

Imposter for hire: How fake people can gain very real access



Uncovering imposters in the hiring pipeline

In this, our 7th cyberattack series report, we explore the case of a customer who spotted red flags around a remote developer job applicant—mismatched photos, altered documents, and odd voice characteristics—and engaged [Microsoft Incident Response](#) (also known as DART) to help. What began as a proactive engagement focused on early detection and threat hunting quickly evolved into a reactive investigation. Supported by Microsoft Threat Intelligence, we traced the activity to North Korea’s remote IT workforce. Operatives used AI-edited identities, voice changers, virtual private networks (VPNs), and remote monitoring and management (RMM) tools utilized by facilitators **to infiltrate companies, steal data, and generate revenue** for the Democratic People's Republic of Korea (DPRK). Microsoft tracks this threat actor activity as Jasper Sleet and related clusters.

Read on to learn more about their tactics, the tradecraft and tools they use, how Microsoft Incident Response countered their actions and how organizations can detect, investigate, and eradicate this unique security threat.



What happened?



The attack flow



How did Microsoft respond?



What can customers do to strengthen defenses?

What happened?

A total of four user accounts were observed connecting PiKVM devices to their workstations. These devices allow for remote access and control of other computers via the network. By connecting a PiKVM device to their employer-provided workstations, unknown third-parties could perform remote, hands-on activity, on the workstation as if they were sitting there themselves. Using this technique, the threat actor was able to extract sensitive information from the targeted network.

Microsoft Incident Response employed **eight key tools and methods** to investigate the threat from both a proactive viewpoint and a comprehensive response:

- 1 Cosmic** – Provides Azure and Microsoft Entra ID metadata and logs for security and configuration analysis
- 2 Arctic** – Provides Active Directory metadata for security and configuration analysis
- 3 Fennec** – Microsoft Incident Response's proprietary incident response and threat detection tool with custom workloads focused on collecting evidence from Windows, Linux & macOS hosts
- 4 Contextual, forensic metadata from a device** – select event log entries, registry keys, running processes, and configuration data
- 5 Microsoft Entra ID Protection**
- 6 Microsoft Defender for Endpoint**
- 7 Microsoft Defender for Identity**
- 8 Microsoft Defender for Cloud Apps**

January 2025
audit log clearing event is observed.

ADFind.exe
(a command-line tool utilized by threat actors for post-exploitation reconnaissance) was created in C:\Tools in February.

Initial distinct USB mount event attaching a PiKVM device. A total of 17 mount events took place in June.

Distinct USB mount event attaching a PiKVM device to a customer device for remote computer management in June.

Second distinct USB mount event attaching a PiKVM device in July.

Initial loss of data (egress) begins using an unauthorized PiKVM device.

New event in series of USB mounts attaching a PiKVM device. A total of 5 USB mount events attaching PiKVM devices on one customer device.

August saw the **last event in a series of USB mount events** attaching a PiKVM device.

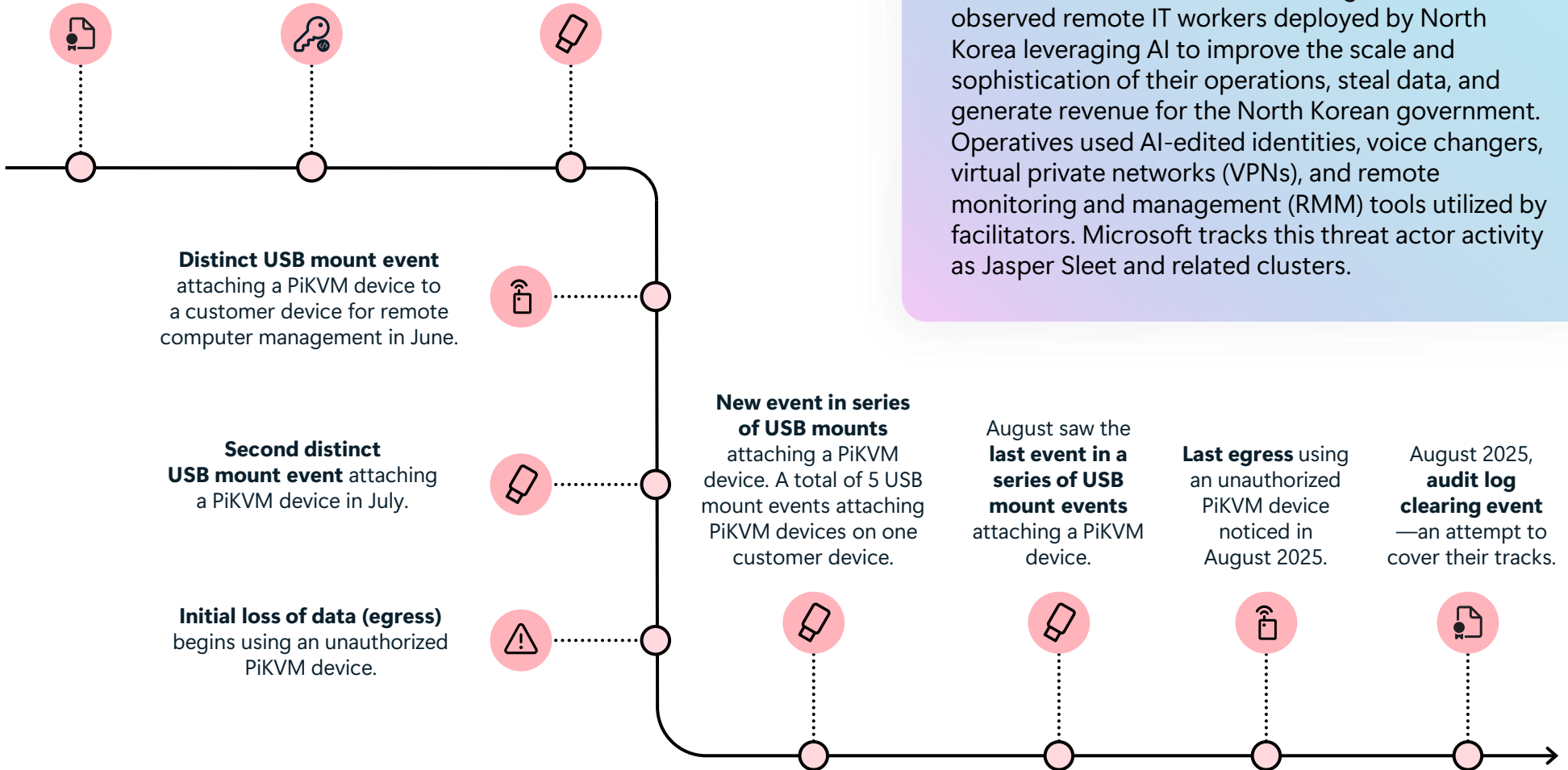
Last egress using an unauthorized PiKVM device noticed in August 2025.

August 2025, **audit log clearing event**—an attempt to cover their tracks.



The attack flow

Since 2024, Microsoft Threat Intelligence has observed remote IT workers deployed by North Korea leveraging AI to improve the scale and sophistication of their operations, steal data, and generate revenue for the North Korean government. Operatives used AI-edited identities, voice changers, virtual private networks (VPNs), and remote monitoring and management (RMM) tools utilized by facilitators. Microsoft tracks this threat actor activity as Jasper Sleet and related clusters.



How did Microsoft respond?

Recognizing the potential impact, Microsoft Incident Response took immediate steps to respond to the threats.

Microsoft directly notified targeted customers, shared information to secure their environments, and provided additional information on tactics, techniques, and procedures (TTPs) on our security blog. **Our response included:**

- Disabling accounts used by the threat actor.
- Remotely restoring any devices associated with the threat actor activity to a backup dated to before the threat activity.
- Conducting a comprehensive extraction and behavioral analysis of Unified Audit Log entries, focusing on activities surrounding the compromised identities. As part of this, Microsoft used the Unified Audit Log data to identify the threat actors' interactions and activities, including what files and emails they may have accessed.
- Leveraging Microsoft Defender for Identity and Microsoft Defender for Endpoint to detect anomalous authentication patterns, lateral movement, and credential misuse across hybrid identity infrastructures.

Additionally, given the unique TTPs and ongoing threat, Microsoft suspended 3,000 accounts known to have been created by North Korean IT workers as part of the activities to disrupt the wider, global threat campaign and protect customers.



INSIGHT

Recent Gartner research reveals that surveyed employers report they are increasingly concerned about candidate fraud. **Gartner predicts that by 2028, one in four candidate profiles worldwide will be fake**, with possible security repercussions far beyond simply making “a bad hire.”¹



INSIGHT

The **deployment of remote IT workers under false identities** went beyond every day security threats. These operatives successfully infiltrated customer environments by posing as legitimate hires, often using AI-generated resumes, falsified documents, and voice changers to pass interviews and onboarding processes. Once embedded, they leveraged corporate trust to gain access to sensitive systems and data.



TACTIC

PiKVM devices

Low-cost, hardware-based remote access tools—were utilized as egress channels. These devices allowed threat actors to maintain persistent, out-of-band access to systems, bypassing traditional endpoint detection and response (EDR) controls. In one case, an identity linked to Jasper Sleet authenticated into the environment via PiKVM, enabling covert data exfiltration.

¹AI Fuels Mistrust Between Employers and Job Candidates; Recruiters Worry About Fraud, Candidates Fear Bias

What can customers do to strengthen their defenses?

Unlike many security incidents, multifactor authentication and improved security posture alone won't solve this threat. Today's remote-first workforce can introduce threats that look like leading job candidates, some of whom were reported to be talented, well-performing employees. To prevent similar exploitation in the future, organizations must compliment SOC alerting and actions with a robust insider-threat strategy supported by Data Loss Prevention (DLP) and compliance policies. Human Resource leadership must implement stricter pre-employment vetting and employees must be blocked from using unapproved IT management tools.

The following steps can help companies prepare for similar incidents:



IMPROVE VISIBILITY

Enable Microsoft 365 Defender and Unified Audit Logs integration (a feature of Microsoft 365 within the Microsoft Purview Compliance portal) to improve visibility and response capabilities.



MANAGE INSIDER THREATS

Leverage Insider Risk Management in Microsoft Purview to identify and mitigate risky user behavior.



PROTECT SENSITIVE DATA

Implement Data Loss Prevention (DLP) policies in Microsoft Purview to monitor and safeguard sensitive data across storage, transmission and user activities.



BEWARE OF USB DEVICES

Monitor, alert and respond to the attachment of USB devices, specifically PiKVM devices.



STAY UP TO DATE

Periodically review the Threat Analytics dashboard in Microsoft Defender as it shows high priority and prevalent attack techniques.



ACT ON ALERTS

Review, annotate and close Microsoft Defender alerts.



FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

Thoroughly vet any potential employees before employment, and ensure employees are only given the minimum privileges necessary to do their role.

Conclusion

Microsoft Incident Response proved critical in identifying systemic gaps and restoring control. But this incident in particular serves as a stark reminder that security is everyone's priority in an organization, and threats can go well beyond the usual TTPs. The incident revealed sophisticated and evolving tradecraft employed by the North Korean threat actor Jasper Sleet, whose operations continue to challenge traditional detection paradigms. Rather than relying on malware or overt exploitation, Jasper Sleet exploited human trust. Their approach hinges on social engineering, impersonation, and trusted access—a strategy that has unfortunately proven both stealthy and scalable.

Learn more about how DART can help you before, during, and after a security incident:

Learn more

