Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Void Blizzard Isn't Knocking It's Already Inside 20+ NGO Networks

Date of Publication	Admiralty Code	TA Number
May 29, 2025	A1	TA2025166

Summary

Active Since: April 2024
Threat Actor: Void Blizzard (aka Laundry Bear)
Targeted Countries: North America, Europe, NATO Members
Targeted Industries: Aviation, Defense, Education, Government, Healthcare, IT, Law Enforcement, Media, NGO, Telecommunications, Transportation
Attack: Void Blizzard, a Russia-backed espionage group active since 2024, is accelerating a relentless campaign against NATO, Ukraine, and critical sectors like defense, aviation, and government operations, not through sophisticated exploits, but by hijacking the weakest link, the stolen credentials.

Attack Timeline

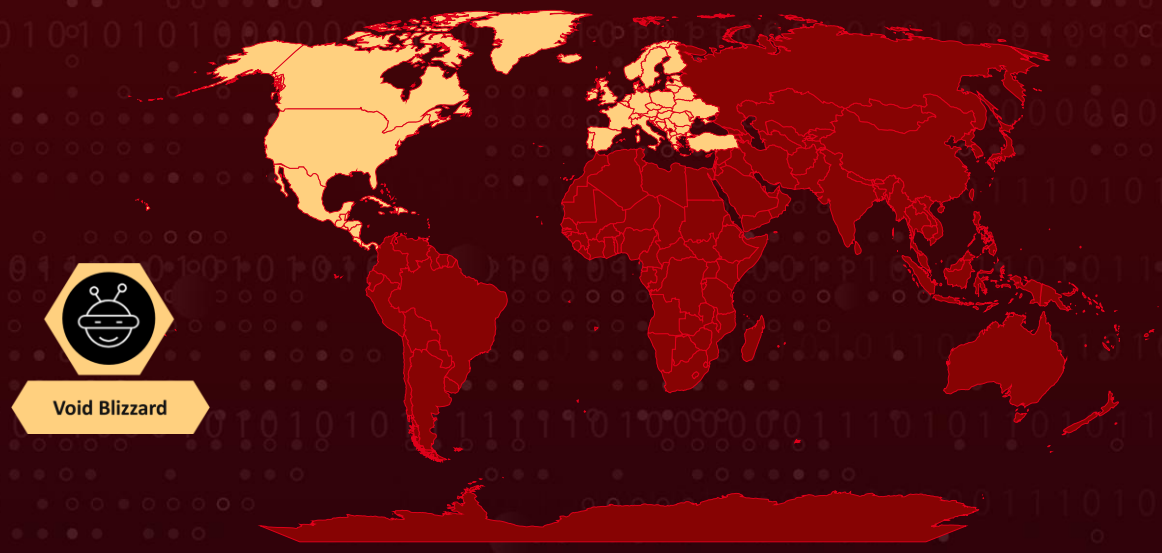
April 2024 — **Void Blizzard** identified as a **Russia-affiliated** threat actor

September 2024 — Hacked **Dutch** organizations, targeting **military equipment intel**

October 2024 — Compromised accounts at a **Ukrainian aviation** organization

April 2025 — Launched AitM spear phishing campaign against **20+ NGOs** in **Europe** & the **US**

Attack Regions



Attack Details

#1 Void Blizzard, also known as Laundry Bear, is a Russia-affiliated threat actor active since at least April 2024. The group is engaged in espionage operations, predominantly targeting entities that serve Russian state interests, with a particular focus on government, law enforcement, and military organizations within NATO member states and Ukraine.

#2 A significant incident occurred in October 2024, when Void Blizzard successfully compromised several accounts at a Ukrainian aviation organization, a target previously attacked by Seashell Blizzard, a GRU-linked actor, in 2022. This persistent targeting highlights Russia's sustained strategic interest in aviation-related sectors since the start of its invasion of Ukraine.

#3 Void Blizzard refined its tactics by introducing more direct credential harvesting techniques, notably through spear phishing campaigns. These operations impersonated trusted entities to deceive targets into surrendering their login credentials. The group also acquires cookies and login data through criminal marketplaces, leveraging this information to infiltrate platforms like Exchange Online and SharePoint Online for data theft.

#4 In April 2025, the group launched a notable adversary-in-the-middle (AitM) phishing campaign, targeting over 20 non-governmental organizations across Europe and the United States. This operation utilized a typosquatted domain mimicking Microsoft Entra's authentication portal, disguised as invitations to a fabricated European Defense and Security Summit.

#5 Malicious PDF attachments embedded with QR codes redirected recipients to a phishing site hosted on micsrosoftonline[.]com, designed to capture both login credentials and session cookies. Void Blizzard employed Evilginx, an open-source AitM phishing framework, to intercept authentication data, effectively bypassing multi-factor authentication mechanisms.

#6 Following a successful compromise, the group exploits legitimate cloud service APIs such as Microsoft Graph and Exchange Online to enumerate user mailboxes and cloud-stored files. Their data collection methods are likely automated, enabling bulk extraction of data from compromised accounts, file shares, and accessible folders.

#7 Void Blizzard’s pivot toward sophisticated phishing and exploitation of cloud environments exposes critical risks to sensitive data, decision-making processes, and operational resilience. This reinforces the imperative for identity-centric security and proactive cloud defense strategies at the highest levels of organizational oversight.

Recommendations

Centralized Identity Management: Consolidate all identity management into a unified platform such as Microsoft Entra. Integrating on-premises directories with cloud directories will provide centralized monitoring, enabling quicker detection of malicious access attempts. Additionally, synchronizing user accounts, excluding privileged accounts, between on-prem and cloud environments enhances security while maintaining separation between environments.

Implement Mailbox Auditing: Ensure mailbox auditing is enabled by default for all mailboxes to log actions performed by mailbox owners, delegates, and administrators. This helps track any unauthorized activities and detect potential breaches quickly.

Review and Strengthen Cloud Application Security: Implement proactive security measures such as continuous monitoring and anomaly detection for cloud apps. Ensure that any suspicious behavior is flagged, investigated, and mitigated promptly to avoid further compromise.

Simulate Attacks and Phishing Drills: Conduct regular exercises to simulate sophisticated attacks, including phishing campaigns and identity-based intrusions, mimicking tactics used by threat actors like Void Blizzard. These exercises test your organization's ability to detect, respond to, and mitigate these threats in real time.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1078 Valid Accounts	T1078.004 Cloud Accounts

T1566 Phishing	T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link	T1557 Adversary-in-the-Middle
T1204 User Execution	T1204.002 Malicious File	T1586 Compromise Accounts	T1586.003 Cloud Accounts
T1588 Obtain Capabilities	T1588.002 Tool	T1110.003 Password Spraying	T1550.004 Web Session Cookie
T1552.001 Credentials In Files	T1087 Account Discovery	T1087.004 Cloud Account	T1018 Remote System Discovery
T1082 System Information Discovery	T1114 Email Collection	T1114.002 Remote Email Collection	T1530 Data from Cloud Storage
T1119 Automated Collection	T1071.001 Web Protocols		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	micsrosoftonline[.]com, ebsumrnit[.]eu, outlook-office[.]micsrosoftonline[.]com
SHA256	06a5bd9cb3038e3eec1c68cb34fc3f64933dba2983e39a0b1125af8af32c8ddb

References

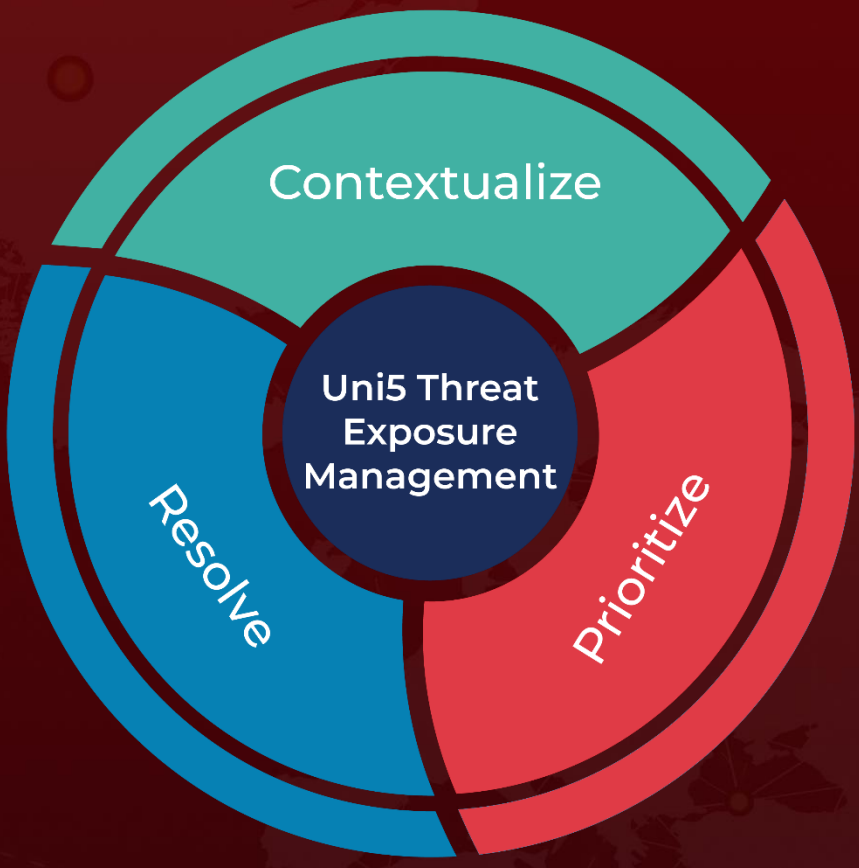
https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/

https://www.aivd.nl/actueel/nieuws/2025/05/27/onbekende-russische-groep-achter-hacks-nederlandse-doelen

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 29, 2025 • 5:30 AM

More at www.hivepro.com