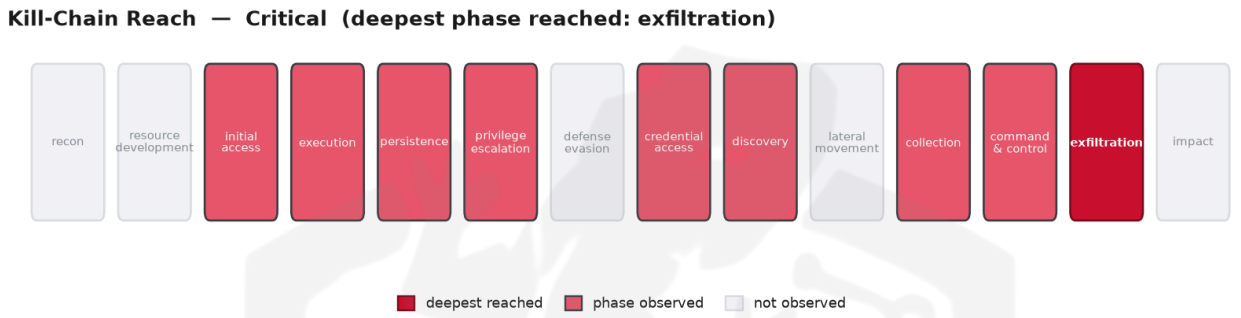
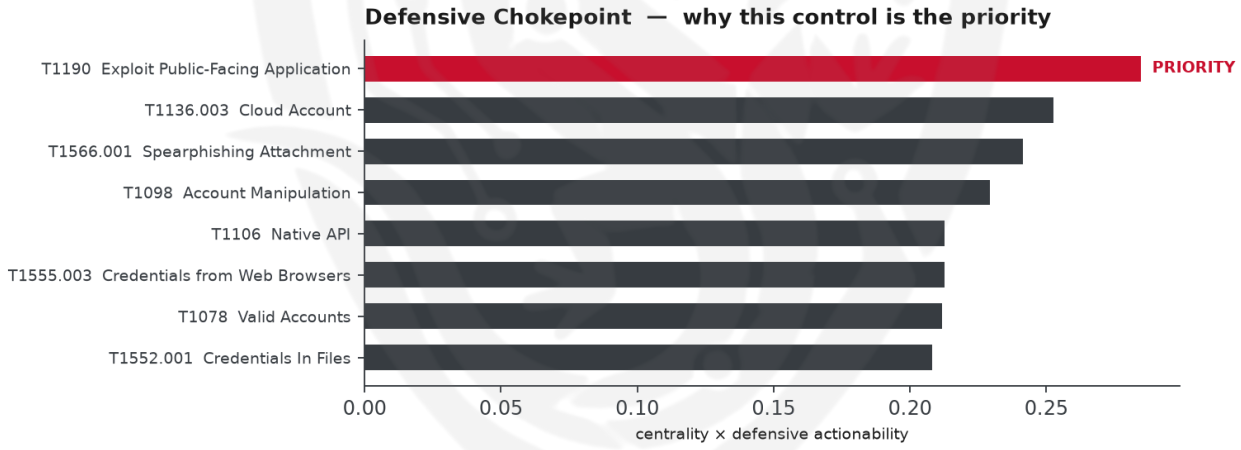
THREAT REPORT: TA488 ZIMBRA MAILSERVERS CAMPAIGN

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 TA488, who has been targeting Zimbra mailservers in the United States of America and Ukraine with the ZimReaper malware, exploiting the CVE-2025-66376 vulnerability. The targeted sectors include Government, Defense, Energy, and Education. Priority should be given to patching the affected systems to prevent further exploitation. The threat actor's actions have reached a critical operational risk band, indicating a high level of exfiltration.

Threat Overview

TA488 has been observed using the ZimReaper malware to exploit the CVE-2025-66376 vulnerability in Zimbra mailservers. The targeted countries are the United States of America and Ukraine, with a focus on

the Government, Defense, Energy, and Education sectors. The malware family used is ZimReaper, and the central CVE exploited is CVE-2025-66376.

Attack Chain and Priority Control

The observed techniques used by TA488 form a complex attack chain, involving various methods such as standard encoding, JavaScript, and external remote services. The priority technique is T1190 Exploit Public-Facing Application, which is the graph chokepoint. To mitigate this threat, the priority control is to: Patch CVE-2025-66376 on all affected systems as the top priority, then: Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this campaign. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB 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)

- T1132.001 Standard Encoding
- T1059.007 JavaScript
- T1133 External Remote Services
- T1539 Steal Web Session Cookie
- T1071.004 DNS
- T1566.001 Spearphishing Attachment
- T1106 Native API
- T1190 Exploit Public-Facing Application
- T1087.003 Email Account
- T1555.003 Credentials from Web Browsers
- T1020 Automated Exfiltration
- T1552.001 Credentials In Files
- T1041 Exfiltration Over C2 Channel
- T1136.003 Cloud Account
- T1098 Account Manipulation
- T1078 Valid Accounts
- T1114.002 Remote Email Collection
- T1203 Exploitation for Client Execution
- T1567.002 Exfiltration to Cloud Storage
- T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.2846).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3668; 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
APT33	0.3668
TA505	0.3269
Leafminer	0.317
Kimsuky	0.3159
MuddyWater	0.3149

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	zimbra-metadata[.]com
Domain	emailanalytics[.]com[.]ua
Domain	mailnalysis[.]com
Domain	analyticemailmeter[.]com
Domain	zimbrastat[.]com
Domain	zimbrasoft[.]com[.]ua

Type	Indicator
Domain	istc-cloud[.]com
Domain	synacorzimbra[.]nl
Domain	zmailanalytics[.]com
Hash	c010f64080b0b0997b362a8e6b9c618e
Hash	e3ce7d13a83716594787a12edf6cbeedc76b9a65
Hash	98df604ecc57f884a2e6ce3266a0013ad64455cac48442c2312cfa4765007aaf
Hash	1517b3caa495f6c4e832df9c75fc94667e3c233773f7fa4e056d5e30e5ead760
Hash	60db9abae75cd8ccc49dd7ea5feb41677566dcd442f12ebc5745ffd2810fb874
Hash	b1f5beb1175fc5c7d1806a2f0d900eb124c54f0286c5c52b66eea7a6633adb1d

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:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** TA488 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 adversary, TA488, could pivot to using T1078 Valid Accounts to maintain access and achieve their objectives by potentially exploiting weak passwords or authentication procedures on existing accounts. They may attempt to use compromised credentials to blend in with normal user activity, which would likely require the defender to enhance their account monitoring and authentication controls. The defensive countermeasure to mitigate this potential pivot is 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