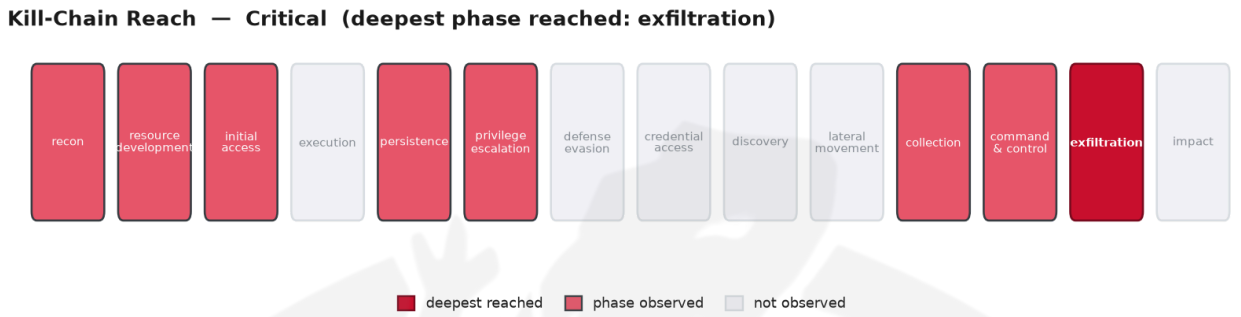
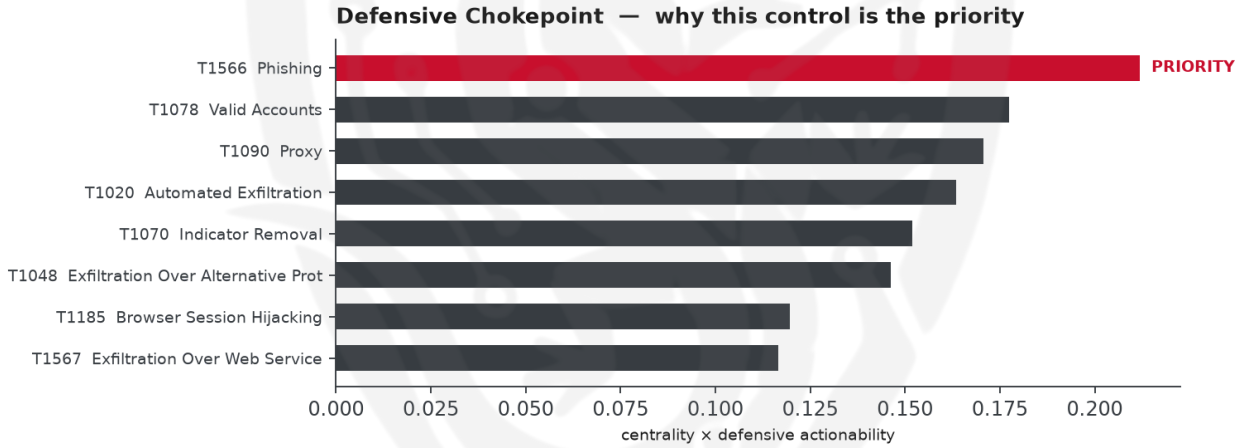
THREAT REPORT: VOID BLIZZARD

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 various sectors in the United States of America, including Education, Finance, and Government. The threat actor is utilizing multiple techniques to compromise victim networks, with a priority focus on phishing attacks. Priority should be given to defensive actions that mitigate phishing threats. The actor's campaign poses a critical operational risk due to the potential for exfiltration.

Threat Overview

Void Blizzard, the observed threat actor, is targeting organizations in multiple sectors, leveraging various techniques such as external remote services, email collection, and application layer protocol exploitation. The central vulnerability or malware family used in the attack is not specified due to insufficient data. The threat actor's activities are focused on compromising victim accounts, gathering identity information, and exfiltrating data over web services.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including external remote services, email collection, and phishing attacks. The priority technique is T1566 Phishing, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to: Enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with the threat actor's infrastructure. Additionally, no malware families have been corroborated by abuse.ch, and AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

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

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

- T1133 External Remote Services
- T1114 Email Collection
- T1071 Application Layer Protocol
- T1562 Impair Defenses
- T1567 Exfiltration Over Web Service
- T1589 Gather Victim Identity Information
- T1185 Browser Session Hijacking
- T1090 Proxy
- T1020 Automated Exfiltration
- T1588.001 Malware
- T1070 Indicator Removal
- T1586 Compromise Accounts
- T1590 Gather Victim Network Information
- T1048 Exfiltration Over Alternative Protocol
- T1588.002 Tool
- T1566 Phishing
- T1078 Valid Accounts
- T1573 Encrypted Channel
- T1598 Phishing for Information
- T1213 Data from Information Repositories

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2119).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3873; 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
PittyTiger	0.3873
POLONIUM	0.3371
FIN5	0.3354
Star Blizzard	0.3213
APT28	0.315

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
Domain	Instagram[.]com
Domain	ebsummlt[.]eu
Domain	miscrsosoft[.]com
Domain	ffice365[.]com
Domain	micsroft[.]com
URL	hxxp://Instagram[.]com/wlsperrrrr/

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.k@3sdragon.eu

- **Control applied:** T1566 Phishing (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).

The Void Blizzard actor could pivot to using T1078 Valid Accounts by attempting to leverage compromised credentials obtained through previous phishing attempts or other means to maintain access to the target network, potentially exploiting weak password policies or unsecured accounts. They may try to use these valid accounts to blend in with normal user activity, making it more challenging to detect their presence. To counter this, the mandated defensive control of Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons should be implemented.

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
- **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
- **Harden:**
  - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
  - Least-privilege review; separate admin from daily-driver accounts
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account