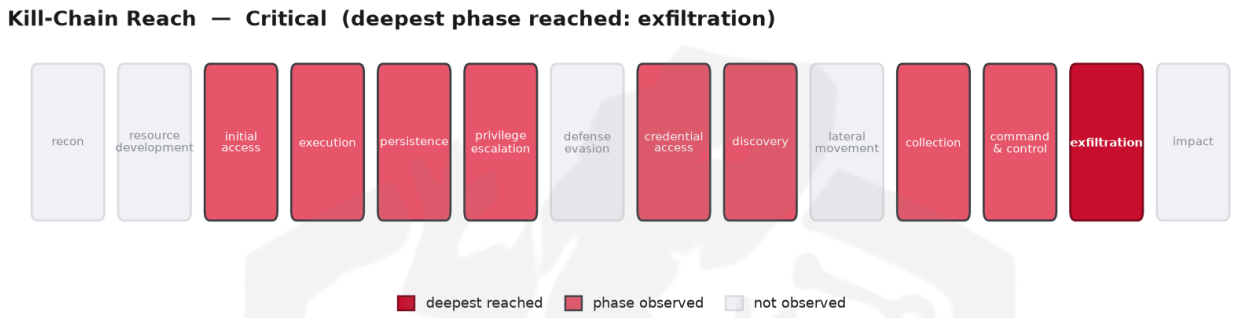
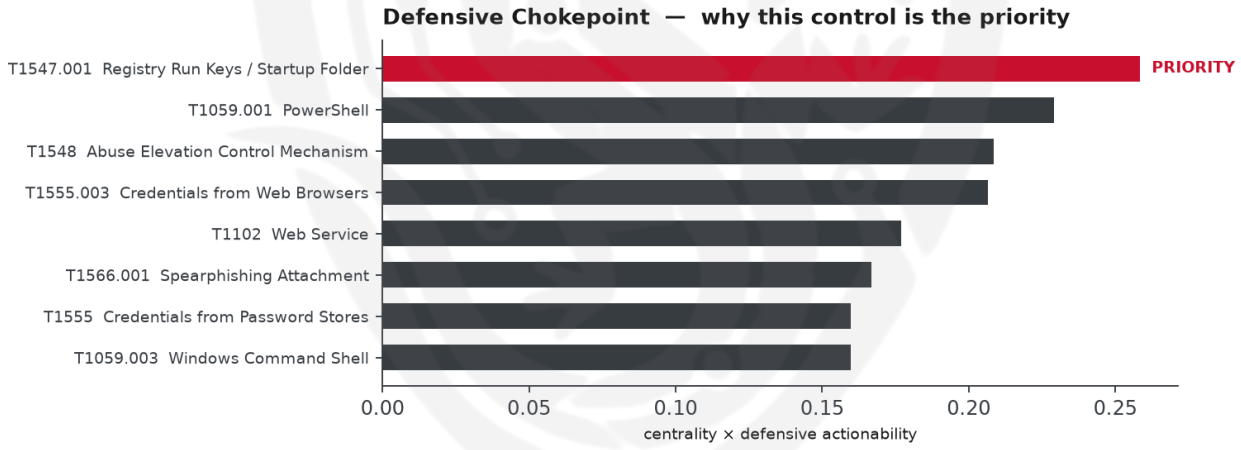
THREAT REPORT: UNKNOWN_ADVERSARY TARGETS THAILAND'S HEALTHCARE SECTOR

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 targeting Thailand's healthcare and government sectors, utilizing the sim.py malware family to gain unauthorized access. The threat actor's primary goal appears to be data exfiltration, making it a high-priority concern. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. The lack of clear attribution and the critical operational risk band emphasize the need for immediate attention to this threat.

Threat Overview

The threat actor, whose identity is currently unknown, is using the sim.py malware family to target organizations in Thailand. Although the central CVE exploited is insufficient, the actor's techniques include system owner/user discovery, boot or logon autostart execution, and spearphishing attachment, among

others. The victimology indicates a focus on the healthcare and government sectors, with the ultimate goal of exfiltrating sensitive data.

Attack Chain and Priority Control

The observed techniques employed by the threat actor form a complex attack chain, involving various methods to gain and maintain access, as well as exfiltrate data. The priority technique identified is T1547.001 Registry Run Keys / Startup Folder, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to "Audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries; alert on .lnk or script creation in Startup by browser/email temp paths."

Infrastructure and Corroboration

Although the hosting providers and ASNs observed are not available, third-party corroboration from abuse.ch indicates the presence of the Braodo malware family. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. These findings provide additional context to the threat landscape but do not override the primary source information.

Technical Appendix

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

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

- T1033 System Owner/User Discovery
- T1547 Boot or Logon Autostart Execution
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1005 Data from Local System
- T1555 Credentials from Password Stores
- T1567 Exfiltration Over Web Service
- T1036 Masquerading
- T1560 Archive Collected Data
- T1555.003 Credentials from Web Browsers
- T1548 Abuse Elevation Control Mechanism
- T1102 Web Service
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1567.002 Exfiltration to Cloud Storage
- T1059.003 Windows Command Shell
- T1213 Data from Information Repositories
- T1070.004 File Deletion

- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2721).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5892; 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
APT37	0.5892
Nomadic Octopus	0.5322
Windshift	0.5204
Patchwork	0.5189
BRONZE BUTLER	0.515

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Braodo.
- 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
Hash	8a5dadc5faf424df1e8a0efad023df81	Braodo
Hash	4a1a6ed11fd50b621659d7976899d050ba2e15d3	Braodo

Type	Indicator	Context
Hash	442e0f4e822842922e7e4685840194e99fd68c7f0ec38c1925914b8f724d5865	
Hash	4eebc38297a307d18784d6f9ebc8aa6e6f69860be970cc70d9e544deb1ff6ce0	
Hash	523388567630e4fbdc359f75232bf2ad82671a680d4bfdce0237fc30dfec4c80	
Hash	74bb6ad7e1310f30a3e24fd3cbbffa2c0c41c64e89e5d0dd1d6900e96b914183	
Hash	7709d8c34d490509f3624104611eb75a862944dd9d7a642f44514ada16c85ee9	Braodo
Hash	e5f6d9d405819e6b05b5d8268a2e973294859ad65237ede36ab612b536d0ac2b	
Hash	f4d4b8cac004bb63834c6df436721babd9464c09787c80b268d839e0aada9f87	

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:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Observed here:** the threat actor used T1547 Boot or Logon Autostart Execution here as an alternative persistence technique.
- **Projected pivot:** T1547 Boot or Logon Autostart Execution (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to T1547 Boot or Logon Autostart Execution to maintain persistence, potentially by leveraging other autostart locations that were not blocked, which may allow them to continue their objective. This technique could be used as an alternative to the blocked Registry Run Keys / Startup Folder, as it still enables the actor to execute malicious code automatically. The defensive countermeasure would be to baseline and monitor autostart locations (Run keys, startup folders); alert on new persistence entries.

Detection and hardening for the pivot (T1547 Boot or Logon Autostart Execution)

- **Telemetry:** Sysmon (registry + process); EDR autostart/ASEP inventory
- **Detect:**
  - Sysmon 13 (registry value set) on Run/RunOnce keys under HKLM & HKCU ...\CurrentVersion\Run*
  - Sysmon 11 for shortcuts/scripts created in Startup folders
  - Periodic ASEP (autostart extensibility point) diff against a known-good baseline
- **Harden:**
  - Restrict write access to autostart registry keys and Startup folders

    - Application control to block unsigned autostart binaries
- **MITRE:** M1047 Audit, M1038 Execution Prevention · DS0019 Service, DS0024 Windows Registry, DS0022 File