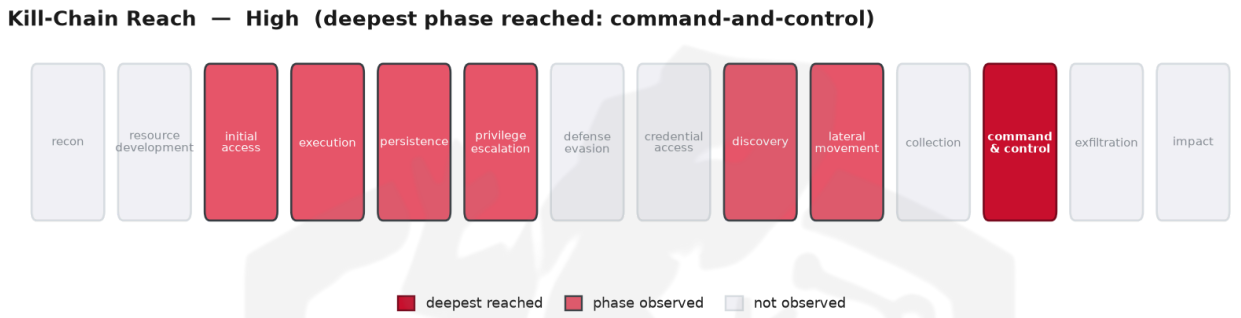
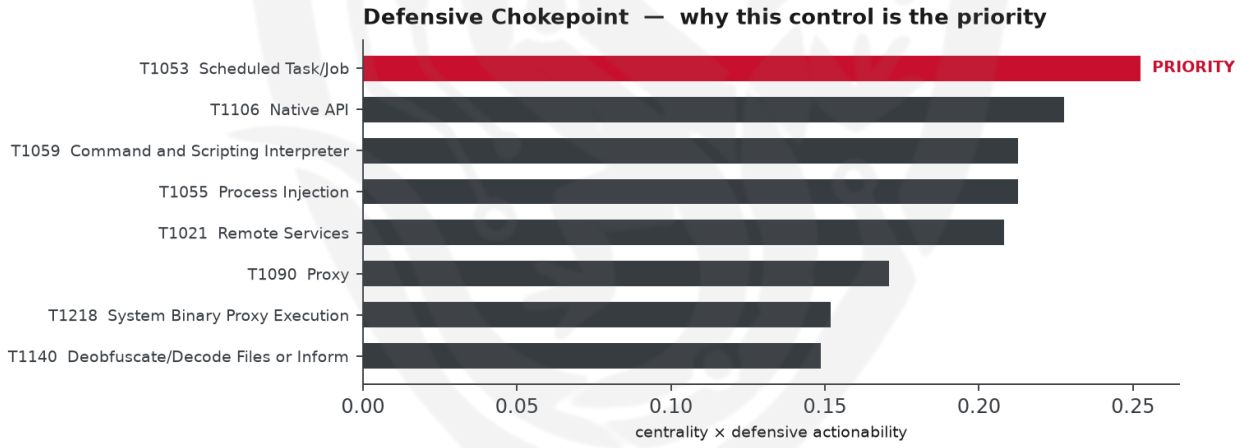
THREAT REPORT: LAZARUS GROUP 3CXDESKTOPAPP INTRUSION CAMPAIGN

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 Lazarus Group is attributed by the source to be behind an intrusion campaign targeting the finance and energy sectors. The campaign involves the use of TxRLoader and ArcfeedLoader malware families. Priority should be given to monitoring and restricting scheduled tasks to prevent further exploitation. The lack of specific information on targeted countries and central CVEs highlights the need for vigilance across various systems.

Threat Overview

The Lazarus Group, as attributed by the source, utilizes the TxRLoader and ArcfeedLoader malware families to target organizations in the finance and energy sectors. Although the central CVE is insufficient, the group's techniques include creating or modifying system processes, DNS manipulation, and system

information discovery. The victimology suggests a focus on compromising software supply chains and establishing encrypted channels.

Attack Chain and Priority Control

The observed techniques form a complex chain, starting with system information discovery and proceeding through various stages, including process injection, file and directory discovery, and encrypted channel establishment. The priority technique is T1053 Scheduled Task/Job, which serves as a critical chokepoint in the attack chain. To mitigate this, the recommended control is to "Alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators."

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed in this campaign. 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)

- T1543 Create or Modify System Process
- T1071.004 DNS
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1082 System Information Discovery
- T1071 Application Layer Protocol
- T1053 Scheduled Task/Job
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1218 System Binary Proxy Execution
- T1021 Remote Services
- T1090 Proxy
- T1059 Command and Scripting Interpreter
- T1083 File and Directory Discovery
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1195.002 Compromise Software Supply Chain
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1053 Scheduled Task/Job (centrality 0.2658).
- 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 0.4737; 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
Tropic Trooper	0.4737
Cobalt Group	0.4627
APT18	0.4423
Higaisa	0.4233
Daggerfly	0.4188

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	akamaicontainer[.]com
Domain	azureonlinecloud[.]com
Domain	officeaddons[.]com
Domain	akamaitechcloudservices[.]com
Domain	azuredeploystore[.]com
Domain	azureonlinestorage[.]com

Type	Indicator
Domain	dunamistrd[.]com
Domain	glcloudservice[.]com
Domain	journalide[.]org
Domain	msedgepackageinfo[.]com
Domain	msstorageazure[.]com
Domain	msstorageboxes[.]com
Domain	officestoragebox[.]com
Domain	pbxcloudeservices[.]com
Domain	pbxphonenetwork[.]com
Domain	pbxsources[.]com
Domain	qwepoi123098[.]com
Domain	sbmsa[.]wiki
Domain	visualstudiofactory[.]com
Domain	zacharryblogs[.]com
Hash	5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290
Hash	59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983
Hash	92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61
Hash	aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868
Hash	b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb
Hash	dde03348075512796241389dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc
Hash	e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec
Hash	fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405
Hash	7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896

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:** T1053 Scheduled Task/Job (execution)
- **Observed here:** Lazarus Group used T1059 Command and Scripting Interpreter here as an alternative execution technique.
- **Projected pivot:** T1059 Command and Scripting Interpreter (execution)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The Lazarus Group could pivot to using T1059 Command and Scripting Interpreter to execute commands and scripts, potentially leveraging built-in tools like PowerShell or cmd.exe to maintain their objective after the block on scheduled tasks. They may attempt to use these interpreters to execute malicious scripts or commands, which would likely be a key part of their campaign. To counter this, the mandated defensive control of constraining PowerShell for unprivileged users, enabling script-block logging, and blocking wscript/cscript where unneeded should be implemented.

Detection and hardening for the pivot (T1059 Command and Scripting Interpreter)

- **Telemetry:** Sysmon / EDR process + command line; PowerShell Script Block Logging (4104); AMSI
- **Detect:**
  - Security 4688 / Sysmon 1 with full command lines; encoded or obfuscated PowerShell
  - PowerShell 4104 script-block content; suspicious cmdlets and download cradles
  - Office or browser processes spawning powershell/cmd/wscript
- **Harden:**
  - Enable Script Block Logging + AMSI; Constrained Language Mode
  - Application control (WDAC/AppLocker); remove/limit unused interpreters
- **MITRE:** M1049 Antivirus/Antimalware, M1038 Execution Prevention, M1042 Disable or Remove Feature, M1045 Code Signing · DS0009 Process, DS0012 Script, DS0017 Command