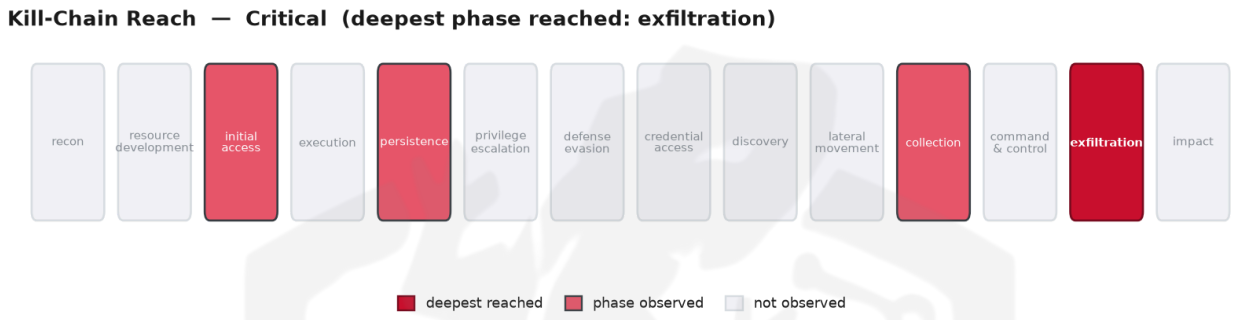
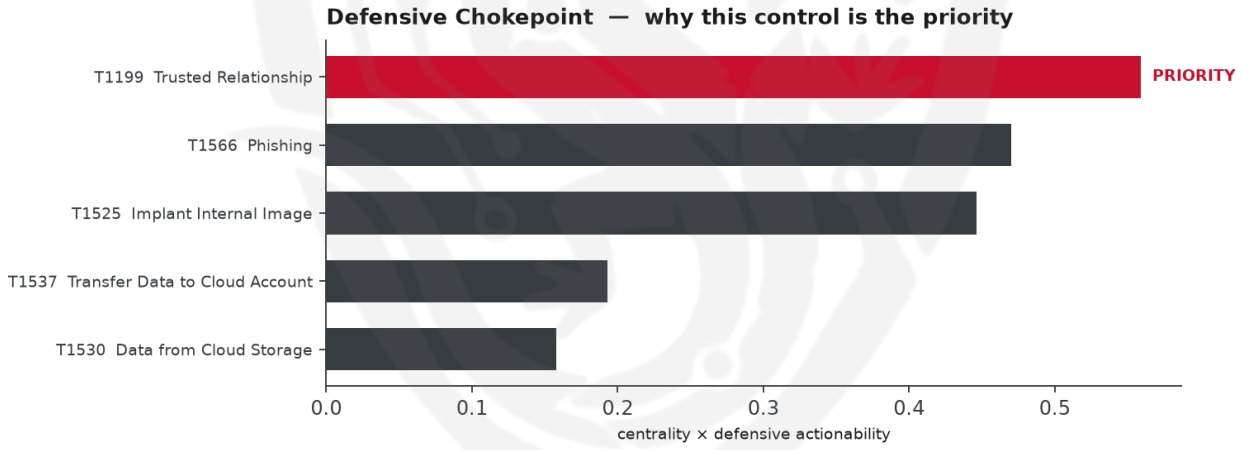
THREAT REPORT: UKRAINE-TARGETED PHISHING CAMPAIGN USING QR CODES

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 Ukraine, specifically the Financial, Technology, and Retail sectors, using phishing tactics and malicious Android applications such as NagaPocker.apk and ludashi_home.apk. The threat actor's identity remains unknown. Priority should be given to auditing and securing trusted third-party connections to prevent further exploitation. The campaign's use of trusted relationships as a primary technique poses a significant risk to targeted organizations.

Threat Overview

The threat actor, whose identity is currently unknown, has been utilizing various malware families, including NagaPocker.apk, app-u7cp-release.apk, ludashi_home.apk, and k12sns.apk, to target Ukrainian

organizations. The primary technique employed by the actor involves exploiting trusted relationships, although the specific vulnerability used remains insufficiently documented.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including phishing, implanting internal images, and transferring data to cloud accounts. The priority technique, identified as T1199 Trusted Relationship, serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to "Audit and least-privilege trusted third-party/B2B connections; monitor partner-account activity."

Infrastructure and Corroboration

There is currently no observed hosting provider or ASN associated with 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)

- T1530 Data from Cloud Storage
- T1525 Implant Internal Image
- T1199 Trusted Relationship
- T1566 Phishing
- T1537 Transfer Data to Cloud Account

Analytical Scores

- Priority technique (graph chokepoint): T1199 Trusted Relationship (centrality 0.559).
- Operational risk: Critical (score 0.822, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3536; 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
AppleJeus	0.3536
GOLD SOUTHFIELD	0.2887
APT30	0.25
RedCurl	0.1936
TA459	0.1768

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	xx[.]com
Domain	gui[.]snitch-dev[.]site
Domain	kzeva2010[.]sbs
Domain	gui[.]snitch-dev[.]online
Domain	snitch-dev[.]space
Domain	gui-snitch[.]online
Domain	gui[.]snitch-dev[.]xyz
Domain	gui[.]dev-snitch[.]xyz
Domain	2fbing[.]com
Domain	awawc[.]icu
Domain	bostonsportsthenandnow[.]com
Domain	gricanjolt[.]com
Domain	gui-grafit[.]online
Domain	kccomputech[.]in

Type	Indicator
Domain	kropyva-group[.]online
Domain	malicious-website[.]com
Domain	radenspinrtp[.]cloud
Domain	signal-qr[.]org
Domain	solulu[.]vip
Domain	ve1edm[.]cc
Domain	ve2edm[.]cc
Domain	weppf[.]icu
Domain	wswwc[.]icu
Domain	90999[.]fdjk34sddsf90999[.]cc
Domain	azojwdsj[.]xinchaoshan[.]com
Domain	cdnimg[.]jeayacrai[.]in[.]net
Domain	csdh[.]wangzhan[.]mobi
Domain	fable[.]tele-tale[.]cn
Domain	gld45a[.]cqxqlsz[.]com
Domain	gui[.]dev-snitch[.]cloud
Domain	gui[.]dev-snitch[.]online
Domain	gui[.]dev-snitch[.]site
Domain	link[.]members-ms[.]jp
Domain	resourcepro[.]tycheint[.]com
Domain	signal[.]skyriver[.]ch
Domain	snitch[.]open-group[.]site
Domain	t[.]k12[.]com[.]cn
Domain	www[.]malicious-url[.]com
Domain	www[.]phishing-meeting-link-url[.]com

Type	Indicator
Domain	www[.]sgnl-web[.]org-status[.]nl

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:** T1199 Trusted Relationship (initial-access)
- **Observed here:** T1199 Trusted Relationship was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 5+ groups that use Trusted Relationship, this pairing runs 1.7x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1203 Exploitation for Client Execution to maintain their objective by leveraging vulnerabilities in client applications, such as browsers or Office software, which may be used by the targeted organization, potentially allowing them to execute malicious code on the client-side. This technique may be particularly appealing as it could enable the actor to bypass the blocked trusted relationship and still gain a foothold within the organization. The defensive countermeasure to mitigate this would likely involve the mandated defensive control: Patch client applications (Office, browsers, PDF); enable exploit mitigations (ASLR/DEP/CFG); application isolation.

Also plausible (same tactic): T1047 Windows Management Instrumentation (n=5, lift 1.7), T1059 Command and Scripting Interpreter (n=10, lift 1.2)

Detection and hardening for the pivot (T1203 Exploitation for Client Execution)

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**
  - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs
  - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash
  - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
  - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
  - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015

Application Log