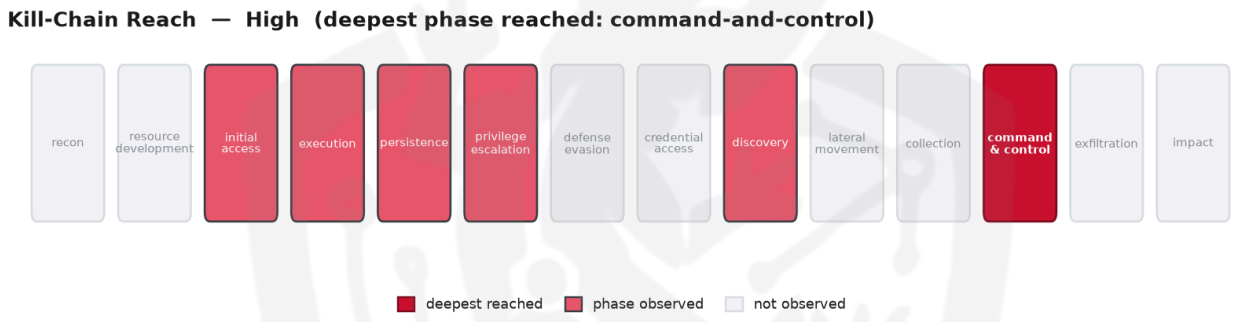
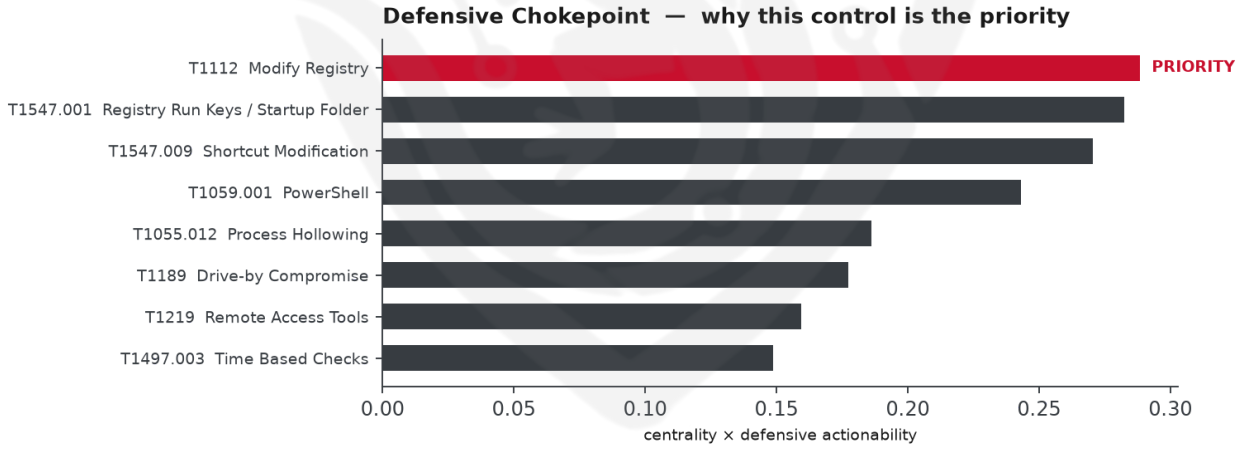
THREAT REPORT: FROM POISONED SEARCH RESULTS TO GPU MINING: A CRYPTOJACKING CAMPAIGN ABUSING SCREENCONNECT AND MICROSOFT .NET UTILITIES

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

This brief covers activity involving SimpleRunPE, RuntimeHost, with no single central CVE identified, affecting targets not specified by the source. The source does not attribute this activity to a named actor. The operational risk is assessed as High. Priority should be given to the control described below, centred on T1112 Modify Registry.

Threat Overview

The activity is associated with an as-yet unattributed cluster of activity. Malware observed: SimpleRunPE, RuntimeHost. Reported victimology: targets not specified by the source.

Attack Chain and Priority Control

The source records the following techniques: - T1053.005 Scheduled Task - T1036.005 Match Legitimate Resource Name or Location - T1497.001 System Checks - T1082 System Information Discovery - T1218.007 Msiexec - T1140 Deobfuscate/Decode Files or Information - T1219 Remote Access Tools - T1547.009 Shortcut Modification - T1497.003 Time Based Checks - T1112 Modify Registry - T1059.001 PowerShell - T1547.001 Registry Run Keys / Startup Folder - T1562.001 Impair Defenses: Disable or Modify Tools - T1055.012 Process Hollowing - T1027 Obfuscated Files or Information - T1573 Encrypted Channel - T1189 Drive-by Compromise - T1071.001 Web Protocols - T1574.002 Hijack Execution Flow - T1105 Ingress Tool Transfer

Priority should be given to T1112 Modify Registry. Recommended control: Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users.

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
- T1036.005 Match Legitimate Resource Name or Location
- T1497.001 System Checks
- T1082 System Information Discovery
- T1218.007 Msiexec
- T1140 Deobfuscate/Decode Files or Information
- T1219 Remote Access Tools
- T1547.009 Shortcut Modification
- T1497.003 Time Based Checks
- T1112 Modify Registry
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1189 Drive-by Compromise
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (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 0.4539; 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
TA2541	0.4539
APT19	0.4507
Darkhotel	0.4372
Molerats	0.4315
Daggerfly	0.4297

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
Domain	direct-download[.]gleeze[.]com
Domain	minemine[.]gleeze[.]com
Domain	start-download[.]gleeze[.]com
URL	hxxp://minemine[.]gleeze[.]com:8443/ws
Hash	1b2555b09ac62164638f47c8272beb6b0f97186e37d3a54cb84c723ff7a2eee5
Hash	4125681f9276487f4318c7ce9c8b6786

Type	Indicator
Hash	512b49f441765698c679b5da5f0cc868
Hash	56b75638beabd690f38de434f7efd623
Hash	661d4551df34661f3ffc565e2f4ecdbc
Hash	d58ce78503c60c19926ed642f0eb9d53
Hash	017830597704acd90fb171f3025bc6f28745da57
Hash	62d5e9ed6c1444469e4b89f3ca6c2047a5e8eb98
Hash	bbeaac7ef00268bd5cc583e26624e760085581dc
Hash	c27a1688fa5a4ec9497da0fc9bd88c8b362234c5
Hash	f9ea4f4b636614226579ac6cbfc8abe21539a8da
Hash	062bb28765fbaa11f8cc341fa16e2c7f942a122d929cb41f4a0f755b4429f246
Hash	16562974deec80e41ef57a71a6de8c03ceb393005fb1432f8d9d82c61294ef8c
Hash	2ee93ccbcd49ed94c65dcf52e7dcb8f0fa0a443ca24c0e0c7f79152efba657b7
Hash	69077fcf940fc5852fb32beed15636756ebc04ac971b7ed71d36251e7ea70a20
Hash	7035c2abeb617e828dfda1b119b8544fa9ae15a1d263d18bc5506acaf381f496
Hash	9ff07c9fafa9c03fdf69e4abf6806aa7c938b5480e7e258f227db0719ecd6386
Hash	a460d00ef93c8ce70d32e48e55781af66a53328fc2dde45519be196c265de074
Hash	c7425fbe6c3a4937934215c54027d4b67202d12ab490682fae03498870d66d06
Hash	cf3f8160eb5a5580e0c35054847e3ac4d01e9fe74fab8bc12bf6e8a40bf696b2
Hash	db2d33c4e6e4a5c2263b56e8303c343305a94dde1fc2968304ba260acbbd9f9f
Hash	e021662a652ba95c8778b991056696ab3c9b0f60d5e23b1e6cf73c3847db6610

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:** the threat actor used T1053.005 Scheduled Task here as an alternative persistence technique.
- **Projected pivot:** T1053.005 Scheduled Task (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

With T1112 Modify Registry blocked, the threat actor could preserve the same objective by pivoting to T1053.005 Scheduled Task, a technique observed in this campaign. Defensive countermeasure: Alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Detection and hardening for the pivot (T1053.005 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