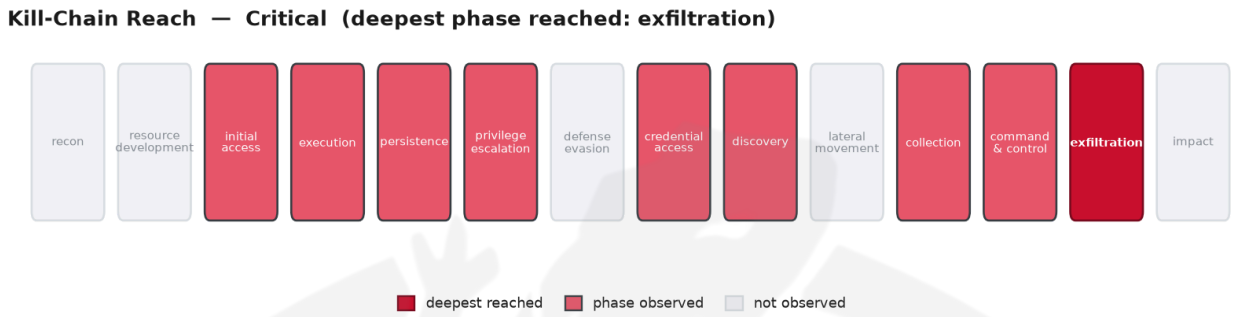
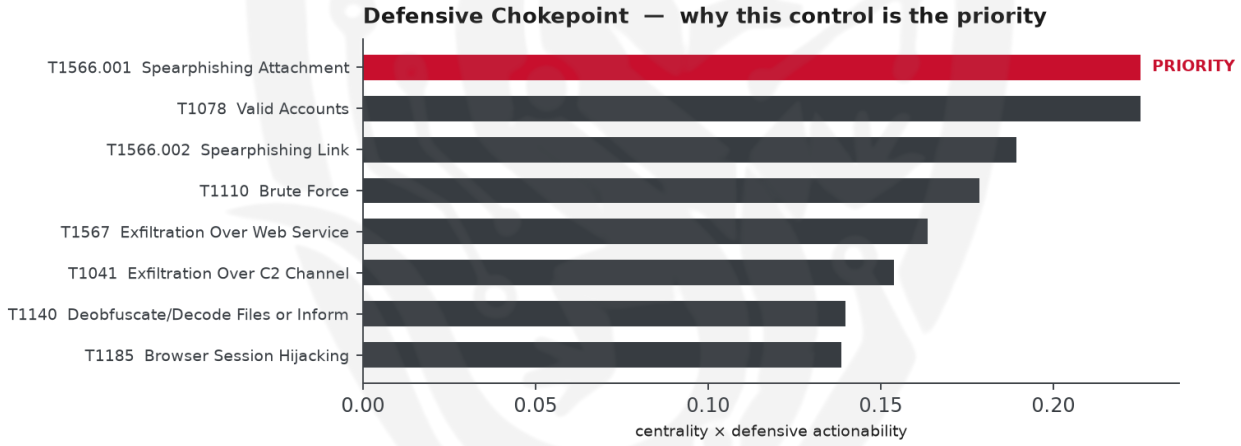
# THREAT REPORT: VOID BLIZZARD

## Visual Summary




How far down the attack chain this campaign reached; deepest phase in crimson.




The control that most disrupts the attack (priority in crimson).

## Summary

The source attributes this activity to Void Blizzard, a threat actor targeting Ukraine's government, defense, transportation, and finance sectors. The actor is exploiting CVE-2025-66376 to carry out their operations. Priority should be given to patching this vulnerability on all affected systems to prevent further compromise. The threat actor's use of spearphishing attachments as a primary technique necessitates immediate attention to email security.

## Threat Overview

Void Blizzard, the attributed threat actor, is exploiting CVE-2025-66376, although the specific malware families used are not sufficiently identified. The actor is targeting various sectors in Ukraine, including government, defense, transportation, and finance, indicating a broad range of interests. The exploitation of this vulnerability allows the actor to engage in a range of malicious activities.

## Attack Chain and Priority Control

The observed techniques form a complex chain, starting with initial access techniques such as spearphishing, followed by system information discovery, and culminating in exfiltration over web services. The priority technique identified is T1566.001 Spearphishing Attachment, which serves as a critical chokepoint in the attack chain. To counter this, the recommended priority control is to "Patch CVE-2025-66376 on all affected systems as the top priority, then: Sandbox and detonate email attachments; block executable/script archive contents at the gateway; strip mark-of-the-web bypass; user report-phish button."

## Infrastructure and Corroboration

The malicious infrastructure associated with this activity is hosted by providers such as Mulgin Alexander Sergeevich and Global Connectivity Solutions LLP. However, according to abuse.ch, there are no corroborated malware families associated with this activity. Additionally, AbuseIPDB does not flag any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. These findings are attributed to their respective sources, abuse.ch and AbuseIPDB.

---

## Technical Appendix

*Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.*

### Observed Techniques (ATT&CK, expert-tagged by source)

- T1056.001 Keylogging
- T1059.007 JavaScript
- T1539 Steal Web Session Cookie
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1567 Exfiltration Over Web Service
- T1185 Browser Session Hijacking
- T1016 System Network Configuration Discovery
- T1087 Account Discovery
- T1114.003 Email Forwarding Rule
- T1041 Exfiltration Over C2 Channel
- T1110 Brute Force
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1114.002 Remote Email Collection
- T1189 Drive-by Compromise
- T1071.001 Web Protocols

## Analytical Scores

- Priority technique (graph chokepoint): T1566.001 Spearphishing Attachment (centrality 0.2253).
- Operational risk: Critical (score 0.968, reaches exfiltration).

## Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5021; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

| Historical Profile | Behavioural Overlap |
|---|---|
| FIN4 | 0.5021 |
| Winter Vivern | 0.4082 |
| Windshift | 0.375 |
| APT19 | 0.3608 |
| Ke3chang | 0.36 |

## Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

## Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

| Type | Indicator | Context |
|---|---|---|
| IP | 185[.]86[.]79[.]95 | AbuseIPDB 0% (UA) · AS201094 Mulgin Alexander Sergeevich |
| IP | 194[.]156[.]103[.]193 | AbuseIPDB 0% (AM) · AS215540 Global Connectivity Solutions LLP |
| Domain | zimbra-metadata[.]com | |
| Domain | emailanalytics[.]com[.]ua | |
| Domain | mailnalysis[.]com | |
| Domain | analyticemailmeter[.]com | |

| Type | Indicator | Context |
|---|---|---|
| Domain | zimbrastat[.]com | |
| Domain | zimbrasoft[.]com[.]ua | |
| Domain | istc-cloud[.]com | |
| Domain | synacorzimbra[.]nl | |
| Domain | zmailanalytics[.]com | |

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

## Flame Cell // Adversary Pivot [ BETA ]

*BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com*

- **Control applied:** T1566.001 Spearphishing Attachment (initial-access)
- **Observed here:** Void Blizzard used T1078 Valid Accounts here as an alternative initial-access technique.
- **Projected pivot:** T1078 Valid Accounts (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

Void Blizzard could pivot to using T1078 Valid Accounts by exploiting existing credentials that were not compromised during the initial spearphishing attempt, potentially using them to maintain access or escalate privileges within the network. This technique may allow Void Blizzard to blend in with normal user activity, making it more challenging to detect their presence. To counter this, the defensive control would be to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

**Detection and hardening for the pivot (T1078 Valid Accounts)**

- **Telemetry:** Windows Security (logon events); Azure AD / IdP sign-in logs; VPN and remote-access logs; Proxy / DLP / data-egress volume telemetry
- **Detect:**
  - Security 4624/4625 (logon success/fail), 4768/4769 (Kerberos TGT/TGS), 4776 (NTLM)
  - Impossible-travel, new-geo, and off-hours sign-ins from the IdP
  - Service or dormant accounts logging on interactively
  - Under valid credentials the identity signal goes quiet: baseline per-account data-egress volume and alert on peer-group and historical deviation (the real exfiltration tell)
- **Harden:**
  - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
  - Least-privilege review; separate admin from daily-driver accounts
  - Set per-account and per-partner egress baselines with DLP thresholds on sensitive stores

- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account