QUARTERLY THREAT COLLECTION REPORT

Q2 2026 Threat Landscape

Three months. 372 open source threat intelligence reports collected and analyzed. One notable shift: supply chain compromise, cloud infrastructure targeting, and credential theft are no longer three separate trends. They are the same attack, observed from three angles simultaneously.

372	74	445	519
REPORTS INGESTED	UNIQUE ACTORS	MALWARE FAMILIES	ATT&CK TECHNIQUES

- April 1 to June 30 2026
- Sol Intelligence Engine
- 121 source vendors
- 189 unique campaigns

01 — KEY FINDINGS

What this quarter tells us

Six findings that define Q2 2026 and set the agenda for Q3 monitoring.

Finding 01

The supply chain is now reliably profitable, not opportunistically exploited

Five independent actor clusters operated against the same npm, PyPI, and VSCode attack surface simultaneously in May. When unrelated actors converge on the same surface independently, it signals structural profitability rather than a trend or campaign. The roster is likely to expand in Q3.

Finding 02

Defense Evasion investment is disproportionate and accelerating

91 unique Defense Evasion techniques — nearly double all others. Adversaries are investing more in staying hidden than in novel initial access or impact. The MachineGUID-derived decryption, monoglyph obfuscation, and AppDomainManager hijacking all represent significant R&D investment in detection avoidance specifically.

Finding 03

Criminal and nation-state activity reached parity in May for the first time

24 nation-state vs 24 criminal attributed reports in May. This is driven almost entirely by UNC6780. Remove UNC6780 and criminal activity is flat. But the statistical event is notable: if criminal supply chain actors continue scaling, the historical 2:1 nation-state dominance may not return in Q3.

Finding 04

DPRK blurs the nation-state and criminal boundary deliberately

Lazarus Group, Emerald Sleet, and NICKEL TAPESTRY collectively account for 17 of 27 nation-state reports. All three carry financial gain as primary motivation alongside espionage. This pulls financial motivation counts to near-parity with pure espionage (73 vs 75 reports), complicating traditional actor-type attribution.

Finding 05

Geopolitical events now trigger measurable cyber campaigns within 60 days

Operation Epic Fury is the clearest documented case in this corpus of a real-world military event (US Operation Epic Fury, Feb 28 2026) directly triggering a named IRGC cyber campaign (Nimbus Manticore) within two months. This correlation between geopolitical calendar and cyber operational tempo is becoming a reliable planning tool for defenders.

Finding 06

2026 CVEs are being weaponised within weeks of disclosure

CVE-2026-21509 (Office OLE) and CVE-2026-45321 (npm registry) both appeared in the corpus within weeks of disclosure, already actively exploited by APT28 and UNC6780 respectively. If this pace continues, the window between disclosure and active exploitation will shrink below the realistic patching cycle for most organisations in Q3.

02 — NET NEW INTELLIGENCE

What appeared for the first time this quarter

10 net-new threat actors, 280+ net-new malware families, 29 net-new MITRE techniques, 54 net-new named campaigns, and 14 net-new CVEs entered the corpus with zero prior coverage in Jan to Mar 2026.

10

NEW THREAT ACTORS

UAC-0194 (Russia-nexus, Ukraine-targeting) is still active in June — the only new actor trending upward. **Nimbus Manticore** (IRGC) launched Operation Epic Fury in direct response to US military action on Feb 28 2026.

280+

NEW MALWARE FAMILIES

GlassWorm introduced the first blockchain C2 architecture in the corpus — commands embedded in Solana transaction memo fields, impossible to sinkhole. **JS.MonoGlyphRAT** used monoglyph obfuscation, a previously uncatalogued technique with 29/59 VirusTotal evasion at discovery.

29

NEW ATT&CK TECHNIQUES

T1574.014 AppDomainManager Hijacking — near-zero detection coverage in most enterprise stacks. **T1588.007** AI as adversary capability acquisition — first formalised instance of LLM use for malware development. **T1657** Financial Theft formalised crypto heist operations.

54

NEW CAMPAIGNS

Operation Epic Fury (Nimbus Manticore / IRGC) is the clearest documented case of a real-world geopolitical event directly triggering a named cyber campaign. **FrostArmada** (APT28) DNS hijacking hit 18,000+ victims across 120 countries.

14

NEW CVES REFERENCED

5 carry a 2026 identifier — same-year weaponisation. **CVE-2026-21509** (Microsoft Office OLE) was weaponised by APT28 within weeks of disclosure. **CVE-2026-45321** (npm registry) exploited by UNC6780 in supply chain campaigns.

85+

NEW TOOLS TRACKED

SyncFuture — a legitimate Chinese RMM tool abused by TA4922 for persistent interactive access post-compromise across EMEA targets. First instance of a Chinese-market RMM appearing as an adversary persistence tool in Western victim environments.

FIVE ANALYTICALLY SIGNIFICANT NET-NEW FINDINGS

1. **Blockchain C2 (GlassWorm)** — First on-chain C2 in the corpus. Structurally cannot be disrupted by conventional blocking.

2. **AppDomainManager Hijacking (T1574.014)** — .exe.config file plant invisible to file reputation, AV, and most EDR. Used across 3 consecutive campaign waves.

3. **AI as formalised adversary capability (T1588.007)** — Transition from theoretical to operational AI weaponisation. GREYVIBE used LLMs for phishing lure generation and malware evasion tuning.

4. **Monoglyph obfuscation (JS.MonoGlyphRAT)** — Previously uncatalogued technique. No known prior art in public threat intelligence. Currently unattributed.

5. **Geopolitically-triggered IRGC surge (Operation Epic Fury)** — Direct causal link between US military action Feb 28 2026 and a documented cyber campaign within 60 days.

---

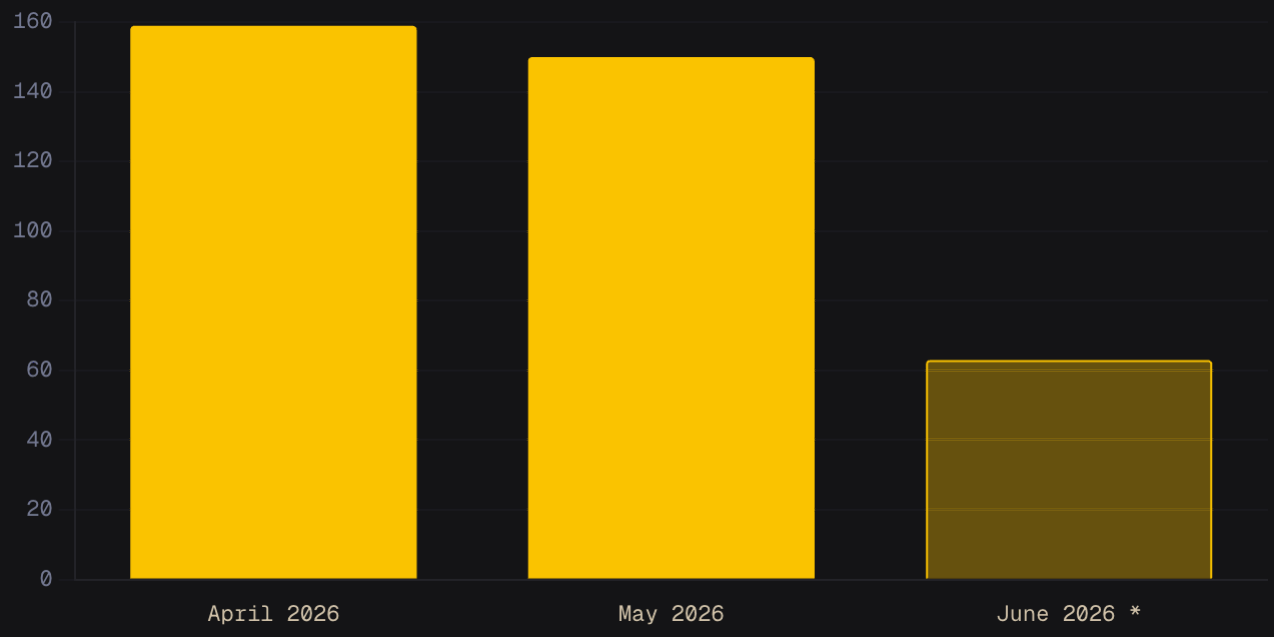
03 — OVERVIEW

Corpus at a glance

April peaked at 159 reports, May sustained at 150. June data covers only 3 days (Jun 1 to 3) and is noted throughout as partial. The true quarterly total is estimated at 450 to 460 reports when June is fully ingested.

> June caveat: Only Jun 1 to 3 data is present in the corpus (63 reports). The June count is severely undersampled. Trend lines and monthly comparisons should be read with this in mind throughout this report.

MONTHLY INGESTION VOLUME APR–JUN 2026



INGESTION RATE VS JAN–MAY

124

REPORTS/MONTH AVG

vs 94/month Jan–May. Ingestion rate is accelerating quarter on quarter.

MALWARE DENSITY FAMILIES PER REPORT

1.19

FAMILIES PER REPORT

445 families across 372 reports. New malware is surfacing at 2 to 3 families per report on average.

TTP SATURATION VS FULL PRIOR CORPUS

95%

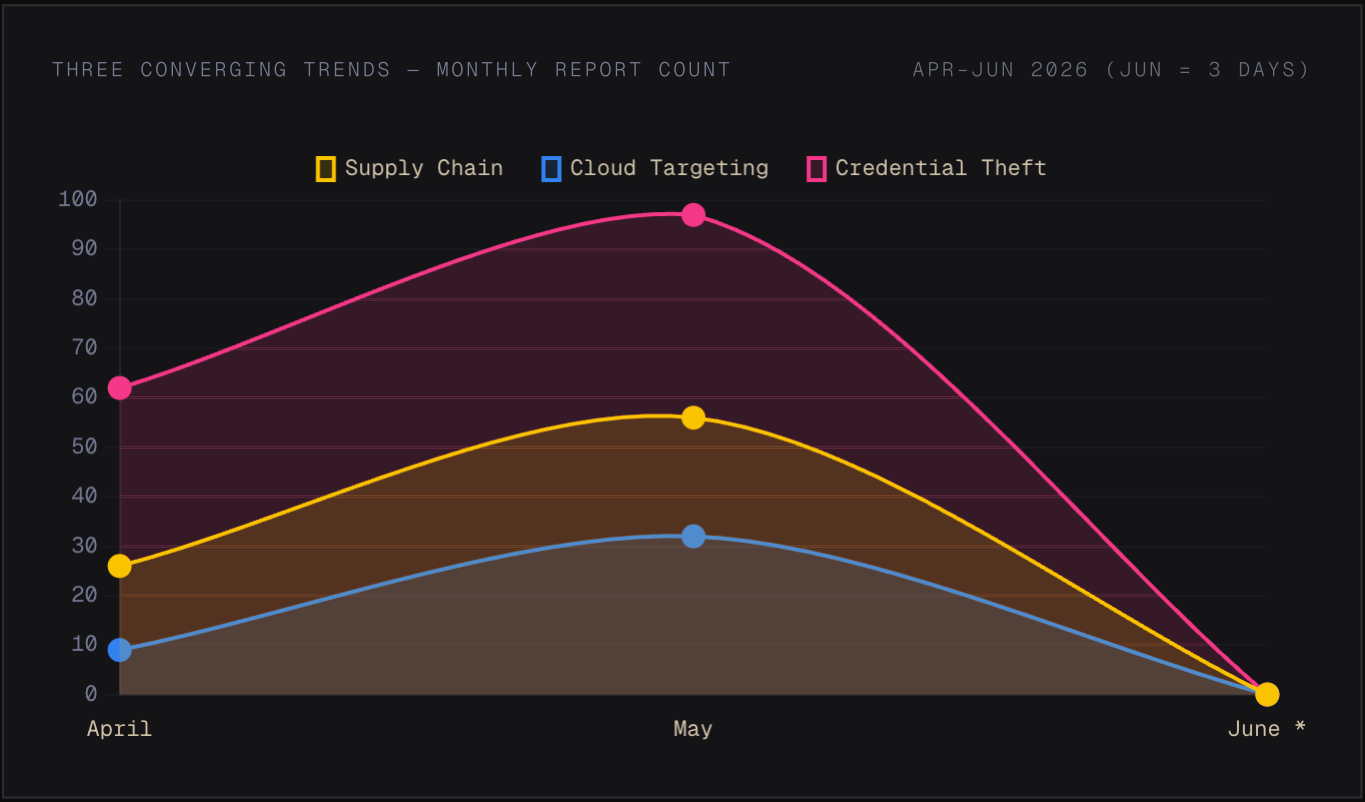
ATT&CK COVERAGE

519 of 548 prior techniques reappeared. New reports add depth, not new technique IDs.

04 — TRENDS

Three vectors, one paradigm

Supply chain compromise, cloud infrastructure targeting, and credential theft grew independently but are operationally linked. Together they describe a single maturing attack: compromise the developer ecosystem to harvest cloud secrets at scale.



SUPPLY CHAIN

Reports grew from 26 in April to 56 in May. A 5,500% increase since January. Five independent actor clusters now operate concurrently against npm, PyPI, VSCode, and GitHub Actions.

CLOUD TARGETING

Cloud infrastructure is no longer a nation-state-only target. Espionage (APT28), criminal (UNC6780), and destructive (Storm-2949) actors all converged on cloud as the primary target environment by May.

CREDENTIAL THEFT

The credential surface expanded from browser passwords in January to include cloud API keys, SSH keys, Telegram sessions, crypto wallet seeds, webcam streams, and CI/CD pipeline secrets by May.

STRATEGIC READ

All three trends share the same architecture: supply chain compromise is the delivery mechanism, cloud infrastructure is the target environment, credential theft is the objective. UNC6780, NICKEL TAPESTRY, and Shai-Hulud all embody this exact convergence simultaneously and independently of each other.

05 — TTPS

Top 10 techniques with procedure detail

519 unique ATT&CK techniques observed across the quarter. Click any row to expand the concrete procedure example observed in this corpus. These are real implementations, not generic descriptions.

01 T1027

Obfuscated Files or Information

DEFENSE EVASION

UNC6780, Emerald Sleet, UAC-0194, Mustang Panda, Lazarus Group + 10 others

261 REPORTS

Mini Shai-Hulud procedure: The npm payload encodes its exfiltration logic using a multi-layer scheme. The outer package postinstall script contains a Base64-encoded gzip blob that decodes to a second-stage JavaScript file, which itself uses String.fromCharCode() array shuffling to reconstruct the C2 URL and credential-harvesting routines at runtime. The malicious string literals are never present in plain text in any static analysis pass of the package source. Detection is only possible through behavioral analysis of runtime execution.

02

T1071.001

Web Protocol C2

COMMAND AND CONTROL

UNC6780, Emerald Sleet, Void Arachne, GOLD FLAME, GlassWorm

219 REPORTS

GlassWorm procedure (novel Solana C2): Rather than conventional HTTP C2 beaconing, GlassWorm issues read-only RPC calls to the Solana blockchain via api.mainnet-beta.solana.com to retrieve commands embedded in the memo field of on-chain transactions. All C2 traffic appears as legitimate HTTPS requests to a well-known blockchain API endpoint, indistinguishable from DeFi application activity on standard proxy logs. This C2 architecture cannot be sinkholed or blocked without blocking all Solana API traffic.

03

T1036.005

Match Legitimate Resource Name

DEFENSE EVASION

Mustang Panda, Void Arachne, UAC-0194, Emerald Sleet, APT28, NICKEL TAPESTRY + 15 others

195 REPORTS

NICKEL TAPESTRY procedure: Published a trojanized npm package named @bitwarden/cli@2026.4.0, a version string that exactly matches the legitimate Bitwarden CLI release cadence. The package passed initial automated scanning because its package.json metadata, README, and exported API surface were copied verbatim from the real package. Only the postinstall lifecycle hook contained the malicious credential-harvesting payload. Any developer installing it via npm install would see no visible difference from the legitimate package.

04

T1041

Exfiltration Over C2 Channel

EXFILTRATION

UNC6780, Emerald Sleet, Void Arachne, GOLD FLAME, calipology

156 REPORTS

MicrosoftSystem64 procedure: Exfiltrates harvested AWS keys, GitHub tokens, and npm registry credentials by encoding them as JSON and uploading directly to the attacker's HuggingFace model repository via the HuggingFace Hub API at huggingface.co/api/datasets. The exfiltration traffic is HTTPS to a legitimate, widely-used ML platform, virtually identical to normal developer workflow traffic in any organisation using AI tooling. Standard DLP rules based on destination reputation would not flag this channel.

05

T1082

System Information Discovery

DISCOVERY

Emerald Sleet, GOLD FLAME, APT23, UAT-8302

152 REPORTS

PLASMAGRID iOS procedure: Immediately post-exploitation, the implant queries UIDevice.current for device model, iOS version, UDID, carrier name, and battery state, then issues a CTTelephonyNetworkInfo call to retrieve the current radio access technology (4G or 5G). This triage packet is sent to the C2 within 800ms of initial execution. Operators use this to determine whether to proceed with full data exfiltration or silently terminate on sandbox or virtual device detections.

06

T1105

Ingress Tool Transfer

COMMAND AND CONTROL

UNC6780, Emerald Sleet, Mustang Panda, NICKEL TAPESTRY, Lazarus Group

150 REPORTS

BeaverTail procedure (DPRK Contagious Interview): After initial execution via a malicious npm package in a fake coding interview task, BeaverTail downloads its second-stage payload InvisibleFerret by issuing a GET request to a GitHub Gist URL constructed dynamically at runtime from encoded string fragments. This ensures the staging URL is never static in the malware binary and rotates across campaigns, making indicator-based blocking ineffective without behavioral detection of the construction pattern itself.

07

T1140

Deobfuscate/Decode Files

DEFENSE EVASION

UAC-0194, Emerald Sleet, Mustang Panda, APT23, GOLD FLAME

112 REPORTS

CastleLoader procedure: The loader arrives as a legitimate-looking DLL sideloaded via a renamed Windows system binary. At runtime it reads an encrypted blob from a .dat file in the same directory, decrypts it using a hardcoded RC4 key derived from the victim machine's MachineGUID registry value, making the decrypted payload machine-specific and non-portable. The result is decompressed via ZLib before reflective loading into memory. An analyst cannot decrypt the payload without the specific victim's MachineGUID, severely limiting static analysis.

08

T1059.001

PowerShell

EXECUTION

UAC-0194, Emerald Sleet, Mustang Panda, SHADOW-EARTH-053, GOLD FLAME

111 REPORTS

UAC-0194 ClickFix procedure: Delivers a ClickFix-themed lure page that instructs victims to paste a PowerShell one-liner with ExecutionPolicy Bypass and WindowStyle Hidden flags directly into the Windows Run dialog. The encoded command downloads a second-stage PS1 from a compromised Ukrainian government-adjacent domain, patches AMSI in the current session, then loads a .NET reflective RAT. The entire execution chain runs in-memory with no files written to disk post-initial-execution.

09

T1583.001

Acquire Infrastructure: Domains

RESOURCE DEVELOPMENT

Mustang Panda, Emerald Sleet, NICKEL TAPESTRY, APT28, Lazarus Group, Nimbus Manticore

109 REPORTS

Emerald Sleet procedure: Registered a cluster of domains mimicking South Korean government tax and authentication portals using privacy-protected registrars in Iceland and Panama, with registration timestamps clustered within a 72-hour window preceding each campaign wave. The domains resolved to the same /24 IP block and served identical TLS certificates. This registration infrastructure pattern enables proactive hunting across all domains even when only one is identified in active use.

10

T1552.001

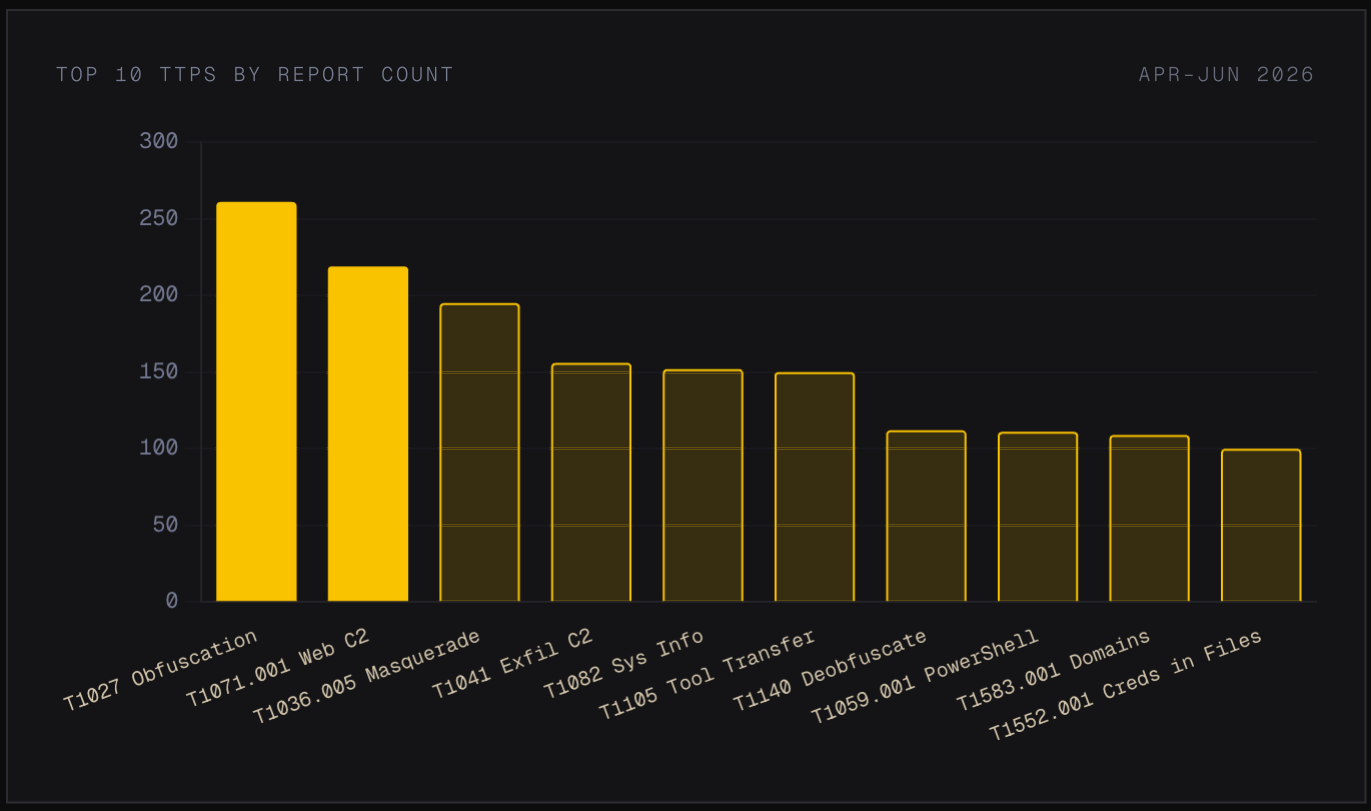
Credentials in Files

CREDENTIAL ACCESS

UNC6780 (dominant, 10+ reports), NICKEL TAPESTRY, GOLD FLAME

100 REPORTS

PCPJack procedure: When installed as a malicious npm package in a CI/CD environment, PCPJack's postinstall hook executes a Node.js script that reads these paths in sequence: ~/.aws/credentials, ~/.config/gcloud/application_default_credentials.json, ~/.npmrc, ~/.pypirc, $GITHUB_TOKEN, and all .env files in the current working directory up to depth 4. All discovered secrets are encoded as base64 and exfiltrated over HTTPS to an oob.moika.tech subdomain. The full harvest occurs in under 2 seconds of package installation.



06 — KILL CHAIN COVERAGE

ATT&CK tactic phase distribution

519 unique techniques mapped across 14 tactic phases. Defense Evasion dominates by a 2:1 margin over C2. Execution has the highest report-to-technique ratio despite only 26 unique techniques, appearing in 306 reports.

POST-COMPROMISE

Defense Evasion

91

351 reports · 511 entities

POST-COMPROMISE

Command and Control

48

323 reports · 450 entities

PRE-COMPROMISE

Resource Development

41

226 reports · 272 entities

POST-COMPROMISE

Discovery

38

231 reports · 263 entities

POST-COMPROMISE
Collection
35
198 reports · 216 entities

POST-COMPROMISE
Credential Access
29
207 reports · 229 entities

OBJECTIVE
Impact
28
134 reports · 133 entities

EXECUTION
Execution
26
306 reports · 372 entities

PRE-COMPROMISE
Reconnaissance
24
69 reports · 76 entities

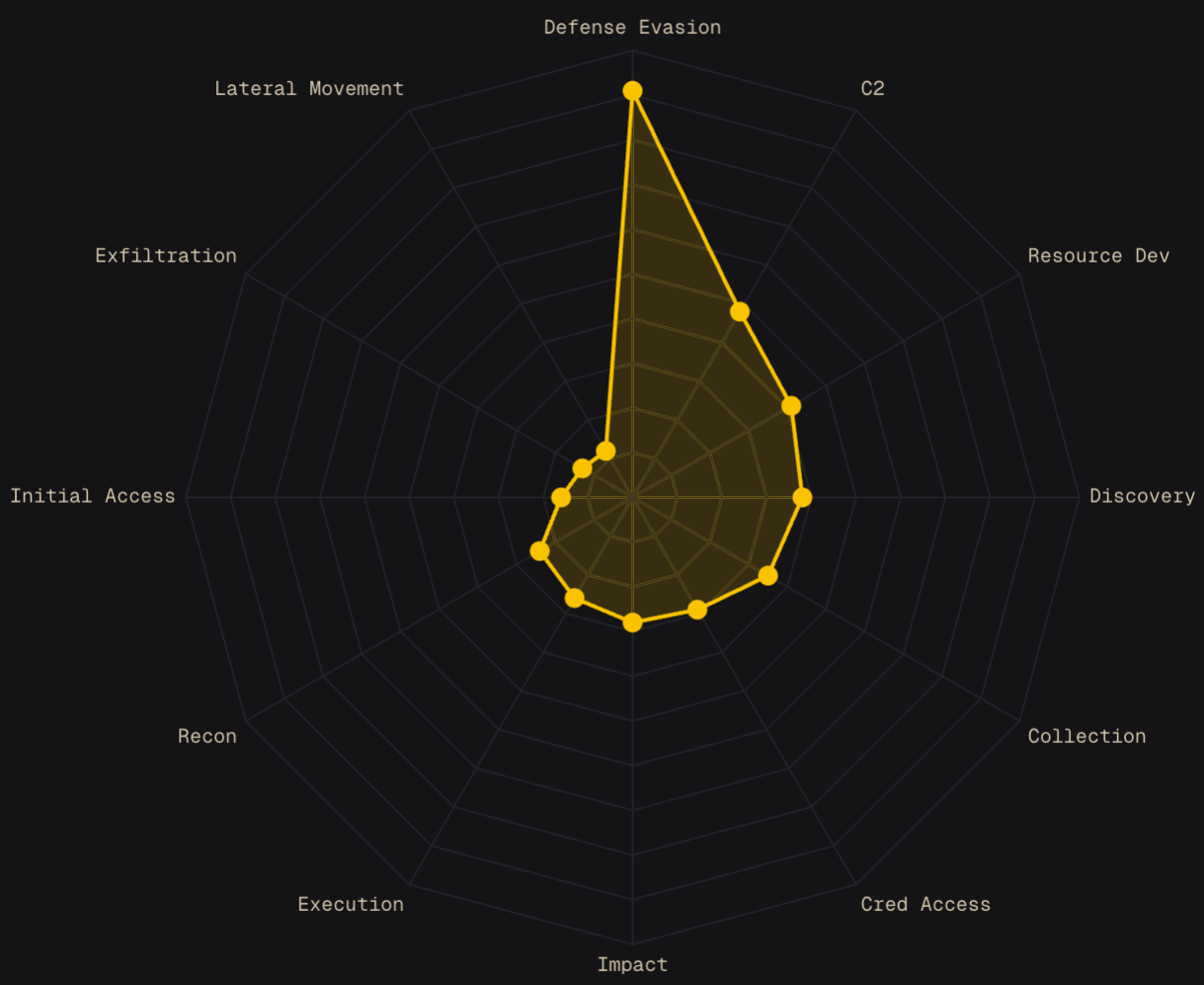
INITIAL ACCESS
Initial Access
16
307 reports · 394 entities

OBJECTIVE
Exfiltration
13
201 reports · 205 entities

POST-COMPROMISE
Lateral Movement
12
58 reports · 59 entities

KILL CHAIN COVERAGE — TECHNIQUES PER TACTIC PHASE

RADAR VIEW



EXECUTION DENSITY ANOMALY

Only 26 unique Execution techniques but referenced in 306 reports — the highest report-to-technique ratio. PowerShell, JavaScript, and Malicious File execution dominate and appear across virtually every campaign. The technique surface is narrow but trafficked intensively.

LATERAL MOVEMENT GAP

Only 12 unique techniques and 58 reports — the thinnest post-compromise tactic. This is either a genuine gap in adversary lateral movement activity, or a corpus gap in post-initial-access reporting depth. Either interpretation warrants investigation in Q3.

07 — THREAT ACTORS

Top 8 actors by report count

DPRK actors hold 3 of the top 8 slots. UNC6780's May explosion (10 reports in a single month) was the defining statistical event of the quarter. Criminal activity reached parity with nation-state reporting for the first time in May.

UNC6780 TeamPCP / Shai-Hulud

Criminal (China-assessed) · Financial

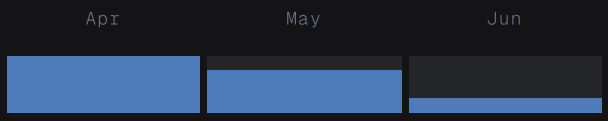
11 TOTAL

CI/CD credential theft via supply chain. 10-report May surge driven by Mini Shai-Hulud, Trivy, Bitwarden CLI, and LiteLLM campaign waves.

Lazarus Group DPRK / TraderTraitor

North Korea (RGB Bureau 121) · Financial + Espionage

8 TOTAL

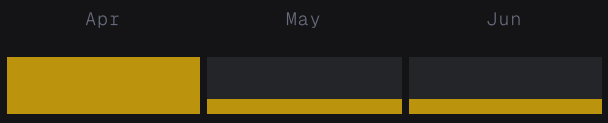


Most consistently active actor across all three months. Bybit follow-on, Drift Protocol heist, Operation 99, npm supply chain campaigns.

Mustang Panda Earth Preta

6 TOTAL

China · Espionage

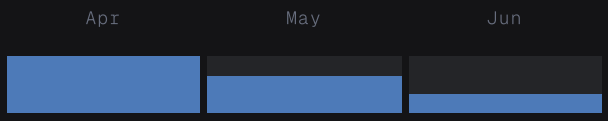


April-heavy: LOTUSLITE, PlugX DLL sideloading, Taiwan government and ASEAN diplomatic mission targeting.

Emerald Sleet Kimsuky / TA427

6 TOTAL

North Korea (RGB Bureau 325) · Espionage

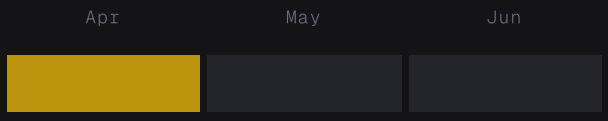


Steady and consistent throughout Q2. South Korean security software spoofing, Webex recruitment impersonation, embassy targeting.

Void Arachne Silver Fox

4 TOTAL

China (criminal) · Financial

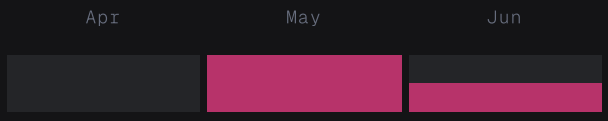


4 reports entirely in April, then absent. Tax-authority lure campaigns across Taiwan, Japan, and Southeast Asia. Possible operational pause.

UAC-0194 Russia-nexus

3 TOTAL

Russia-nexus · Espionage / Disruption



The only actor trending upward month-on-month. ClickFix PowerShell campaigns against Ukrainian Defense Forces. PhantomRelay/LegionRelay RAT deployment. Watch for Q3 escalation.

NICKEL TAPESTRY DPRK IT Workers

3 TOTAL

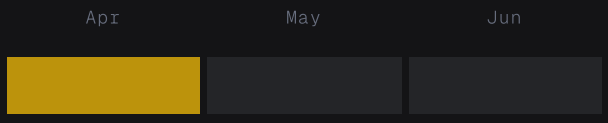
North Korea (RGB) · Financial + Espionage

3 reports entirely in May. Trivy supply chain attack, MicrosoftSystem64/HuggingFace exfil, Bitwarden CLI trojanization. 135+ synthetic IT worker personas active.

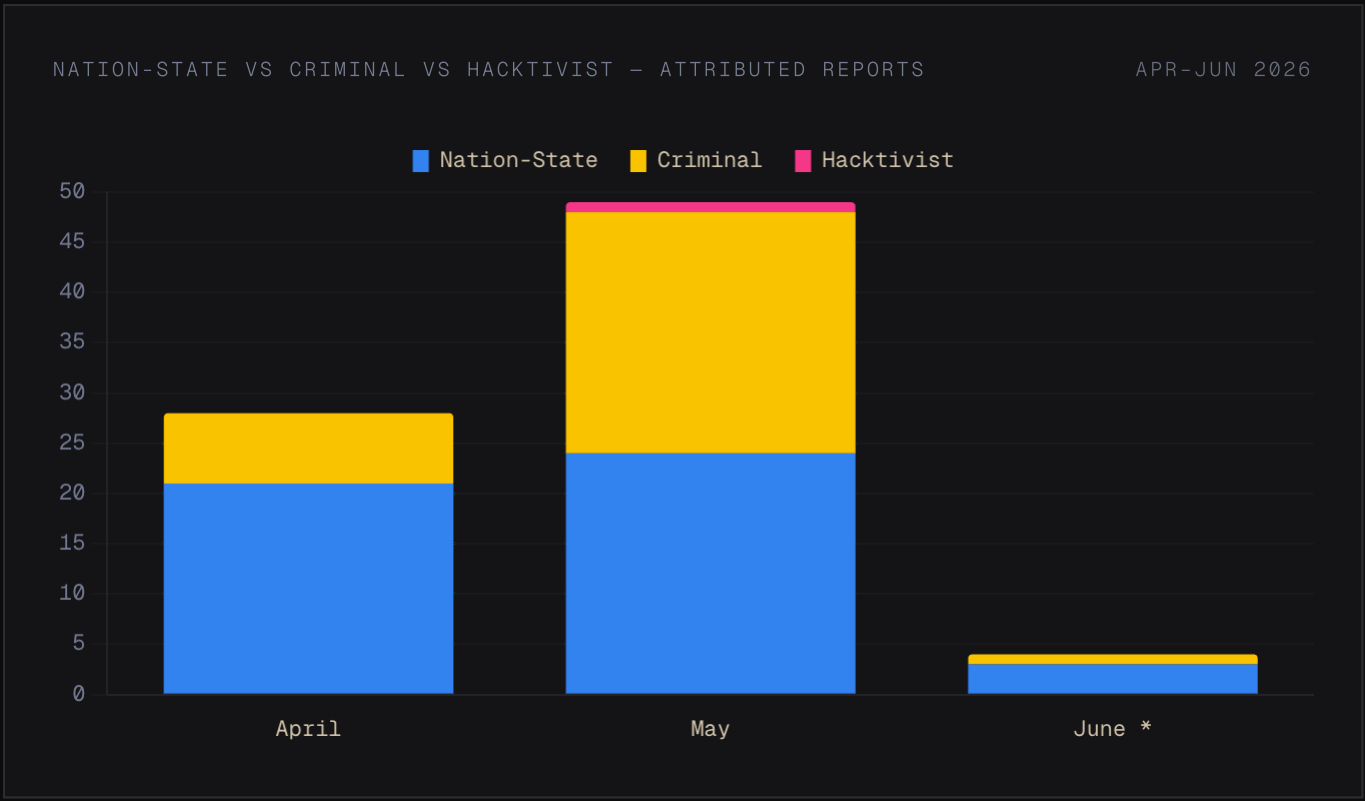
flexhere687-art Unattributed

2 TOTAL

Unknown (UK-targeting) · Credential theft



Low-sophistication but notable: exploiting CVE-2017-11882 (9 years old) via Blogger-hosted payloads delivering XWorm against UK Finance and Government targets in 2026.



08 — VICTIMOLOGY

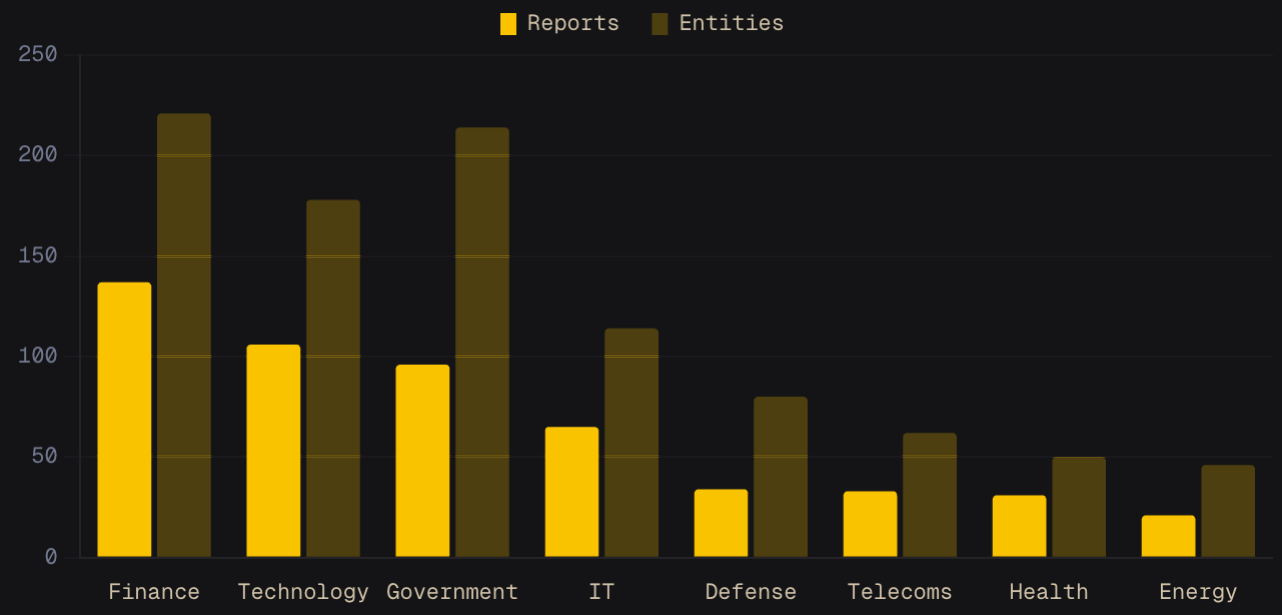
Top 8 targeted sectors

Finance leads with 137 reports across 221 entities. Finance and Technology combined account for 65% of top-8 report volume. Government had the sharpest month-on-month decline (52 to 36 reports). Health is uniquely stable at 14 reports in both April and May.

SECTOR	REPORT COVERAGE	REPORTS	ENTITIES
Finance		137	221
Technology		106	178
Government		96	214
IT		65	114

Defense	34	80
Telecoms	33	62
Health	31	50
Energy	21	46

SECTOR TARGETING — REPORTS VS ENTITIES APR-JUN 2026



✧ SOL

Turn this landscape into proactive defense

This is the global picture. Sol assesses the threats that matter to you, then hunts, simulates, and hardens your defenses across the stack you already run — autonomously, in minutes, not days.

Book a demo →

ELEZAR SOL

Quarterly Threat Landscape · April to June 2026 · 372 reports · 121 vendors

Published July 2026

Kaartheeswaran Ravichandran · linkedin.com/in/kaartheeswaran