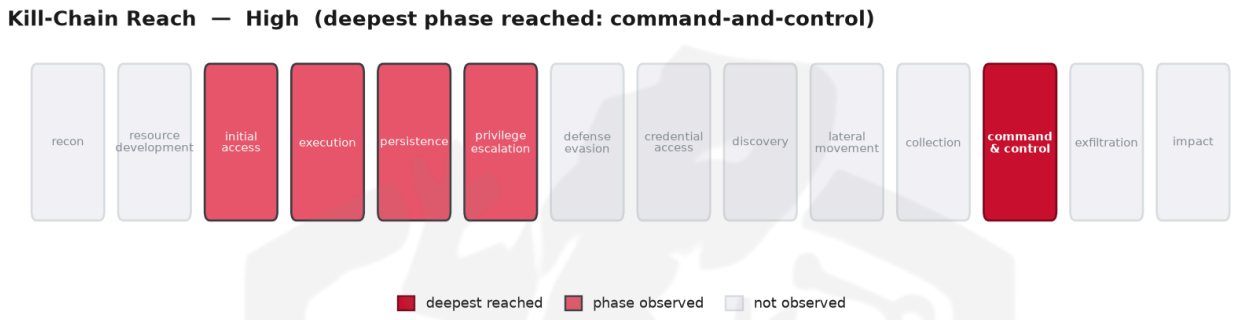
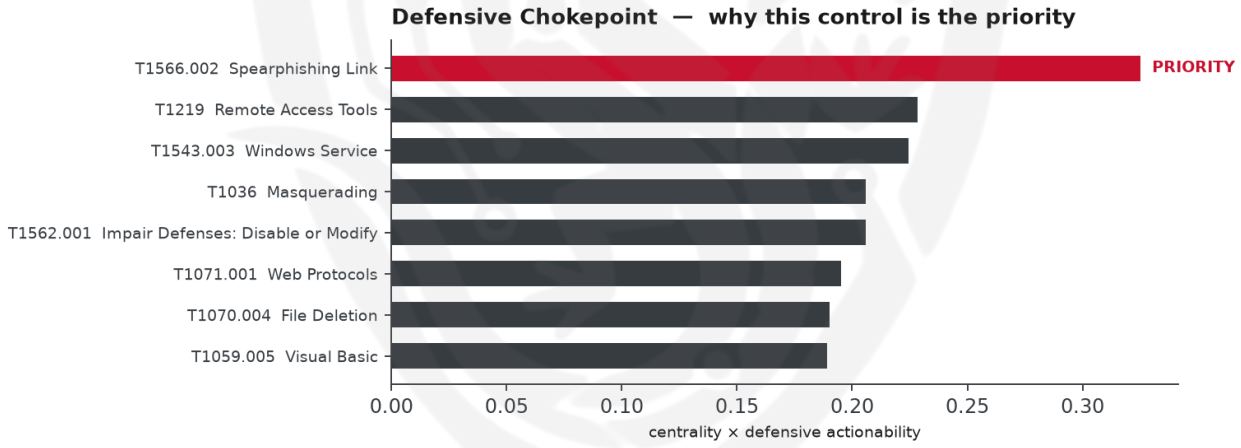
THREAT REPORT: UNATTRIBUTED DOCUSIGN KIT CAMPAIGN

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 involves the use of malware families such as MeshAgent, ScreenConnect, SimpleHelp, and UEMSAgent, targeting Windows systems. The priority defensive action should be given to enabling attachment sandboxing and link rewriting, as well as blocking macro-enabled Office documents from the internet zone. The campaign's impact is considered high, reaching the command-and-control stage. The threat actor's identity and targeted country remain unknown.

Threat Overview

The threat actor, whose identity is unknown, utilizes various malware families, including MeshAgent, ScreenConnect, SimpleHelp, and UEMSAgent. The central vulnerability exploited in this campaign is

unknown. The victimology and targeted sectors are also insufficiently understood, making it challenging to determine the specific goals of the threat actor.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including bypassing user account control, using Windows services, and impairing defenses. However, the priority technique is T1566.002 Spearphishing Link, 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 available information on the hosting providers or ASNs observed in this campaign. Additionally, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB, 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)

- T1548.002 Bypass User Account Control
- T1543.003 Windows Service
- T1566.002 Spearphishing Link
- T1219 Remote Access Tools
- T1036 Masquerading
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1070.004 File Deletion
- T1071.001 Web Protocols
- T1059.005 Visual Basic
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1566.002 Spearphishing Link (centrality 0.3252).
- Operational risk: High (score 0.594, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5331; 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
Evilnum	0.5331
Cobalt Group	0.5013
Windshift	0.4216
Metador	0.4
Rancor	0.3873

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	i8reactorsee[.]xyz
Domain	magroys[.]lat
Domain	rosetomaz[.]com[.]br
URL	hxxps://rosetomaz[.]com[.]br/it/
URL	hxxps://spearbit[.]com/license/check[.]php?[.][.][.]
URL	hxxps://spearbit[.]com/meshagents?[.][.][.]
Hash	2a206b085fedf8b20d1db883814c15e0202617da223dbb4e28b7109df98645df
Hash	4f1c8de304a855c2a4d1995b41069641dee84f1b51b6fb4a6e24eee59c6a30e4

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.

The actor could pivot to T1204 User Execution to maintain their objective by tricking users into executing malicious files, which may be disguised as legitimate documents or applications, potentially exploiting the trust users have in files that appear to be from trusted sources. This technique is particularly concerning as it could be used in conjunction with social engineering tactics to convince users to execute malicious code, which would likely involve creating a sense of urgency or legitimacy around the file. The defensive control to counter this would be to block execution of downloaded HTA/JS/LNK; enforce mark-of-the-web; disable Office macros from the internet; user awareness on lures.

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