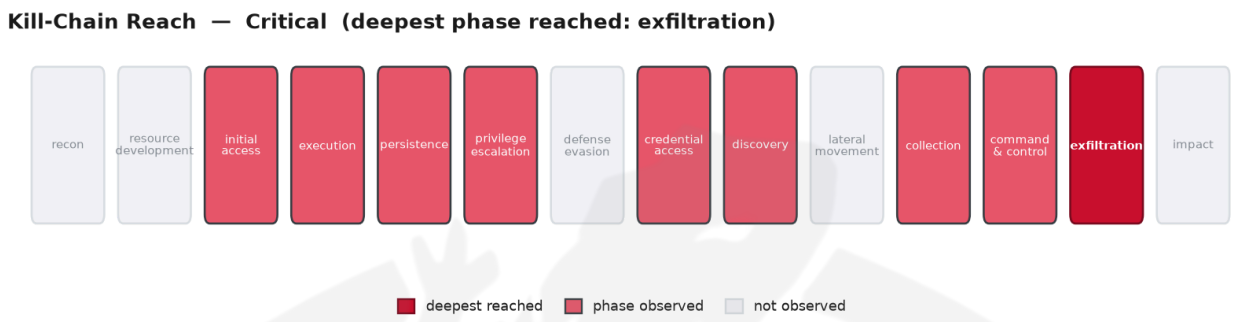
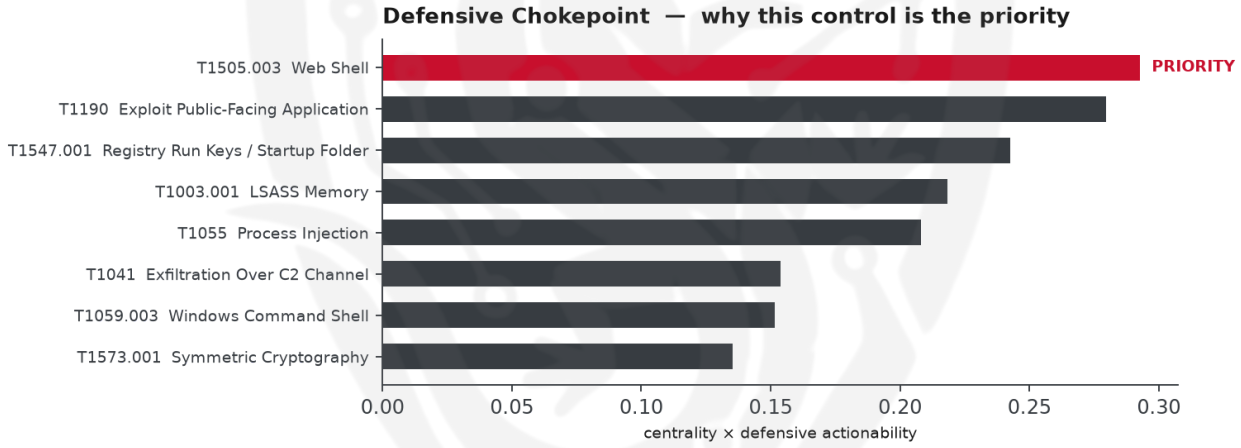
THREAT REPORT: CL-STA-1062

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 CL-STA-1062, a threat actor targeting Southeast Asian governments and critical infrastructure, specifically in Taiwan, with a focus on the Government and Energy sectors. The actor utilizes various malware families, including TinyRCT, Mimikatz, and JuicyPotato. Priority should be given to defending against web shell attacks, as this is the identified chokepoint in the attack chain. The threat actor's activities pose a critical operational risk due to the potential for exfiltration.

Threat Overview

CL-STA-1062, the observed threat actor, employs a range of malware families, including TinyRCT, Mimikatz, and JuicyPotato, to target Taiwanese government and energy sectors. The central vulnerability exploited is currently insufficiently documented. The actor's techniques include multiple methods for persistence, privilege escalation, and data exfiltration, indicating a sophisticated and multi-faceted approach to compromising target systems.

Attack Chain and Priority Control

The attack chain involves various techniques, including scheduled tasks, archiving via utility, screen capture, and symmetric cryptography, among others. The priority technique identified is T1505.003 Web Shell, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended priority control is to "Integrity-monitor web-server directories for web shells; restrict server module/plugin installation."

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 relevant fields. Additionally, no malware families have been corroborated by abuse.ch, and 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)

- T1053.005 Scheduled Task
- T1560.001 Archive via Utility
- T1113 Screen Capture
- T1036.005 Match Legitimate Resource Name or Location
- T1573.001 Symmetric Cryptography
- T1005 Data from Local System
- T1190 Exploit Public-Facing Application
- T1055 Process Injection
- T1505.003 Web Shell
- T1003.001 LSASS Memory
- T1087 Account Discovery
- T1083 File and Directory Discovery
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1059.003 Windows Command Shell
- T1070.004 File Deletion
- T1071.001 Web Protocols
- T1018 Remote System Discovery

Analytical Scores

- Priority technique (graph chokepoint): T1505.003 Web Shell (centrality 0.3082).

- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5852; 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
BRONZE BUTLER	0.5852
RedCurl	0.5274
APT39	0.5252
APT18	0.4815
Magic Hound	0.4624

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	f34bd1d485de437fe18360d1e850c3fd64415e49d691e610711d8d232071a0b1
Hash	2b1ddacbc18763bd8e194c58aea54a4b
Hash	bb47d7ce616b2c11864c30dedb5e3c0402e782a6
Hash	00e09754526d0fe836ba27e3144ae161b0ecd3774abec5560504a16a67f0087c
Hash	4e1f8888d020decd09799ec946f1bf677cac6612b24582ddbf4d8ede425d8384
Hash	9b481b69cd91b09fa7bae7428f646dd89473a4c03393e43da81fe756cde1c472
Hash	cbfe8de6ffadbb1d396f61e63eb18e8b11c29527c1528641e3223d4c516cf7c3
Hash	dce5df29bddff5a4ddaea5c4fec14da91f7b69063a6e1c45ed61e5da4fc6c87b