Microsoft shares latest intelligence on North Korean and Chinese threat actors at CYBERWARCON | Microsoft Security Blog

By Microsoft Threat Intelligence

Published: 2024-11-22 · Archived: 2026-04-05 13:31:53 UTC

This year at CYBERWARCON, Microsoft Threat Intelligence analysts are sharing research and insights representing years of threat actor tracking, infrastructure monitoring and disruption, and attacker tooling.

The talk DPRK – All grown up will cover how the Democratic People's Republic of Korea (DPRK) has successfully built computer network exploitation capability over the past 10 years and how threat actors have enabled North Korea to steal billions of dollars in cryptocurrency as well as target organizations associated with satellites and weapons systems. Over this period, North Korean threat actors have developed and used multiple zero-day exploits and have become experts in cryptocurrency, blockchain, and AI technology.

This presentation will also include information on North Korea overcoming sanctions and other financial barriers by the United States and multiple other countries through the deployment of North Korean IT workers in Russia, China, and, other countries. These IT workers masquerade as individuals from countries other than North Korea to perform legitimate IT work and generate revenue for the regime. North Korean threat actors' focus areas are:

- Stealing money or cryptocurrency to help fund the North Korea weapons programs
- Stealing information pertaining to weapons systems, sanctions information, and policy-related decisions before they occur
- Performing IT work to generate revenue to help fund the North Korea IT weapons program

Meanwhile, in the talk No targets left behind, Microsoft Threat Intelligence analysts will present research on Storm-2077, a Chinese threat actor that conducts intelligence collection targeting government agencies and non-governmental organizations. This presentation will trace how Microsoft assembled the pieces of threat activity now tracked as Storm-2077 to demonstrate how we overcome challenges in tracking overlapping activities and attributing cyber operations originating from China.

This blog summarizes intelligence on threat actors covered by the two Microsoft presentations at CYBERWARCON.

Sapphire Sleet: Social engineering leading to cryptocurrency theft

The North Korean threat actor that Microsoft tracks as Sapphire Sleet has been conducting cryptocurrency theft as well as computer network exploitation activities since at least 2020. Microsoft's analysis of Sapphire Sleet activity indicates that over 10 million US dollars' worth of cryptocurrency was stolen by the threat actor from multiple companies over a six-month period.

Masquerading as a venture capitalist

While their methods have changed throughout the years, the primary scheme used by Sapphire Sleet over the past year and a half is to masquerade as a venture capitalist, feigning interest in investing in the target user's company. The threat actor sets up an online meeting with a target user. On the day of the meeting, when the target user attempts to connect to the meeting, the user receives either a frozen screen or an error message stating that the user should contact the room administrator or support team for assistance.

When the target contacts the threat actor, the threat actor sends a script – a *.scpt* file (Mac) or a Visual Basic Script (*.vbs*) file (Windows) – to "fix the connection issue". This script leads to malware being downloaded onto the target user's device. The threat actor then works towards obtaining cryptocurrency wallets and other credentials on the compromised device, enabling the threat actor to steal cryptocurrency.

Posing as recruiters

As a secondary method, Sapphire Sleet masquerades as a recruiter on professional platforms like LinkedIn and reaches out to potential victims. The threat actor, posing as a recruiter, tells the target user that they have a job they are trying to fill and believe that the user would be a good candidate. To validate the skills listed on the target user's profile, the threat actor asks the user to complete a skills assessment from a website under the threat actor's control. The threat actor sends the target user a sign-in account and password. In signing in to the website and downloading the code associated with the skills assessment, the target user downloads malware onto their device, allowing the attackers to gain access to the system.

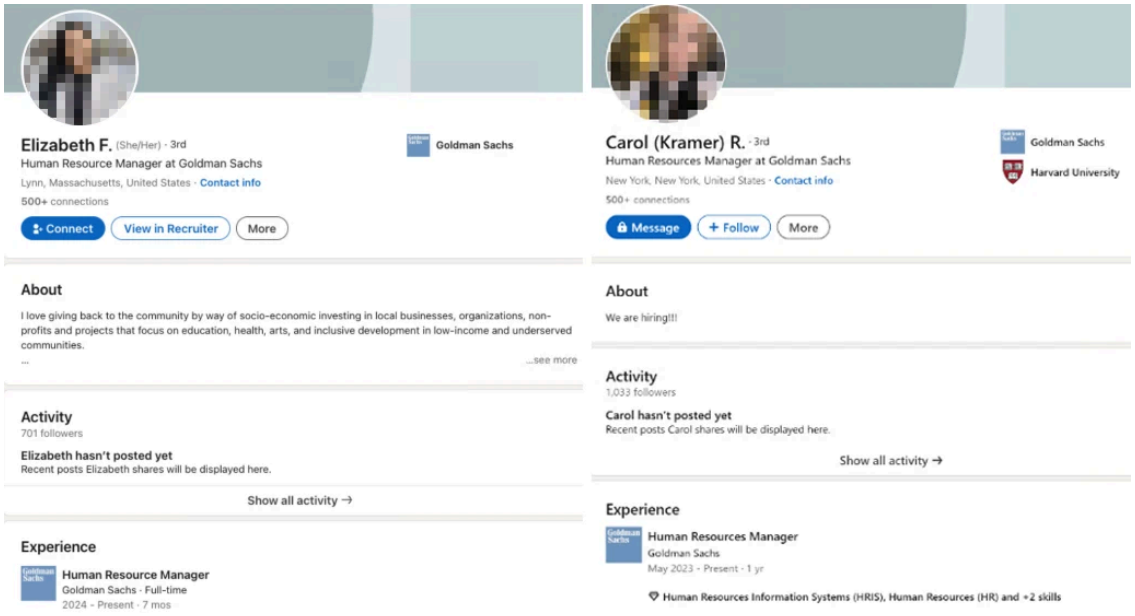

Figure 1. LinkedIn profiles of fake recruiters. LinkedIn accounts identified to be related to this attack have been taken down.

Ruby Sleet: Sophisticated phishing targeting satellite and weapons systems-related targets

Ruby Sleet, a threat actor that Microsoft has been tracking since 2020, has significantly increased the sophistication of their phishing operations over the past several years. The threat actor has been observed signing their malware with legitimate (but compromised) certificates obtained from victims they have compromised. The

threat actor has also distributed backdoored virtual private network (VPN) clients, installers, and various other legitimate software.

Ruby Sleet has also been observed conducting research on targets to find what specific software they run in their environment. The threat actor has developed custom capabilities tailored to specific targets. For example, in December 2023, Microsoft Threat Intelligence observed Ruby Sleet carrying out a supply chain attack in which the threat actor successfully compromised a Korean construction company and replaced a legitimate version of VeraPort software with a version that communicates with known Ruby Sleet infrastructure.

Ruby Sleet has targeted and successfully compromised aerospace and defense-related organizations. Stealing aerospace and defense-related technology may be used by North Korea to increase its understanding of missiles, drones, and other related technologies.

North Korean IT workers: The triple threat

In addition to utilizing computer network exploitation through the years, North Korea has dispatched thousands of IT workers abroad to earn money for the regime. These IT workers have brought in hundreds of millions of dollars for North Korea. We consider these North Korean IT workers to be a triple threat, because they:

- Make money for the regime by performing “legitimate” IT work
- May use their access to obtain sensitive intellectual property, source code, or trade secrets at the company
- Steal sensitive data from the company and in some cases ransom the company into paying them in exchange for not publicly disclosing the company’s data

Microsoft Threat Intelligence has observed North Korean IT workers operating out of North Korea, Russia, and China.

Facilitators complicate tracking of IT worker ecosystem

Microsoft Threat Intelligence observed that the activities of North Korean IT workers involved many different parties, from creating accounts on various platforms to accepting payments and moving money to North Korean IT worker-controlled accounts. This makes tracking their activities more challenging than traditional nation-state threat actors.

Since it’s difficult for a person in North Korea to sign up for things such as a bank account or phone number, the IT workers must utilize facilitators to help them acquire access to platforms where they can apply for remote jobs. These facilitators are used by the IT workers for tasks such as creating an account on a freelance job website. As the relationship builds, the IT workers may ask the facilitator to perform other tasks such as:

- Creating or renting their bank account to the North Korean IT worker
- Creating LinkedIn accounts to be used for contacting recruiters to obtain work
- Purchasing mobile phone numbers or SIM cards
- Creating additional accounts on freelance job sites

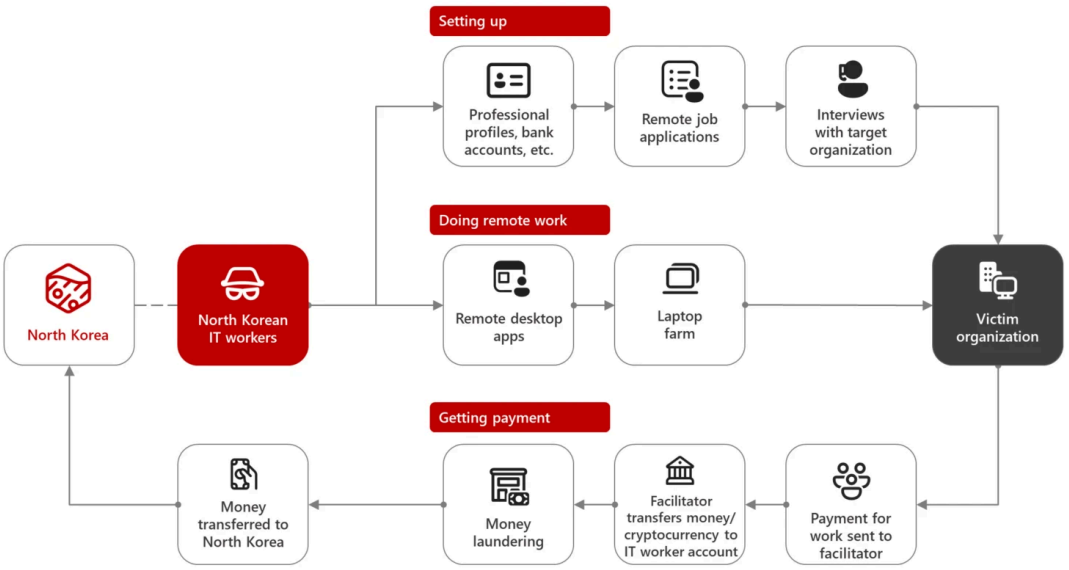

Figure 2. The North Korean IT worker ecosystem

Fake profiles and portfolios with the aid of AI

One of the first things a North Korean IT worker does is set up a portfolio to show supposed examples of their previous work. Microsoft Threat Intelligence has observed hundreds of fake profiles and portfolios for North Korean IT workers on developer platforms like GitHub.

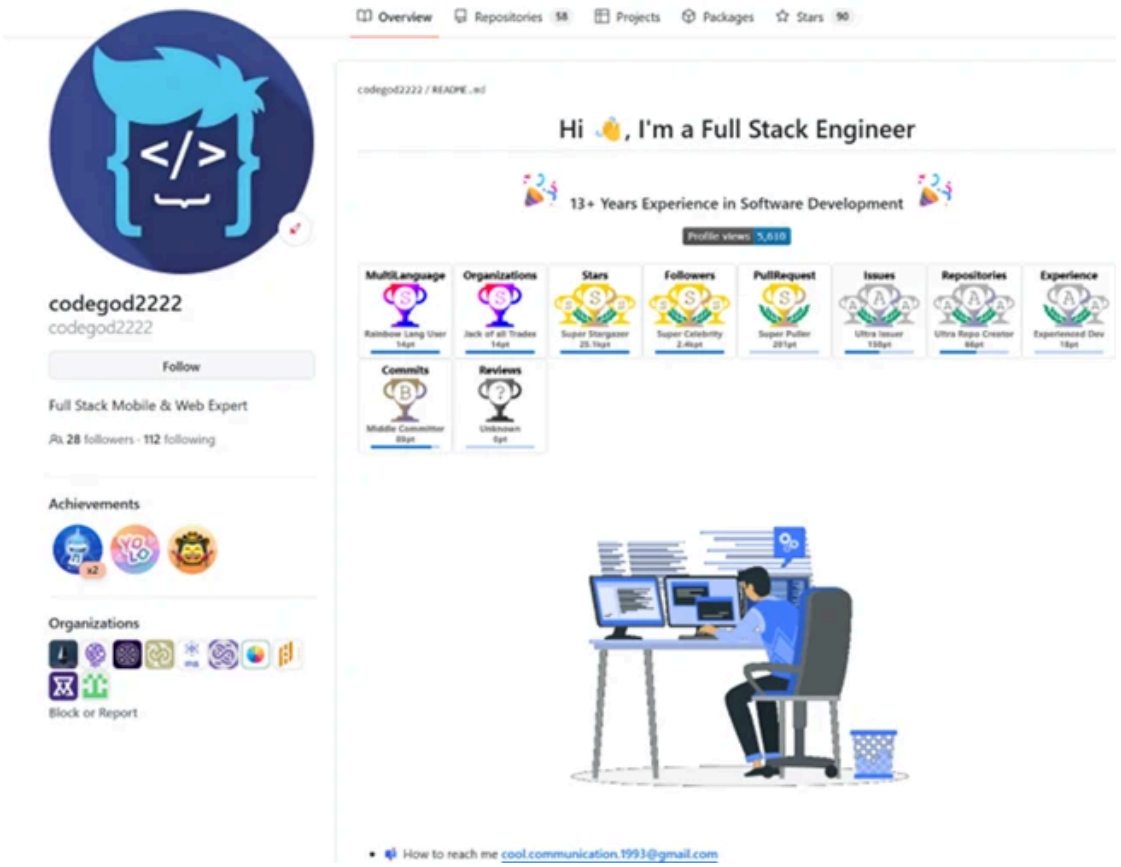

Figure 3. Example profile used by North Korean IT workers that has since been taken down.

Additionally, the North Korean IT workers have used fake profiles on LinkedIn to communicate with recruiters and apply for jobs.

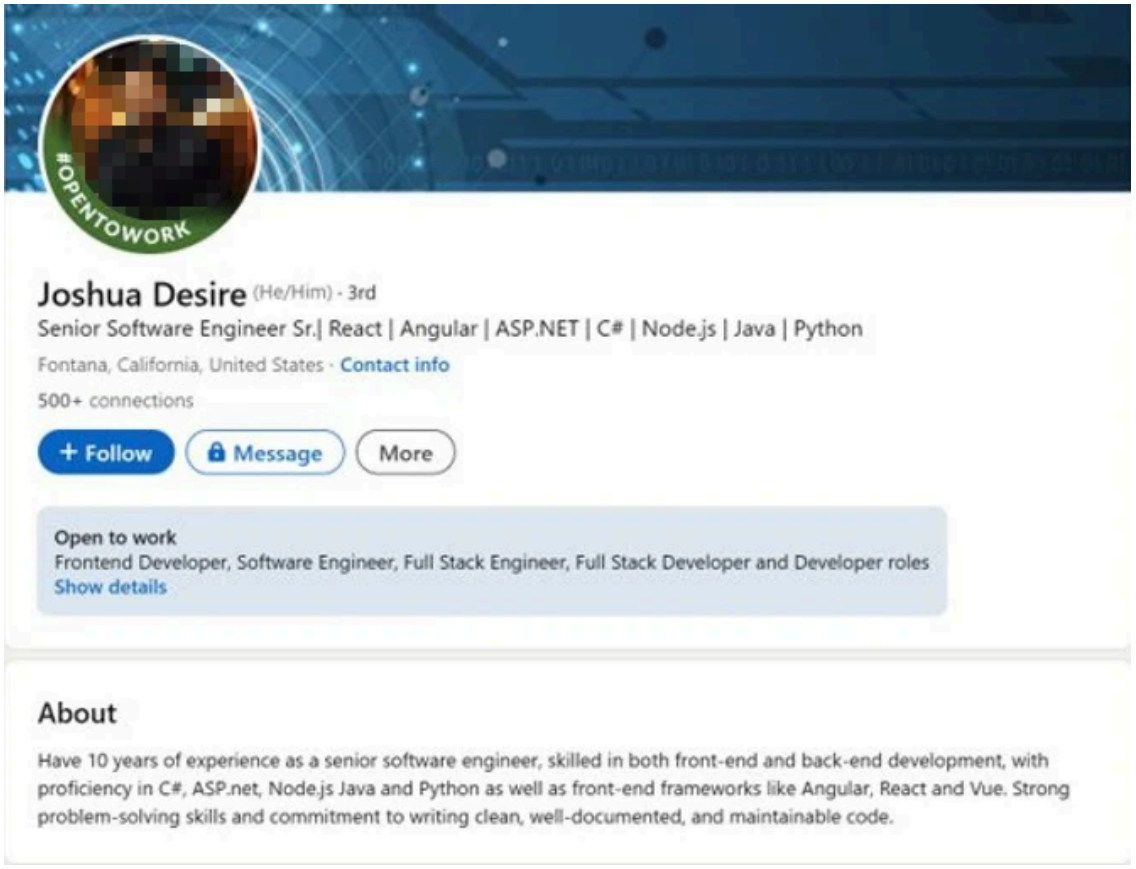

Figure 4. An example of a North Korean IT worker LinkedIn profile that has since been taken down.

In October 2024, Microsoft found a public repository containing North Korean IT worker files. The repository contained the following information:

- Resumes and email accounts used by the North Korean IT workers
- Infrastructure used by these workers (VPS and VPN accounts along with specific VPS IP addresses)
- Playbooks on conducting identity theft and creating and bidding jobs on freelancer websites without getting flagged
- Actual images and AI-enhanced images of suspected North Korean IT workers
- Wallet information and suspected payments made to facilitators
- LinkedIn, GitHub, Upwork, TeamViewer, Telegram, and Skype accounts
- Tracking sheet of work performed and payments received by these IT workers

Review of the repository indicates that the North Korean IT workers are conducting identity theft and using AI tools such as Faceswap to move their picture over to documents that they have stolen from victims. The attackers are also using Faceswap to take pictures of the North Korean IT workers and move them to more professional looking settings. The pictures created by the North Korean IT workers using AI tools are then utilized on resumes or profiles, sometimes for multiple personas, that are submitted for job applications.

Figure 5. Use of AI apps to modify photos used for North Korean IT workers' resumes and profiles

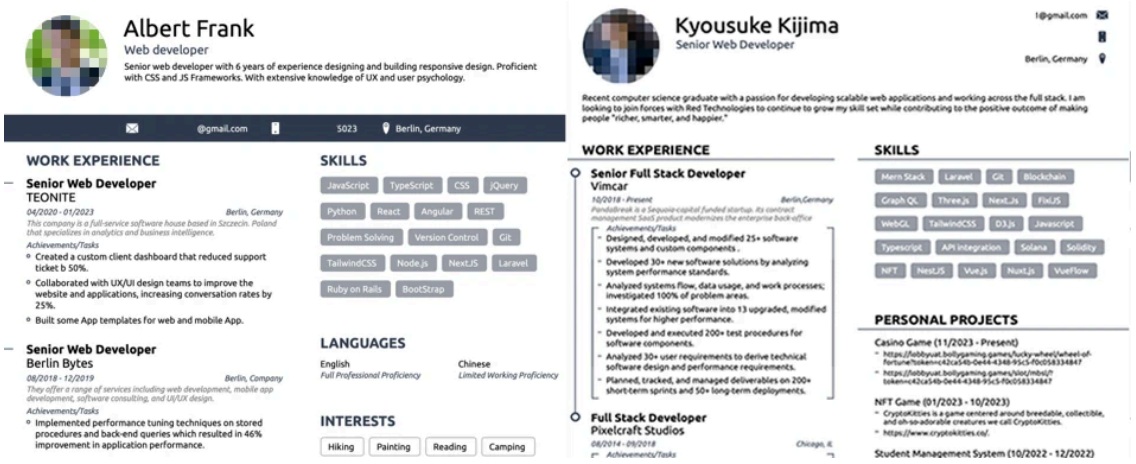

Figure 6. Examples of resumes for North Korean IT workers. These two resumes use different versions of the same photo.

In the same repository, Microsoft Threat Intelligence found photos that appear to be of North Korean IT workers:

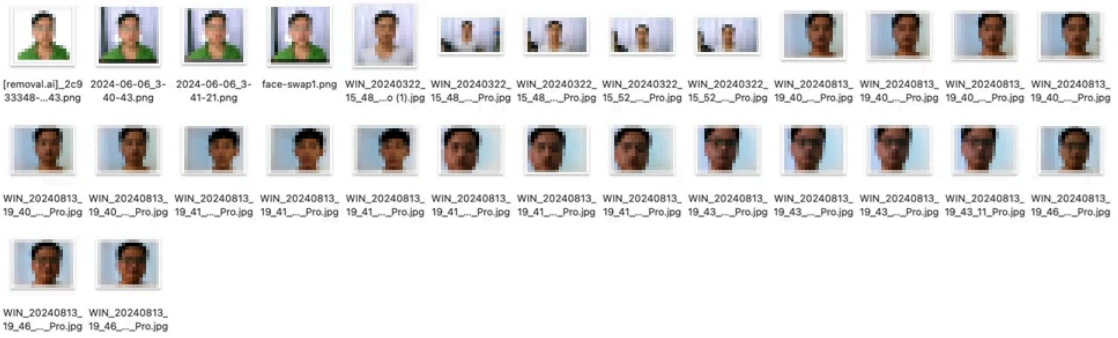

Figure 7. Photos of potential North Korean IT workers

Microsoft has observed that, in addition to using AI to assist with creating images used with job applications, North Korean IT workers are experimenting with other AI technologies such as voice-changing software. This

aligns with observations shared in earlier blogs showing threat actors using AI as a productivity tool to refine their attack techniques. While we do not see threat actors using combined AI voice and video products as a tactic, we do recognize that if actors were to combine these technologies, it's possible that future campaigns may involve IT workers using these programs to attempt to trick interviewers into thinking they are not communicating with a North Korean IT worker. If successful, this could allow the North Korean IT workers to do interviews directly and not have to rely on facilitators obtaining work for them by standing in on interviews or selling account access to them.

Getting payment for remote work

The North Korean IT workers appear to be very organized when it comes to tracking payments received. Overall, this group of North Korean IT workers appears to have made at least 370,000 US dollars through their efforts.

Protecting organizations from North Korean IT workers

Unfortunately, computer network exploitation and use of IT workers is a low-risk, high-reward technique used by North Korean threat actors. Here are some steps that organizations can take to be better protected:

- Follow guidance from the US Department of State, US Department of the Treasury, and the Federal Bureau of Investigation on how to spot North Korean IT workers.
- Educate human resources managers, hiring managers, and program managers for signs to look for when dealing with suspected North Korean IT workers.
- Use simple non-technical techniques such as asking IT workers to turn on their camera periodically and comparing the person on camera with the one that picked up the laptop from your organization.
- Ask the person on camera to walk through or explain code that they purportedly wrote.

Storm-2077: No targets left behind

Over the past decade, following numerous government indictments and the public disclosure of threat actors' activities, tracking and attributing cyber operations originating from China has become increasingly challenging as the attackers adjust their tactics. These threat actors continue to conduct operations while using tooling and techniques against targets that often overlap with another threat actor's operation. While analyzing activity that was affecting a handful of customers, Microsoft Threat Intelligence assembled the pieces of what would be tracked as Storm-2077. Undoubtably, this actor had some victimology and operational techniques that overlapped with a couple of threat actors that Microsoft was already tracking.

Microsoft assesses that Storm-2077 is a China state threat actor that has been active since at least January 2024. Storm-2077 has targeted a wide variety of sectors, including government agencies and non-governmental organizations in the United States. As we continued to track Storm-2077, we observed that they went after several other industries worldwide, including the Defense Industrial Base (DIB), aviation, telecommunications, and financial and legal services. Storm-2077 overlaps with activity tracked by other security vendors as TAG-100.

We assess that Storm-2077 likely operates with the objective of conducting intelligence collection. Storm-2077 has used phishing emails to gain credentials and, in certain cases, likely exploited edge-facing devices to gain initial access. We have observed techniques that focus on email data theft, which could allow them to analyze the

data later without risking immediate loss of access. In some cases, Storm-2077 has used valid credentials harvested from the successful compromise of a system.

We've also observed Storm-2077 successfully exfiltrate emails by stealing credentials to access legitimate cloud applications such as eDiscovery applications. In other cases, Storm-2077 has been observed gaining access to cloud environments by harvesting credentials from compromised endpoints. Once administrative access was gained, Storm-2077 created their own application with mail read rights.

Access to email data is crucial for threat actors because it often contains sensitive information that could be utilized later for malicious purposes. Emails can include sign-in credentials, confidential communication, financial records, business secrets, intellectual property, and credentials for accessing critical systems, or employee information. Access to email accounts and the ability to steal email communication could enable an attacker to further their operations.

Microsoft's talk on Storm-2077 at CYBERWARCON will highlight how vast their targeting interest covers. All sectors appear to be on the table, leaving no targets behind. Our analysts will talk about the challenges of tracking China-based threat actors and how they had to distinctly carve out Storm-2077.

CYBERWARCON Recap

At this year's CYBERWARCON, Microsoft Security is sponsoring the post-event Fireside Recap. Hosted by Sherrod DeGrippo, this session will feature special guests who will dive into the highlights, key insights, and emerging themes that defined CYBERWARCON 2024. Interviews with speakers will offer exclusive insights and bring the conference's biggest moments into sharp focus.

Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn at https://www.linkedin.com/showcase/microsoft-threat-intelligence, and on X (formerly Twitter) at https://twitter.com/MsftSecIntel.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: https://thecyberwire.com/podcasts/microsoft-threat-intelligence.
