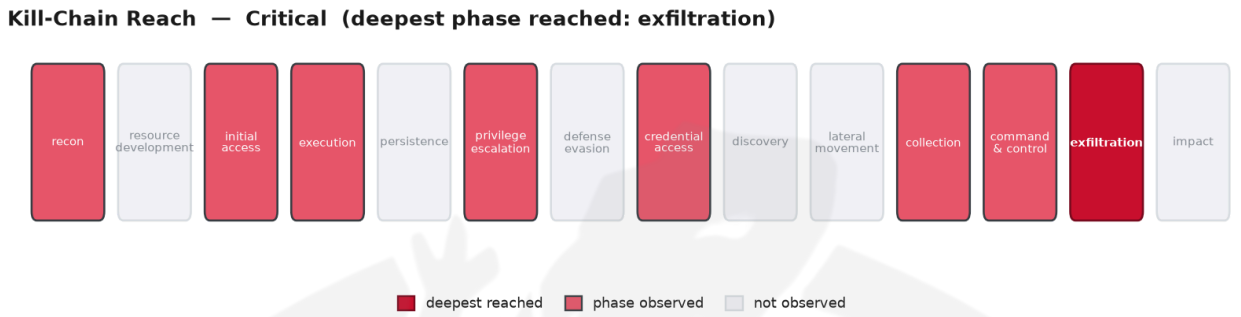
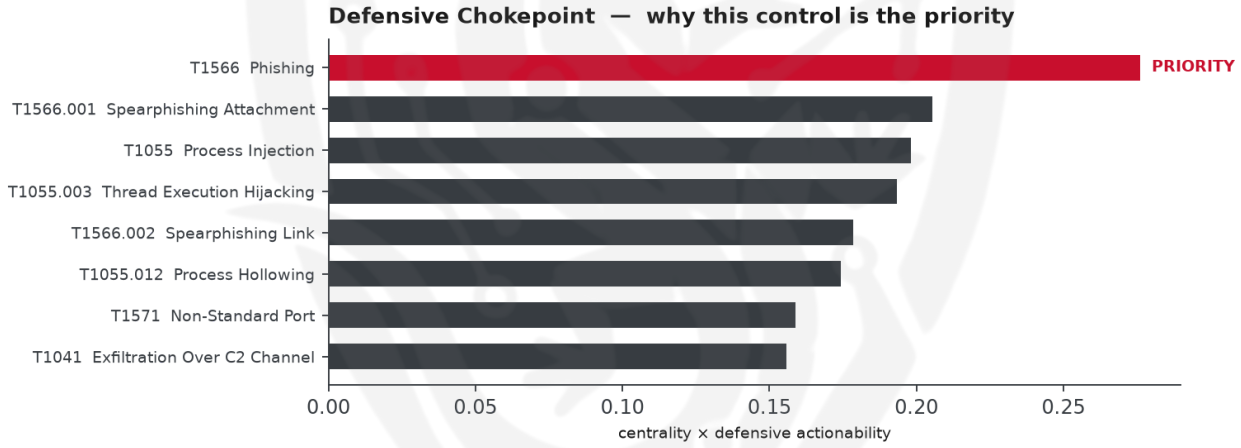
THREAT REPORT: TA4922

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 TA4922, a suspected Chinese crime group that is expanding its operations globally. This group has been observed using various malware families, including Atlas RAT, RomulusLoader, and SilentRunLoader, to target multiple countries across the world. The primary technique used by this group is phishing, which poses a significant threat to organizations. Priority should be given to enabling attachment sandboxing and link rewriting to mitigate this threat.

Threat Overview

TA4922, the observed threat actor, has been associated with multiple malware families, including Atlas RAT, RomulusLoader, SilentRunLoader, ValleyRAT, Winos4.0, HoldingHands, AnyDesk, and SyncFuture. The group's activities have been detected in several countries, including the British Indian Ocean Territory, Germany, India, Indonesia, Italy, Japan, Malaysia, Singapore, South Africa, Taiwan, and the United

Kingdom of Great Britain and Northern Ireland. The exploited vulnerability is currently unknown due to insufficient data.

Attack Chain and Priority Control

The attack chain involves various techniques, including screen capture, keylogging, malicious file execution, and symmetric cryptography. However, the priority technique is T1566 Phishing, which is the primary method used by the group to gain initial access. 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

Although the hosting providers and ASNs used by the group are not available, abuse.ch has corroborated the use of AtlasRAT malware. Additionally, AbuseIPDB has not flagged any indicators with a 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)

- T1113 Screen Capture
- T1056.001 Keylogging
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1119 Automated Collection
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1055.003 Thread Execution Hijacking
- T1055 Process Injection
- T1125 Video Capture
- T1041 Exfiltration Over C2 Channel
- T1566 Phishing
- T1571 Non-Standard Port
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1598 Phishing for Information
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer
- T1204.001 Malicious Link

- T1055.001 Dynamic-link Library Injection
- T1566.003 Spearphishing via Service

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2761).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.506; 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
Ajax Security Team	0.506
Mofang	0.4667
Elderwood	0.4619
PLATINUM	0.4131
APT30	0.4

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: AtlasRAT.
- 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
Domain	nwphotoblog[.]com	
Domain	ws[.]ztts88[.]cyou	
URL	hxxps://nwphotoblog[.]com	

Type	Indicator	Context
URL	hxxps://ws[.]ztts88[.]cyou/file/cg[.]exe	
URL	hxxps://ws[.]ztts88[.]cyou/upload[.]php	
Hash	2d2a251a88632f010fd9671789746908eeccaa5bc5c0a5d25e4649efe4f5b15d	
Hash	0ffb16209def5500ff4380d9e8093437	
Hash	3e7066e44132e64360a30974b6ea3671	
Hash	483a36fb9e4aef9704aa1e4edfb88c492dfe4140	
Hash	7b2c661cfb69e9c75df90d5102647bb014c28ad5	
Hash	0857148fb0bc4aa7adf967ede2307bdb4fc427065d5b6a6db132688a5a8e1eb8	
Hash	3119cf37b8267db8a2dcd11d9a83d5237d7ef1e42388e7c9afa2831b91da8a2d	
Hash	314f4b59535d1b783e1c20c2be00f9e30f8ed27b2e21fad06a73b47ea43279ef	
Hash	40b41979b317406f8abc601677a3b93aaf6ef8ab8ac188b8f383735e388f13b5	
Hash	4fcfa88fffacbce30bbe2136753c9ab5a4c092940d2406fd9d44d5118e745b9d	
Hash	584a9448dda46bd590d7a2f86228100d2ae6e0d6d990c1a4459ed5ee28e07ae8	AtlasRAT
Hash	66a3836b9a17771bce2161f6b73cbc2494a91e49d6aa30d2d53711e8d10de60d	
Hash	8c9b6542f73c5c7fe455b52f5101314407da4f65ff48e7ebf6896605e607c8d0	
Hash	9d0a55c545c4147956db2c2667c4ed931a2875309147548b1dfdd216228f5f73	
Hash	a648db354820ea4d02940cb1702b35974513b7aae83f6dffaacaac4ba31f9295	AtlasRAT
Hash	a75eab31d7ff06b6864960ad7e633be3f9730ff3d3873e4539c8f425fc632dad	AtlasRAT
Hash	de82998ad5fcd63deae030803388e0fb4290d6223fda82368fd25b99b823f0d2	
Hash	e0a6a71c605d9a4076147e9537f82f79f1e1eccadc874595160aa4637ff4088c	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.