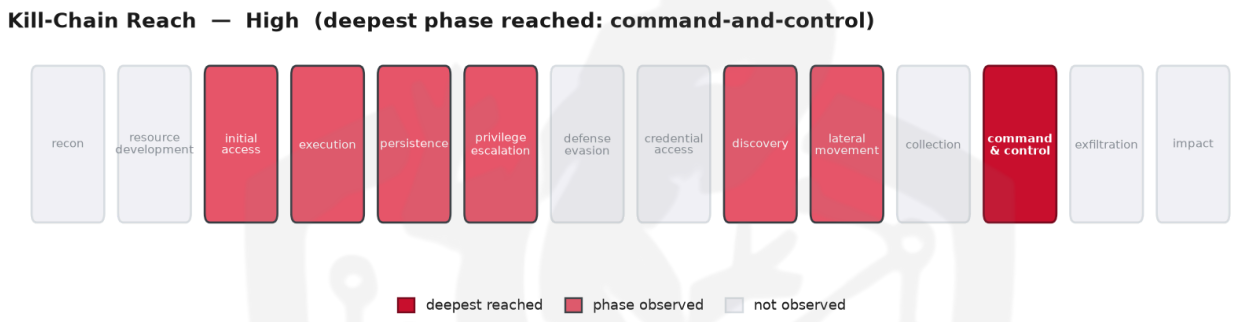
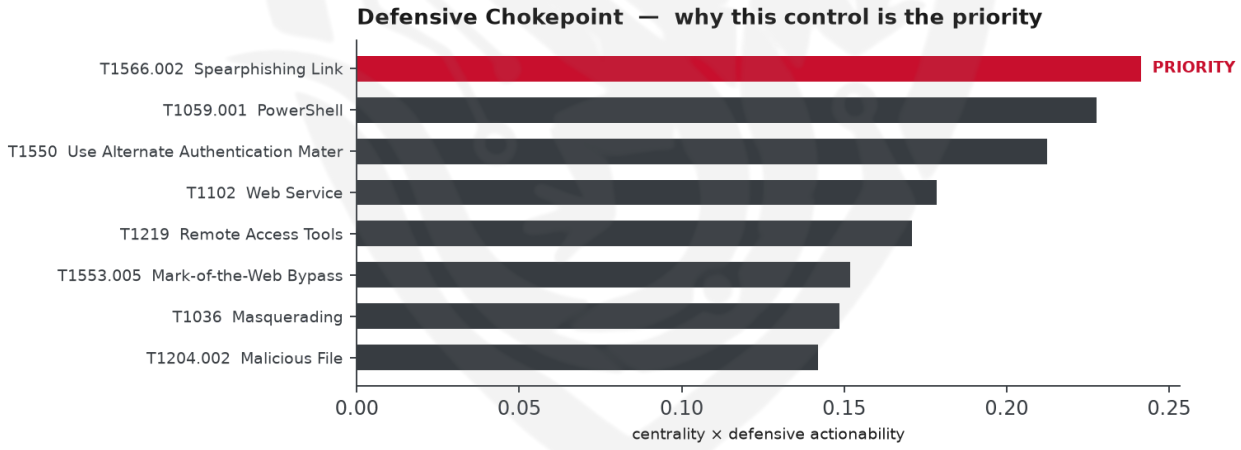
# THREAT REPORT: UNATTRIBUTED SCREENCONNECT RMM ABUSE AND CLOUDFLARE TUNNELING CAMPAIGN

## 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 exploitation of various techniques to gain unauthorized access to systems, with a focus on social-engineering delivery methods. The threat actor is leveraging techniques such as Windows Management Instrumentation, Create or Modify System Process, and Spearphishing Link to compromise targets. Priority should be given to hardening defenses against social-engineering attacks, as the operational risk band is considered High. The campaign's targets and sectors are currently unknown.

## Threat Overview

The threat actor, whose identity is currently unknown, is utilizing a range of techniques, including Windows Management Instrumentation, Create or Modify System Process, and Spearphishing Link, to compromise systems. The malware families and central CVE used in the campaign are currently unknown. The victimology of the campaign is also unknown, making it essential to focus on the technical mechanics of the attack to inform defensive strategies.

## Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, with the priority technique being T1566.002 Spearphishing Link. This technique is the graph chokepoint, indicating its crucial role in the campaign's success. To mitigate this threat, 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

The malicious infrastructure is hosted on providers such as Dynu Systems Incorporated and Hyonix, according to third-party observations. Abuse.ch has corroborated the presence of malware families, including ConnectWise, NetWire RC, and unknown malware. However, AbuseIPDB has only reported indicators with a confidence level of up to 8%, which is below the threshold for high-confidence malicious activity.

---

## Technical Appendix

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

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

- T1047 Windows Management Instrumentation
- T1543 Create or Modify System Process
- T1548.002 Bypass User Account Control
- T1204.002 Malicious File
- T1497.001 System Checks
- T1566.002 Spearphishing Link
- T1218.007 Msiexec
- T1219 Remote Access Tools
- T1036 Masquerading
- T1550 Use Alternate Authentication Material
- T1553.005 Mark-of-the-Web Bypass
- T1102 Web Service
- T1059.001 PowerShell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information

- T1564.003 Hidden Window
- T1059.003 Windows Command Shell
- T1070.004 File Deletion
- T1071.001 Web Protocols
- T1059.005 Visual Basic

## Analytical Scores

- Priority technique (graph chokepoint): T1566.002 Spearphishing Link (centrality 0.2413).
- 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 0.5039; 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 |
|---|---|
| Nomadic Octopus | 0.5039 |
| Evilnum | 0.4686 |
| Rancor | 0.4642 |
| Cobalt Group | 0.4635 |
| Machete | 0.4504 |

## Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 8%.
- Malware families corroborated by abuse.ch: ConnectWise, NetWire RC, Unknown malware.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

## Indicators of Compromise (defanged — non-clickable)

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

| Type | Indicator | Context |
|---|---|---|
| IP | 142[.]202[.]191[.]225 | AbuseIPDB 0% (US) · Unknown malware · AS398019 Dynu Systems Incorporated |

| Type | Indicator | Context |
|---|---|---|
| IP | 207[.]174[.]0[.]143 | AbuseIPDB 8% (US) · Unknown malware · AS398019 Dynu Systems Incorporated |
| IP | 207[.]189[.]11[.]170 | AbuseIPDB 0% (DE) · Unknown malware · AS931 Hyonix |
| Domain | crestmarkhq[.]com | Unknown malware · malware_download |
| Domain | blog[.]derrspecial-onlinedmin[.]live | Unknown malware |
| Domain | subscription-magnetic-recommended-meat[.]trycloudflare[.]com | Unknown malware |
| Domain | derrspecial-onlinedmin[.]live | |
| URL | hxxp://207[.]189[.]11[.]170/Bin/working_payload[.]cs | |
| Hash | 9161a8f7f07741db06b9f9a87b6ec7f277faf2ae3a3a661d6eb09cec4e12b920 | ConnectWise |
| Hash | dc8b056dd6eb75df21e9721ac2e340f91bb5e94d5a6ff412d7d0c7539e0f06e2 | NetWire RC |
| Hash | 433b61c29aefaa5b55fe78063e6ad8597d3835f36e1242d5402ab23e6dc61194 | NetWire RC |
| Hash | 8e87a734daddd95322b3f18f71eb9275219e244aac4f62b8dc6da6e2e91525e9 | ConnectWise |
| Hash | 3cd9b7d5834429632 61f9985128042bf45d25482efcbf903c9248837cb0d744b | ConnectWise |
| Hash | dd23012b4dc29cf7901185ae4fb2d507e737e9ea4d467846eafd6a86b26486bf | ConnectWise |
| Hash | aa84e2ac68f7fc18f4927b89be7b4a7739f2eaf099e489aa0f65c1d3913ce62a | |
| Hash | 3d4d54fb1aaa70005f040558b5d4cd0c | ConnectWise |
| Hash | 5731b2f26146fe379f27bbfc5608f4e9ab11a9d3 | ConnectWise |
| Hash | 01e4cb3c60fa50b2927daa11f25a3c41254968040 6fc121a3d1870a9a33f5d38 | ConnectWise |

| Type | Indicator | Context |
|---|---|---|
| Hash | 9d9f3fa5aaf6bc91091873bd7ee04f0cc23e8709e4ad20c61d2779ff1a43c4b4 | ConnectWise |
| Hash | 04ec5209d922b98a947fea48c73ecaa8 | |
| Hash | 2f1e4fd2937ccf825a555204b1741f89 | |
| Hash | 37da3d949d76c4867c6e8812f2c38f94 | ConnectWise |
| Hash | 3cbf062f600bb6c64849f726566557bc | ConnectWise |
| Hash | 57d20ed65870aa249ca374142d763d13 | NetWire RC |
| Hash | 690401ed2497ad939e05e0bddfd13dbe | |
| Hash | 73167f265dfbd888e514a3730228d82f | ConnectWise |
| Hash | 86db42b1595d14e0f5bd9816e42423cc | ConnectWise |
| Hash | b09c029c6f88a6dad8ef690f9c42f2a5 | ConnectWise |
| Hash | b62119f0ae9ad41612f252dd703799d4 | NetWire RC |
| Hash | e9174663dd353d0faf56f005cf30a652 | ConnectWise |
| Hash | f2d291955c241b3967e636c03cf28c7e | ConnectWise |
| Hash | 19e06d1bf248d1b1ad0d4a1fca8b4dde4733ca43 | ConnectWise |
| Hash | 2c32f560af970493724544b19b05363db6e36d25 | ConnectWise |
| Hash | 2d8faea3e5170802ff2212f862fd5ef1528289ae | ConnectWise |
| Hash | 4e3422e4848147d648c5e82dfeb163035a10bf26 | ConnectWise |
| Hash | 7618dd88cf6a07df1c64ce71dabc1a8167aefcc6 | |
| Hash | 897a9a38ebc67beb0775184520c8ce3b0bec04e5 | NetWire RC |
| Hash | 923a3c6a7006d0e0fde4deadec5a9cd0b075d122 | ConnectWise |
| Hash | a54e21752a34a4663cef87b75efe74be139a2c8e | NetWire RC |
| Hash | a83a5e93cfb4d1fd65054017abfb7827b48f2e5a | ConnectWise |

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:** T1566.002 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:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 38+ 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 T1203 Exploitation for Client Execution in an attempt to execute malicious code on the client-side, potentially by exploiting vulnerabilities in commonly used software, which may allow them to bypass the blocked spearphishing link control by directly targeting client applications. This technique may be particularly appealing as it could enable the actor to leverage existing vulnerabilities to gain initial access, and its pairing with spearphishing link suggests a potential shift in tactics to exploit client-side vulnerabilities. The defensive countermeasure to mitigate this potential pivot would be to patch client applications (Office, browsers, PDF); enable exploit mitigations (ASLR/DEP/CFG); application isolation.

**Also plausible (same tactic):** T1053 Scheduled Task/Job (n=43, lift 1.3), T1106 Native API (n=18, lift 1.6)

**Detection and hardening for the pivot (T1203 Exploitation for Client Execution)**

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**
  - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs
  - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash
  - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
  - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
  - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015 Application Log