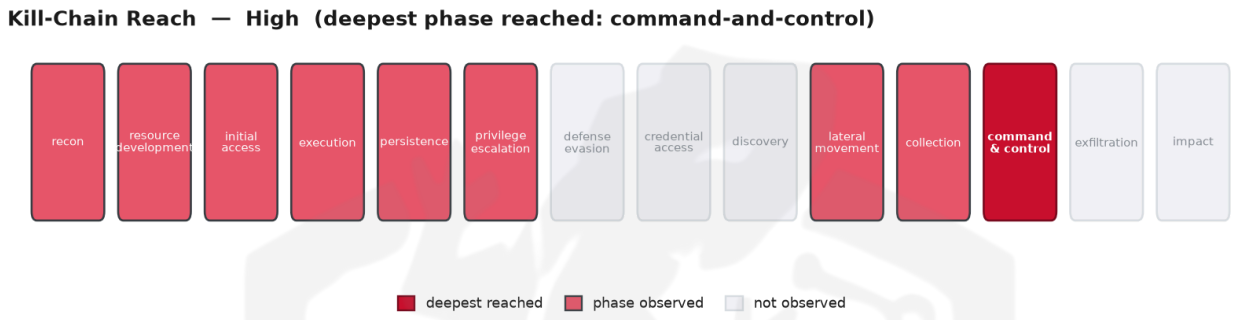
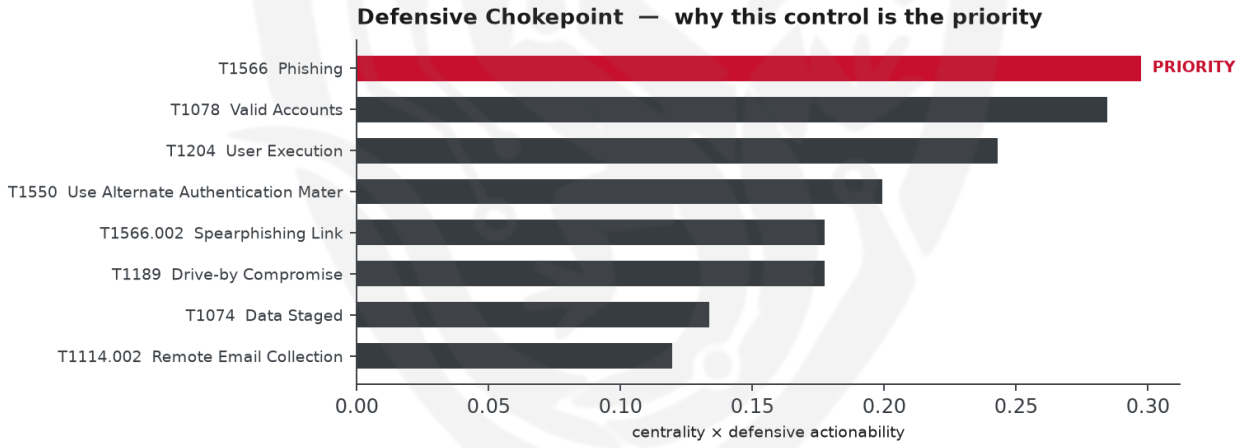
THREAT REPORT: UNKNOWN_ADVERSARY PHISHING CAMPAIGN

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 observed cluster of activity targets organizations in the United States and several European countries, including Austria, Belgium, France, Germany, Italy, Norway, Portugal, Slovenia, Spain, and Sweden. The threat actor is exploiting various techniques to compromise Microsoft 365 accounts, with a focus on phishing attacks. Priority should be given to enabling defensive measures to prevent account takeover. The campaign's operational risk band is considered high, reaching the level of command-and-control.

Threat Overview

The threat actor, whose identity is unknown, is utilizing a range of techniques, including phishing, email collection, and compromise of email accounts, to target Microsoft 365 users. The actor is exploiting

various vulnerabilities, but no specific CVE has been identified. The targeted sectors and malware families used are also unknown.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving initial phishing attempts, followed by email collection, and ultimately, compromise of email accounts. The priority technique identified is T1566 Phishing, which serves as a chokepoint in the attack chain. To mitigate this threat, the recommended 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

The malicious infrastructure associated with this campaign is hosted on LINKdotNET. While no malware families have been corroborated by abuse.ch, some indicators have been flagged by AbuseIPDB with a confidence level of up to 77%. However, none of these indicators have reached the 80% confidence threshold.

Technical Appendix

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

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

- T1583 Acquire Infrastructure
- T1213.002 Sharepoint
- T1114 Email Collection
- T1566.002 Spearphishing Link
- T1598.003 Spearphishing Link
- T1586.002 Email Accounts
- T1583.001 Domains
- T1550 Use Alternate Authentication Material
- T1074 Data Staged
- T1586 Compromise Accounts
- T1204 User Execution
- T1566 Phishing
- T1078 Valid Accounts
- T1114.002 Remote Email Collection
- T1598 Phishing for Information
- T1213 Data from Information Repositories
- T1189 Drive-by Compromise
- T1071.001 Web Protocols
- T1204.001 Malicious Link
- T1078.004 Cloud Accounts

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2973).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4703; 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
Star Blizzard	0.4703
FIN4	0.4392
WIRTE	0.4041
TA577	0.3948
APT28	0.3843

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 77%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	41[.]128[.]0[.]142	AbuseIPDB 77% (EG) · AS24863 LINKdotNET
Domain	buenne[.]de	
Domain	enerdizerandtron[.]de	
Domain	ihrsupportcenter[.]de	
Domain	rundwasser[.]de	
Domain	sonnenbrillenspot[.]de	

Type	Indicator	Context
Domain	dwbud[.]vilaribit[.]com	
Domain	abal[.]my	
Domain	starwellmedia[.]com	
Domain	aabiz[.]de	
Domain	aspireglobal[.]ltd	
Domain	dufllot[.]sbs	
Domain	espaciocf[.]de	
Domain	ilersls[.]org	
Domain	aaalen[.]de	
Domain	smartcontrolengineer[.]com	
Domain	trisrnareprjdocz[.]com	
Domain	razen[.]online	
Domain	theoceanac[.]online	
Domain	jumpast[.]es	
Domain	crm-technik[.]de	
Domain	klenpare[.]com	
Domain	uvarnix[.]cfd	
Domain	xavon[.]sbs	

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 Phishing (initial-access)
- **Observed here:** the threat actor 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 actor could pivot to using T1078 Valid Accounts to maintain access and achieve their objectives, potentially by compromising or reusing existing credentials that were not affected by the phishing block. This technique may allow the actor to blend in with normal user activity, making it more challenging to detect their presence. The defensive countermeasure to mitigate this 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