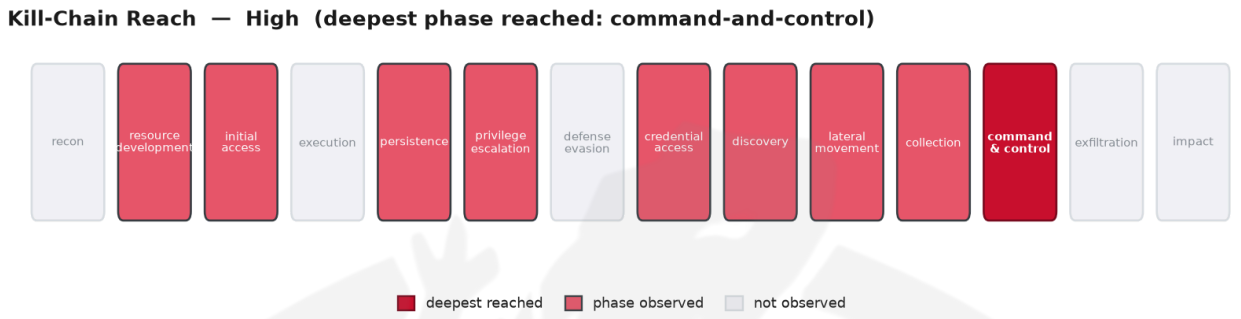
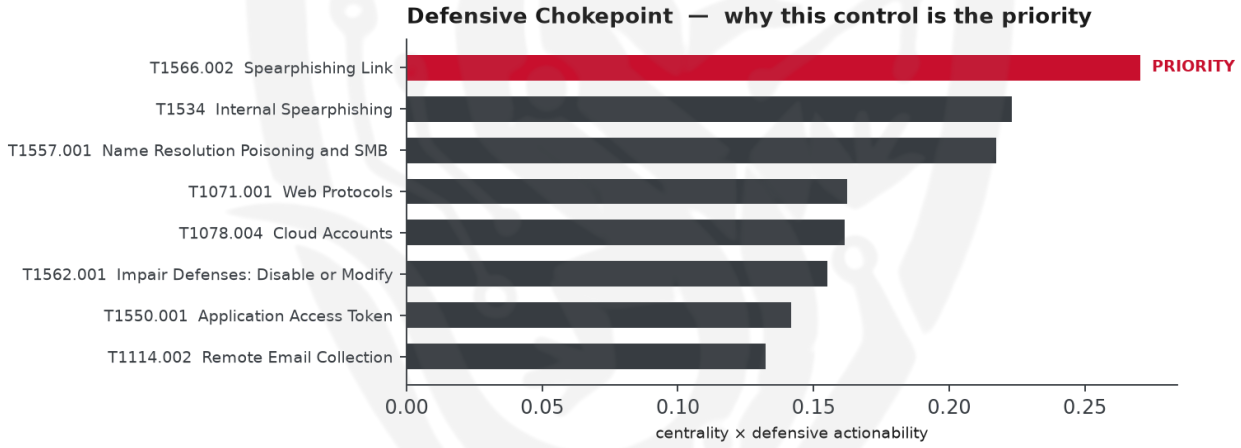
THREAT REPORT: STORM-2755 CAMPAIGN

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 Storm-2755, a threat actor targeting various sectors in the United States of America and Canada, including Healthcare, Education, Manufacturing, and Government. The actor's techniques involve multiple methods to compromise business email, emphasizing the need for defensive measures against social-engineering delivery. Priority should be given to hardening email and link security to mitigate potential attacks. The threat actor's campaign highlights the importance of robust security controls to prevent compromise.

Threat Overview

Storm-2755, the observed threat actor, utilizes a range of techniques to target organizations, including Sharepoint exploitation, stealing web session cookies, and spearphishing. The targeted sectors are diverse, indicating a broad campaign. While specific malware families and central CVEs are not identified,

the actor's techniques suggest a sophisticated approach to compromising business email and internal systems.

Attack Chain and Priority Control

The attack chain involves multiple techniques, including spearphishing links, internal spearphishing, and impairing defenses. The priority technique identified is T1566.002 Spearphishing Link, which serves as a critical point in the attack chain. To counter this, the priority control is to "Harden against social-engineering delivery across email, links and voice/callback lures: attachment sandboxing and link rewriting, block macro-enabled Office docs from the internet zone, train users to verify unexpected requests out-of-band, deploy a report-phish button, and enforce phishing-resistant MFA."

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs used by the threat actor, as indicated by "n/a" in the infrastructure observations. Additionally, no malware families have been corroborated by abuse.ch, and AbuseIPDB confidence levels for indicators are at 0%, suggesting that third-party corroboration does not provide additional insights into the infrastructure used by Storm-2755.

Technical Appendix

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

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

- T1213.002 Sharepoint
- T1539 Steal Web Session Cookie
- T1036.005 Match Legitimate Resource Name or Location
- T1087.002 Domain Account
- T1497.001 System Checks
- T1566.002 Spearphishing Link
- T1583.001 Domains
- T1557.001 Name Resolution Poisoning and SMB Relay
- T1087.004 Cloud Account
- T1534 Internal Spearphishing
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1114.002 Remote Email Collection
- T1071.001 Web Protocols
- T1584.004 Server
- T1550.001 Application Access Token
- T1078.004 Cloud Accounts
- T1090.001 Internal Proxy
- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1566.002 Spearphishing Link (centrality 0.3042).
- 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 0.3293; 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
APT1	0.3293
FIN4	0.3213
VOID MANTICORE	0.3081
WIRTE	0.3049
APT28	0.3005

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	idp[.]kualabemo[.]com
Domain	idp[.]keyreniao[.]com
Domain	idp[.]korminel[.]com
Domain	msauth[.]monlinelogicaline[.]com
Domain	mslogin[.]milocaroline[.]com
Domain	msonline[.]logicalineonline[.]com

Type	Indicator
Domain	office[.]ofrecie[.]com

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:** T1566.002 Spearphishing Link (initial-access)
- **Observed here:** T1566.002 Spearphishing Link was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1204 User Execution (execution)
- **Basis:** of the 89+ groups that use Spearphishing Link, this pairing runs 1.6x above base rate, a disproportionately-coupled move rather than the obvious one.

Storm-2755 could pivot to T1204 User Execution as a means to maintain their campaign momentum by tricking users into manually executing malicious files, potentially exploiting the trust users have in files they themselves have downloaded, which may bypass initial spearphishing link defenses. This technique may be particularly appealing as it leverages social engineering to bypass technical controls, relying on users to willingly execute the malicious payload. To counter this, the defensive control of blocking execution of downloaded HTA/JS/LNK, enforcing mark-of-the-web, disabling Office macros from the internet, and promoting user awareness on lures would likely be effective.

Also plausible (same tactic): T1203 Exploitation for Client Execution (n=38, lift 1.6), T1053 Scheduled Task/Job (n=43, lift 1.3)

Detection and hardening for the pivot (T1204 User Execution)

- **Telemetry:** Endpoint process telemetry; Email/proxy logs
- **Detect:**
  - User double-clicking archive/ISO/LNK contents that spawn interpreters
  - Mark-of-the-Web on delivered files; LOLBIN execution from user temp paths
- **Harden:**
  - Block risky file types; ASR rules; user awareness training
  - Application control to stop execution from user-writable directories
- **MITRE:** M1049 Antivirus/Antimalware, M1038 Execution Prevention, M1017 User Training · DS0009 Process, DS0022 File