.
3. Information about the lawsuit can be found here [Notice of pleadings](#)
4. For genuine Microsoft services and products, please visit the official Microsoft website at www.microsoft.com.
5. Microsoft has made it a top priority to stop the sale of fraudulent or abusive products, or products that falsely claim a connection to Microsoft. Microsoft continuously monitors the Internet and takes action where appropriate, including but not limited to filing civil lawsuits. To those of you who may be considering purchasing these products, we urge you to not do so. By purchasing them, you are supporting unlawful activity. To those creating, selling, or distributing these products, bear in mind that we are watching and taking notice.

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 Nguyen (also known as Nguyễn Văn 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.



The image shows a screenshot of a YouTube channel page for a user named Dương Đình Tú. The profile picture shows a man in a dark jacket holding a phone. The channel name is "Dương Đình Tú" with the handle "@duongdinhtu", 70 subscribers, and 6 videos. Below the name is a "Subscribe" button and a link to "Music- Listen and Feeling ^^". The navigation bar includes "Home", "Videos", "Playlists", "Community", and "Channels". The "Videos" section is active, showing a "Play all" button and a grid of video thumbnails. The first three videos are: "1stCAPTCHA Chrome Extension - Automatic..." (1.4K views, 4 months ago), "bypass arkose labs captcha - pick the spiral galaxy" (2.2K views, 2 years ago), and "TOOL REG HOTMAIL IMAP + POP3 + LIVE 72H" (1.1K views, 2 years ago).

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 today's 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](#)

Follow us: 

What's new	Microsoft Store	Education	Business	Developer & IT	Company
Surface Laptop Studio 2	Account profile	Microsoft in education	Microsoft Cloud	Azure	Careers
Surface Laptop Go 3	Download Center	Devices for education	Microsoft Security	Developer Center	About Microsoft
Surface Pro 9	Microsoft Store support	Microsoft Teams for Education	Dynamics 365	Documentation	Company news
Surface Laptop 5	Returns	Microsoft 365 Education	Microsoft 365	Microsoft Learn	Privacy at Microsoft
Microsoft Copilot	Order tracking	How to buy for your school	Microsoft Power Platform	Microsoft Tech Community	Investors
Copilot in Windows	Certified Refurbished	Educator training and development	Microsoft Teams	Azure Marketplace	Diversity and inclusion
Explore Microsoft products	Microsoft Store Promise	Deals for students and parents	Copilot for Microsoft 365	AppSource	Accessibility
Windows 11 apps	Flexible Payments	Azure for students	Small Business	Visual Studio	Sustainability