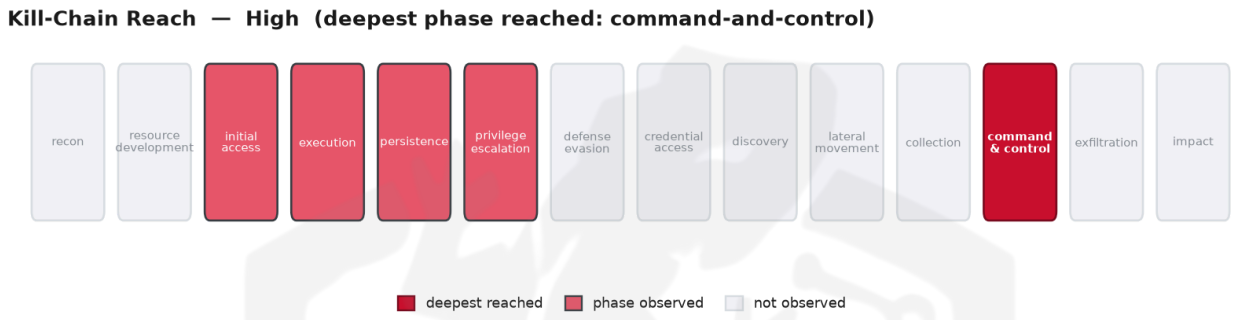
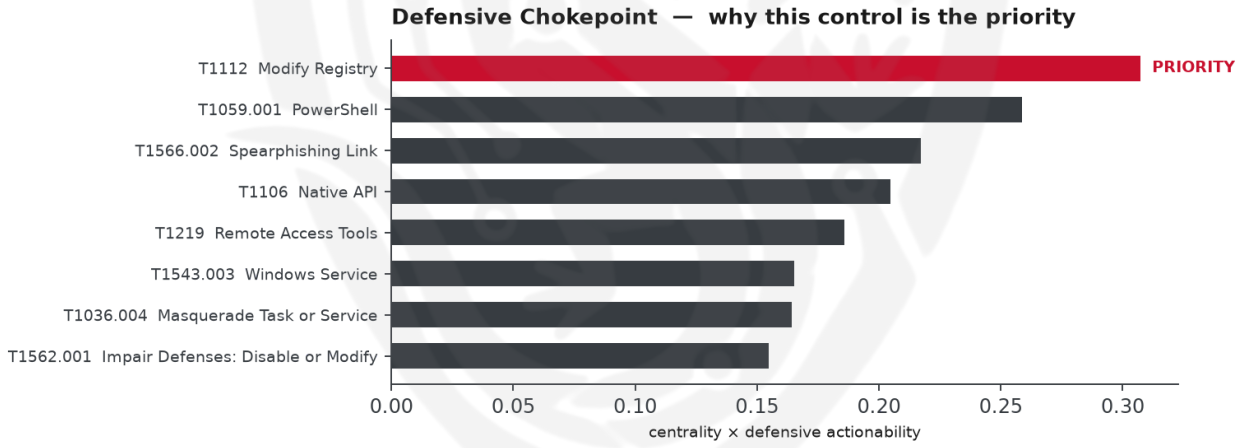
THREAT REPORT: FINANCE SECTOR SCREENCONNECT MALWARE CAMPAIGN

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 has been delivering ScreenConnect malware to finance sector targets via phishing emails. The threat actor's identity and targeted country remain unknown. Priority should be given to monitoring sensitive registry keys for modification to prevent further malicious activity. The finance sector is advised to be vigilant and take immediate action to restrict registry-edit tools for unprivileged users.

Threat Overview

The threat actor, whose identity is unknown, has been using ScreenConnect malware to target the finance sector. The malware's delivery mechanism involves phishing emails, which exploit various techniques to

bypass security controls. The victimology suggests that the finance sector is the primary target, although the specific country and other details remain unclear.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, including bypassing user account control, using malicious files, and modifying Windows services. The priority technique is T1112 Modify Registry, which is the graph chokepoint. To mitigate this threat, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The malicious infrastructure is hosted on Swissnet LLC, according to third-party observations. Additionally, abuse.ch has corroborated the presence of PureRAT malware families, which may be related to the ScreenConnect malware used in this campaign. However, 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)

- T1548.002 Bypass User Account Control
- T1204.002 Malicious File
- T1543.003 Windows Service
- T1566.002 Spearphishing Link
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1219 Remote Access Tools
- T1112 Modify Registry
- T1036.004 Masquerade Task or Service
- T1059.001 PowerShell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1564.003 Hidden Window
- T1071.001 Web Protocols
- T1059.005 Visual Basic
- T1105 Ingress Tool Transfer
- T1564.001 Hidden Files and Directories

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3235).

- 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 0.5539; 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	0.5539
Gorgon Group	0.5108
APT19	0.5052
Windshift	0.4583
Cobalt Group	0.4529

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: PureRAT.
- 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	217[.]60[.]195[.]167	AbuseIPDB 0% (NL) · PureRAT · AS209 373 Swissnet LLC
Domain	bkofamerica[.]com	
Domain	kleinschnitg[.]com	
Domain	sectioncompil[.]com	

Type	Indicator	Context
Domain	ealerts[.]bkofamerica[.]com	
Domain	cdn[.]uploadtourl[.]com	
URL	hxxps://cdn[.]uploadtourl[.]com/3b154d8e-61be-4521-b3c3-75efb845a2e2_msi_base64[.]txt	
URL	hxxps://kleinschnitg[.]com/F3bebOag/?id=email	
URL	hxxps://sectioncompil[.]com/wkudpl/main[.]php	
URL	hxxps://sectioncompil[.]com/wkudpl/notarize[.]php	
URL	hxxps://sectioncompil[.]com/wkudpl/windows/download/AccountGuardSetup[.]zip	
URL	hxxps://sectioncompil[.]com/wkudpl/windows/manage[.]html	
Hash	3e404e542ae99eeb8827fa72e74dafeacc9b2a8af463a8e0789d7efb0a2dbfb8	
Hash	6d1dae4794a80caac5eee48b6189e49c4146eac123bcb03d585194bf2b2a3f10	
Hash	bd987f9f493a234a74580eba1ab95d2178dd38d06bde7a67b991064e09cdc0ee	
Hash	d0913e83d10cadae7af2d737b6c5172638680dfe87d04fa67b509b9c41c0f4bf	
Hash	ed9f4c15d2857260ce635aad8024b8abaaa010eb13bb0ac77f3a8c296a3c66f2	
Hash	f580d528759829f62cba577c9126efe6478529f91609451c3a11e483b239e8a4	

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:** T1112 Modify Registry (persistence)

- **Observed here:** T1112 Modify Registry 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 19+ groups that use Modify Registry, 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 tasks at a later time, potentially leveraging the Windows Task Scheduler to blend in with legitimate system activity and evade detection. This technique may be particularly appealing as it allows the actor to execute commands remotely and at specific intervals, which could be used to re-establish a foothold or regain access to the compromised system. The defensive control to counter this would be to alert on new scheduled tasks (Event ID 4698), restrict schtasks/at to admins, and baseline legitimate task creators.

Also plausible (same tactic): T1547 Boot or Logon Autostart Execution (n=17, lift 1.7), T1505 Server Software Component (n=11, lift 2.0)

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