Disrupting a global cybercrime network abusing generative AI

blogs.microsoft.com/on-the-issues/2025/02/27/disrupting-cybercrime-abusing-gen-ai/

February 27, 2025

In an amended complaint to recent civil litigation, Microsoft is naming the primary developers of malicious tools designed to bypass the guardrails of generative AI services, including Microsoft's Azure OpenAI Service. We are pursuing this legal action now against identified defendants to stop their conduct, to continue to dismantle their illicit operation, and to deter others intent on weaponizing our AI technology.

The individuals named are: (1) Arian Yadegarnia aka "Fiz" of Iran, (2) Alan Krysiak aka "Drago" of United Kingdom, (3) Ricky Yuen aka "cg-dot" of Hong Kong, China, and (4) Phát Phùng Tấn aka "Asakuri" of Vietnam. These actors are at the center of a global cybercrime network Microsoft tracks as Storm-2139. Members of Storm-2139 exploited exposed customer credentials scraped from public sources to unlawfully access accounts with certain generative AI services. They then altered the capabilities of these services and resold access to other malicious actors, providing detailed instructions on how to generate harmful and illicit content, including non-consensual intimate images of celebrities and other sexually explicit content.

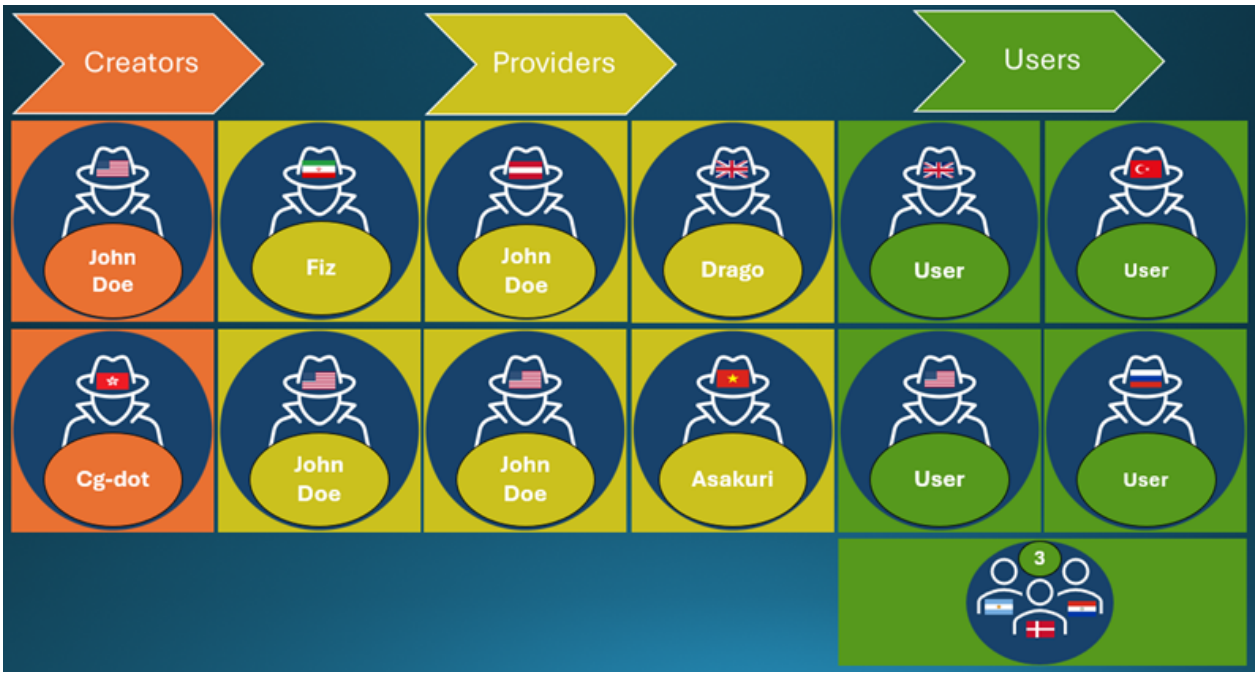
This activity is prohibited under the terms of use for our generative AI services and required deliberate efforts to bypass our safeguards. We are not naming specific celebrities to keep their identities private and have excluded synthetic imagery and prompts from our filings to prevent the further circulation of harmful content.

Storm-2139: A global network of creators, providers and end users.

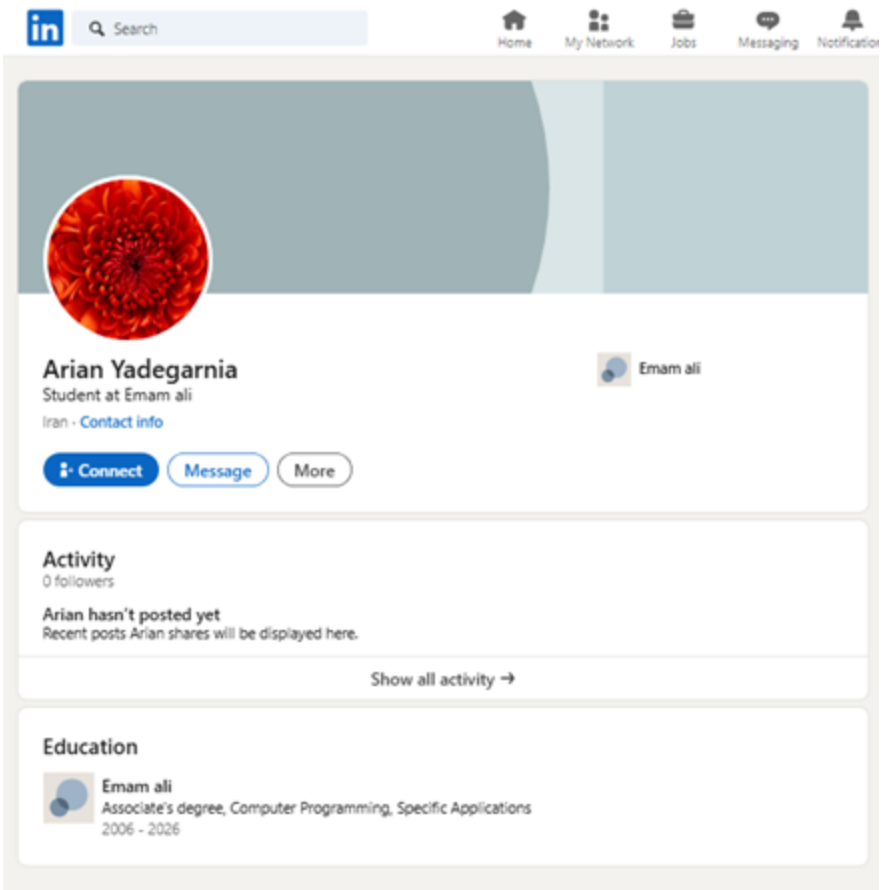
In December 2024, Microsoft's Digital Crimes Unit (DCU) filed a lawsuit in the Eastern District of Virginia alleging various causes of action against 10 unidentified "John Does" participating in activities that violate U.S. law and Microsoft's Acceptable Use Policy and Code of Conduct. Through this initial filing, we were able to gather more information about the operations of the criminal enterprise.

Storm-2139 is organized into three main categories: creators, providers, and users. Creators developed the illicit tools that enabled the abuse of AI generated services. Providers then modified and supplied these tools to end users often with varying tiers of service and payment. Finally, users then used these tools to generate violating synthetic content, often centered around celebrities and sexual imagery.

Below is a visual representation of Storm-2139, which displays internet aliases uncovered as part of our investigation as well as the countries in which we believe the associated personas are located.



Storm-2139's organizational structure.



Screenshot of "Fiz's" LinkedIn profile

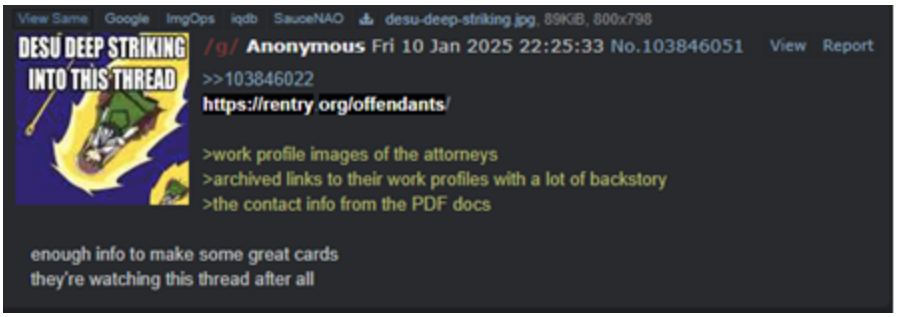
Through its ongoing investigation, Microsoft has identified several of the above-listed personas, including, but not limited to, the four named defendants. While we have identified two actors located in the United States—specifically, in Illinois and Florida—those identities remain undisclosed to avoid interfering with potential criminal investigations. Microsoft is preparing criminal referrals to United States and foreign law enforcement representatives.

Cybercriminals react to Microsoft's website seizure and court filing.

As part of our initial filing, the Court issued a temporary restraining order and preliminary injunction enabling Microsoft to seize a website instrumental to the criminal operation, effectively disrupting the group's ability to operationalize their services. The seizure of this website and subsequent unsealing of the legal filings in January generated an immediate reaction from actors, in some cases causing group members to turn on and point fingers at one another. We observed chatter about the lawsuit on the group's monitored communication channels, speculating on the identities of the "John Does" and potential consequences.

Screenshot of online chatter discussing "Fiz's" real name.

In these channels, certain members also "doxed" Microsoft's counsel of record, posting their names, personal information, and in some instances photographs. Doxing can result in real-world harm, ranging from identity theft to harassment.



Screenshot from post on online channels providing information about the case lawyers.

As a result, Microsoft's counsel received a variety of emails, including several from suspected members of Storm-2139 attempting to cast blame on other members of the operation.

Subject: the guy you are looking for - azure

https://discord.gg/scylla-charybdis This is the discord. They are selling access to azure for over 100 dollars. The old guys you are trying to sue don't even sell anything. These guys do.
This is the site: https://scylla.wtf

This is the main guy(drago) discord id: 325722644060176385 Attached proof of them talking about how they steal keys.
Their illegal proxy has over 3500 users.
NOTE: they know that you guys are looking and they started hiding their proxy's main page. Consider a sinkhole.

Main proxy with 3500 users(main page hidden): https://charybdis.scylla.wtf

Stat page unhidden: https://charybdis.scylla.wtf/status (they forgot to hide this)

Other proxy(main page not hidden): https://unicorn.scylla.wtf

The more advanced proxy software these people use: https://gitgud.io/Drago/oai-reverse-proxy (also written by drago the main ring leader)
Other fork: https://gitgud.io/yae-miko/oai-reverse-proxy/ (written by another person known as asakuri the assistant leader)

Related proxy by another person known as asakuri in the same discord available in the scylla.wtf domain:
https://rentry.org/GuujiYaeProxy
https:// guujiyae.me/

Note: they are lying about the keys being donated. These people are stealing the keys. This is just a straight up lie.

This is a real enterprise unlike the other group you are looking for. Sekrit, khanon, fiz are NOT the enterprise. These guys have potentially stolen millions of dollars from stolen azure and aws keys. Including dall-e stolen from upper tier customers with specific dall-e instances without any safety filters!
Link to the illegal azure proxy ran by drago and asakuri: https://shark-lost-brilliant-harbor.trycloudflare.com/

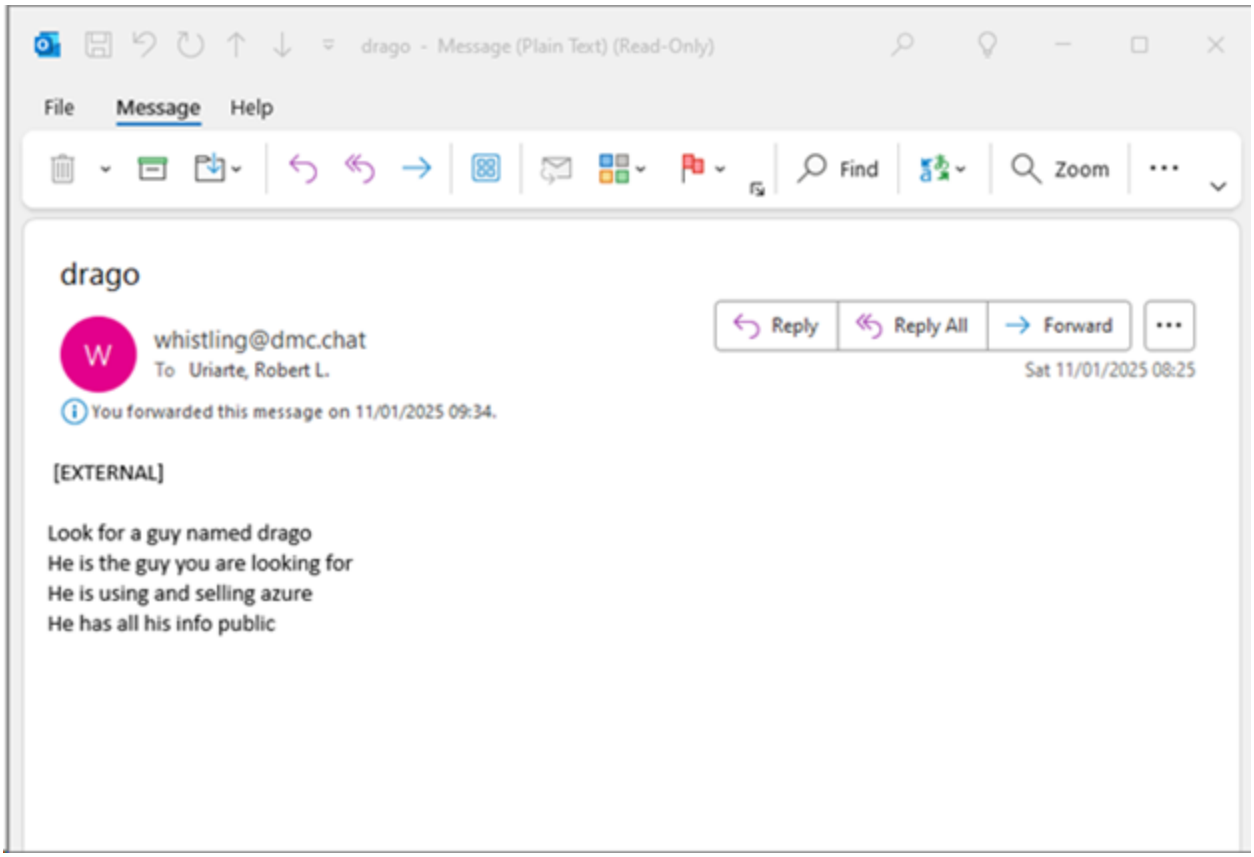
Attached screenshots in case they take it down.

You can find a lot of proof and info in the provided Discord server.

notable people:

dragOn3xt
Mr. Yae (asakuri)
rarestmeow

NOTE: these people are professionals. Consider restraining orders. I can provide you with more info if necessary.



Screenshots of emails received by counsel of record.

This reaction underscores the impact of Microsoft's legal actions and demonstrates how these measures can effectively disrupt a cybercriminal network by seizing infrastructure and create a powerful deterrent impact among its members.

Continuing our commitment to combatting the abuse of generative AI.

We take the misuse of AI very seriously, recognizing the serious and lasting impacts of abusive imagery for victims. Microsoft remains committed to protecting users by embedding robust AI guardrails and safeguarding our services from illegal and harmful content. Last year, we committed to continuing to innovate on new ways to keep users safe by outlining a comprehensive approach to combat abusive AI-generated content. We published a whitepaper with recommendations for U.S. policymakers on modernizing criminal law to equip law enforcement with the tools necessary to bring bad actors to justice. We also provided an update on our approach to intimate image abuse, detailing the steps we take to protect our services from such harm, whether synthetic or otherwise.

As we've said before, no disruption is complete in one day. Going after malicious actors requires persistence and ongoing vigilance. By unmasking these individuals and shining a light on their malicious activities, Microsoft aims to set a precedent in the fight against AI technology misuse.

Tags: AI, cybercrime, Digital Crimes Unit, Microsoft Azure OpenAI Service, Microsoft Digital Crimes Unit, Responsible AI