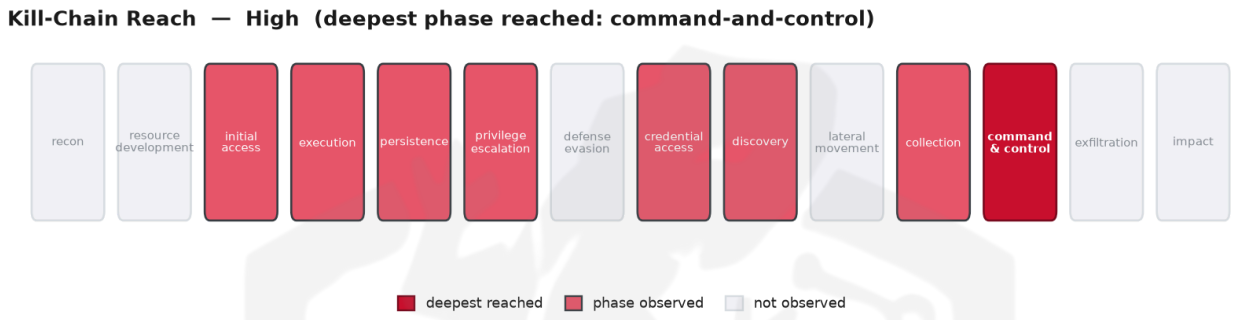
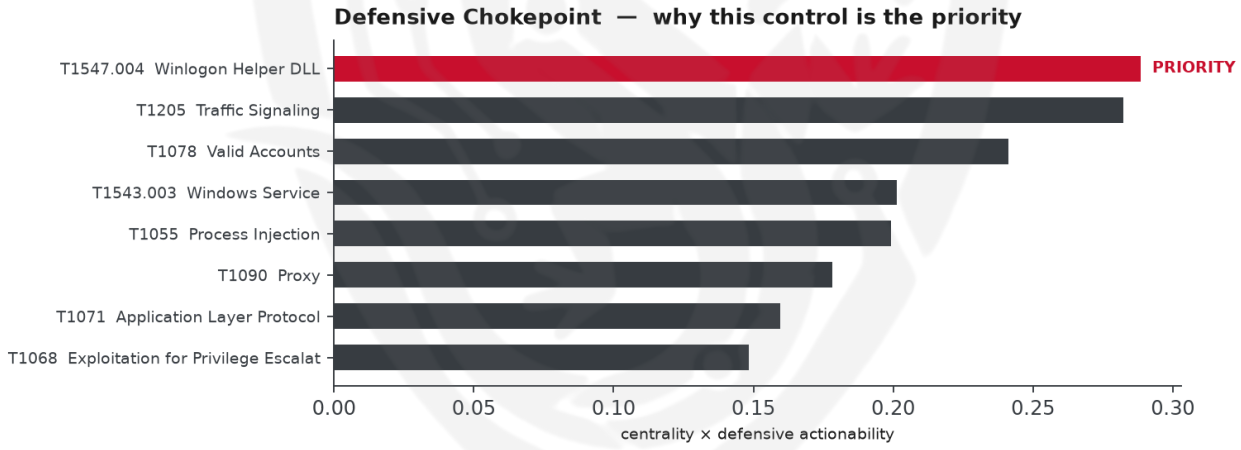
THREAT REPORT: DAXIN MALWARE RESURFACES IN TAIWAN

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 has been linked to the Daxin and Stupig malware families, targeting manufacturing and technology sectors in Taiwan. The threat actor's identity remains unknown. Priority should be given to monitoring autostart locations and alerting on new persistence entries to mitigate the threat. The malware's ability to establish a stealthy presence and exploit system vulnerabilities poses a significant risk to affected organizations.

Threat Overview

The threat actor, whose identity is unknown, has been observed using the Daxin and Stupig malware families to target organizations in Taiwan. The malware's capabilities include keylogging, system

information discovery, and process injection, among others. The targeted sectors include manufacturing and technology, indicating a potential interest in intellectual property or sensitive business information.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving system owner/user discovery, adversary-in-the-middle tactics, and exploitation for privilege escalation. The priority technique is T1547.004 Winlogon Helper DLL, which allows the malware to maintain persistence on compromised systems. To counter this, the priority control is to baseline and monitor autostart locations (Run keys, startup folders); alert on new persistence entries.

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs used by the threat actor, and no malware families have been corroborated by abuse.ch. Additionally, 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)

- T1557 Adversary-in-the-Middle
- T1033 System Owner/User Discovery
- T1056.001 Keylogging
- T1014 Rootkit
- T1543.003 Windows Service
- T1082 System Information Discovery
- T1071 Application Layer Protocol
- T1055 Process Injection
- T1205 Traffic Signaling
- T1547.004 Winlogon Helper DLL
- T1016 System Network Configuration Discovery
- T1090 Proxy
- T1083 File and Directory Discovery
- T1049 System Network Connections Discovery
- T1078 Valid Accounts
- T1068 Exploitation for Privilege Escalation
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1134 Access Token Manipulation
- T1569.002 Service Execution

Analytical Scores

- Priority technique (graph chokepoint): T1547.004 Winlogon Helper DLL (centrality 0.3037).
- 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 0.3858; 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
Ke3chang	0.3858
Tropic Trooper	0.3819
APT41	0.3426
APT32	0.337
Velvet Ant	0.33

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
Hash	49c827cf48efb122a9d6fd87b426482b7496ccd4a2dbca31ebbf6b2b80c98530
Hash	5bb5cffda4647940919a185df37aab2aef71ca3010a6c1d05bdcc8bc8fb3af3f

---

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:** T1547.004 Winlogon Helper DLL (persistence)
- **Observed here:** T1547.004 Winlogon Helper DLL was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1053 Scheduled Task/Job (persistence)
- **Basis:** of the 37+ groups that use Winlogon Helper DLL, this pairing runs 1.9x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious code at a scheduled time, potentially leveraging the Windows Task Scheduler's ability to run tasks under the context of privileged accounts, which may allow them to regain a foothold in the system. This technique may be particularly appealing as it enables the actor to execute tasks without requiring direct user interaction, and its use could be disguised as a legitimate system task. To counter this potential move, the defensive control of alerting on new scheduled tasks (Event ID 4698), restricting schtasks/at to admins, and baselining legitimate task creators should be implemented.

Also plausible (same tactic): T1098 Account Manipulation (n=12, lift 2.0), T1112 Modify Registry (n=17, lift 1.7)

Detection and hardening for the pivot (T1053 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
  - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
  - Restrict schtasks/at to administrators; disable the legacy at.exe
  - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File