SOL THREAT INTELLIGENCE

June 2026 Government, Public Administration and Defense Regional Sector Brief

- 1 JUN TO 30 JUN 2026
- 3 REGIONAL ASSESSMENTS
- 4 PAGES PER REGION
- PREPARED BY KAARTHEESWARAN RAVICHANDRAN

AMERICAS

EXECUTIVE SUMMARY

Major-event convergence, PeopleSoft exploitation and destructive activity drive risk

The Americas Government, Public Administration and Defense sector faced a convergence of broad-surface exploitation, event-driven targeting and destructive activity in June 2026. The FIFA World Cup across the United States, Canada and Mexico created a shared attack surface across transport, telecommunications, energy and public services. ShinyHunters exploited Oracle PeopleSoft CVE-2026-35273 against government-deployed systems, while Operation Endgame revealed extensive SocGholish reach into government networks. Iranian-linked Ababil of Minab activity added a destructive wiper dimension against US transportation infrastructure.

KEY INSIGHTS

1	The FIFA World Cup created concurrent nation-state, hacktivist and criminal targeting of tri-national government and critical infrastructure.
2	ShinyHunters exploited PeopleSoft CVE-2026-35273 and used MeshCentral agents disguised as Azure services.
3	SocGholish reached 55 percent of government networks in Infoblox telemetry and progressed to tier-two C2 on a subset.
4	Iranian-linked Ababil of Minab conducted destructive activity against US transportation infrastructure including LACMTA.

5	NKWIPER and FSWIPER samples appeared on the first two tournament days, elevating wiper-monitoring requirements.
6	Government risk came from broad exploitation and event-driven convergence rather than a single precision espionage campaign.

Top threat entities and June trend shifts

- **ShinyHunters** CRIMINAL EXTORTION

  Exploited Oracle PeopleSoft zero-day and used MeshCentral C2 disguised as Microsoft Azure tooling.

- **GOLD PRELUDE / TA569** INITIAL ACCESS BROKER

  Operated SocGholish through compromised WordPress sites, staged JScript and domain-shadowed C2.

- **Ababil of Minab** NATION-STATE

  Iranian MOIS-linked destructive actor associated with data-wiping activity against US transportation infrastructure.

- **VOLTZITE** NATION-STATE

  Assessed threat to tournament-adjacent critical infrastructure through long-term pre-positioning.

- **Sandworm / Iridium** NATION-STATE

  Historical major-event destructive capability and relevant Olympic Destroyer precedent.

- **NoName057(16) / Handala** HACKTIVIST

  DDoS and politically motivated targeting of government and critical infrastructure.

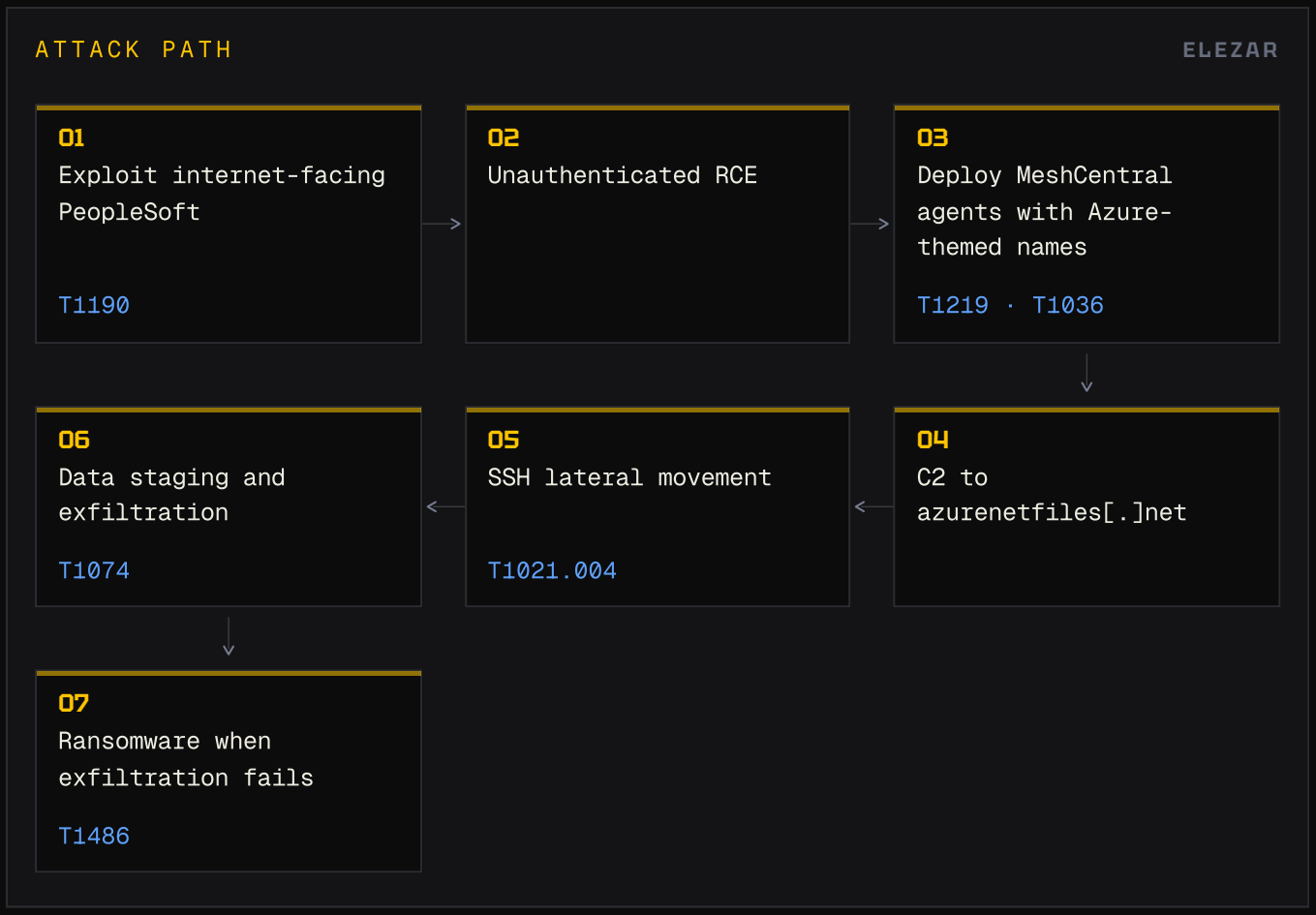
Trend shifts versus May 2026

1	Major-event operations created simultaneous risk across three national jurisdictions.
2	Government-deployed PeopleSoft became an active zero-day exploitation surface.
3	SocGholish exposure was quantified at scale across government networks.
4	Destructive Iranian activity against US public infrastructure was directly confirmed.
5	Azure-themed masquerading and legitimate RMM tooling continued to blur malicious and administrative traffic.

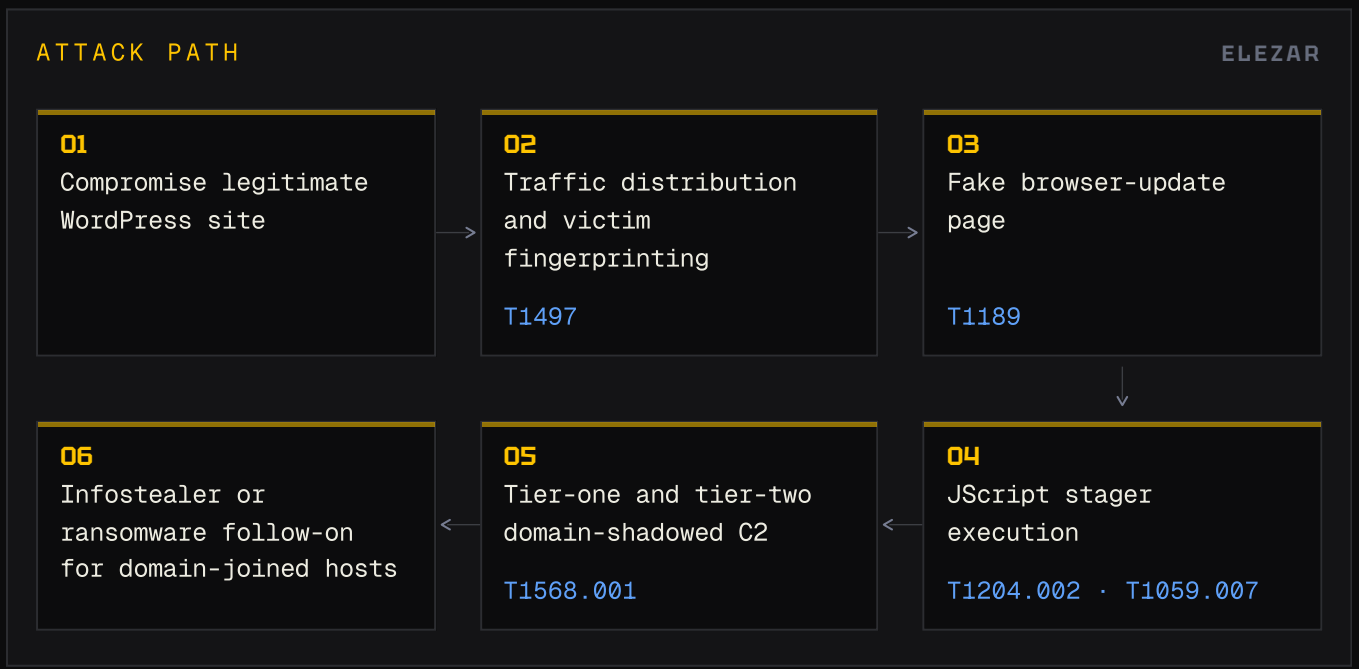
Attack chains, vulnerabilities and indicators

CVE	PRODUCT	SEVERITY	JUNE CONTEXT
CVE-2026-35273	Oracle PeopleSoft	Critical	ShinyHunters zero-day exploitation
CVE-2026-21509	Document client	High	APT36 spear-phishing relevance
CVE-2021-40539	ManageEngine ADSelfService Plus	Critical	Identity infrastructure exploitation
CVE-2026-48027	Nx Console VSCode Extension	High	Government developer supply-chain risk

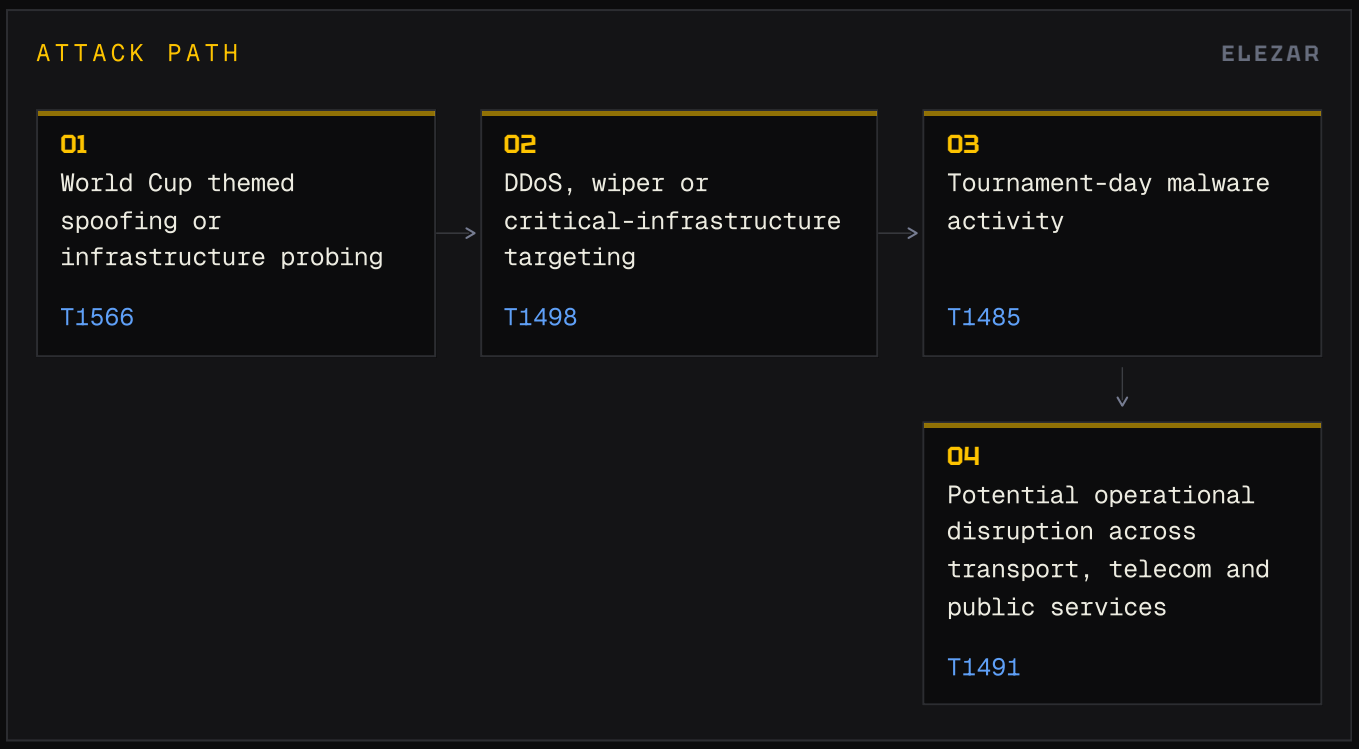
ShinyHunters PeopleSoft



SocGholish



Event and destructive threat



Selected indicators

TYPE	INDICATOR	ATTRIBUTION
Domain	azurenetfiles[.]net	ShinyHunters MeshCentral C2
IP	142[.]11[.]200[.]186-190 / 176[.]120[.]22[.]24	ShinyHunters
File	meshagent32-azure-ops.exe / meshagent64-azure-ops.exe	ShinyHunters
Domain	pa-portal[.]benningtonspringsmhp[.]com	SocGholish tier one
Domain	billing[.]roofnrack[.]us	SocGholish tier one
IP	198[.]37[.]123[.]126 / 159[.]203[.]45[.]201	Iranian-associated activity
File	RECOVERY_INFO.txt / .lalia	Lalia ransomware indicators

Prioritized defensive guidance

Recommendations are calibrated for government identity systems, public-service platforms, defense-adjacent networks, cloud services, remote-access infrastructure and high-impact operational continuity requirements.

IMMEDIATE: ACT WITHIN 72 HOURS

1. Patch PeopleSoft CVE-2026-35273 and investigate pre-patch exposure.
2. Block ShinyHunters C2 and hunt unauthorized MeshCentral agents.
3. Audit transportation and public-service systems for destructive Iranian activity.
4. Validate offline recovery for wiper scenarios.

URGENT: ACT WITHIN 2 WEEKS

1. Deploy DNS-behavioral detection for SocGholish domain shadowing.
2. Hunt JScript execution from browser-download and temporary directories.
3. Maintain elevated World Cup monitoring through the event close.
4. Restrict public PeopleSoft exposure and require VPN-authenticated administration.

STRATEGIC UPLIFT

1. Rotate WordPress administrator credentials and apply file-integrity monitoring.
2. Inventory and allowlist approved RMM tools across government networks.

3. Patch the affected Nx Console extension on developer workstations.

4. Detect Azure-named executables or domains resolving outside Microsoft infrastructure.

June source reports: PolySwarm FIFA World Cup threat assessment, Intel 471 ShinyHunters PeopleSoft analysis, Infoblox Operation Endgame and SocGholish reporting, and CYFIRMA Weekly Intelligence Report dated 5 June 2026.

EMEA

EXECUTIVE SUMMARY

Cloud-resident C2 and long-dwell espionage define the June threat picture

EMEA Government, Public Administration and Defense faced a multi-vector espionage environment in June 2026. Operation Dragon Weave directly targeted Czech government personnel with RUSTCLOAK and the Azure-resident AZUREVEIL implant. UNC5221 remained relevant through BRICKSTORM operations against European industry and government-adjacent environments, while a regional infrastructure study identified 3,923 malicious C2 servers across Eastern Europe. The wider reporting corpus rose from 164 to 455 reports, a 177 percent increase from May.

KEY INSIGHTS

1	Operation Dragon Weave used Czech-language government lures and Azure Blob Storage as a long-lived dead-drop C2 channel.
2	BRICKSTORM used DNS-over-HTTPS, WebSocket, Yamux and nested TLS to evade conventional monitoring.
3	Chinese intelligence services were reported using LinkedIn to target government and military personnel.
4	Eastern Europe hosted 3,923 mapped C2 servers across 302 providers, supporting both espionage and ransomware.
5	QV ransomware added ESXi targeting and bootkit persistence to the regional government threat set.
6	Legitimate cloud infrastructure became the defining C2 concealment method for the month.

Top threat entities and June trend shifts

- **Operation Dragon Weave** ESPIONAGE CAMPAIGN

Targeted Czech government officials with social-security themed lures, RUSTCLOAK and AZUREVEIL.

- **UNC5221 / Silk Typhoon** NATION-STATE

Used edge-device exploitation and BRICKSTORM for long-running espionage and Microsoft 365 access.

- **Cloud Atlas** NATION-STATE

Active in Eastern European infrastructure and targeted Russian and Belarusian government entities.

- **PARISITE / Pioneer Kitten** NATION-STATE

Exploited Palo Alto GlobalProtect from Eastern European infrastructure.

- **Black Basta** RANSOMWARE

Used Teams-based vishing, AnyDesk and credential dumping in the same regional infrastructure ecosystem.

- **QV Ransomware** RANSOMWARE

New Windows and ESXi strain with bootkit persistence and shadow-copy deletion.

Trend shifts versus May 2026

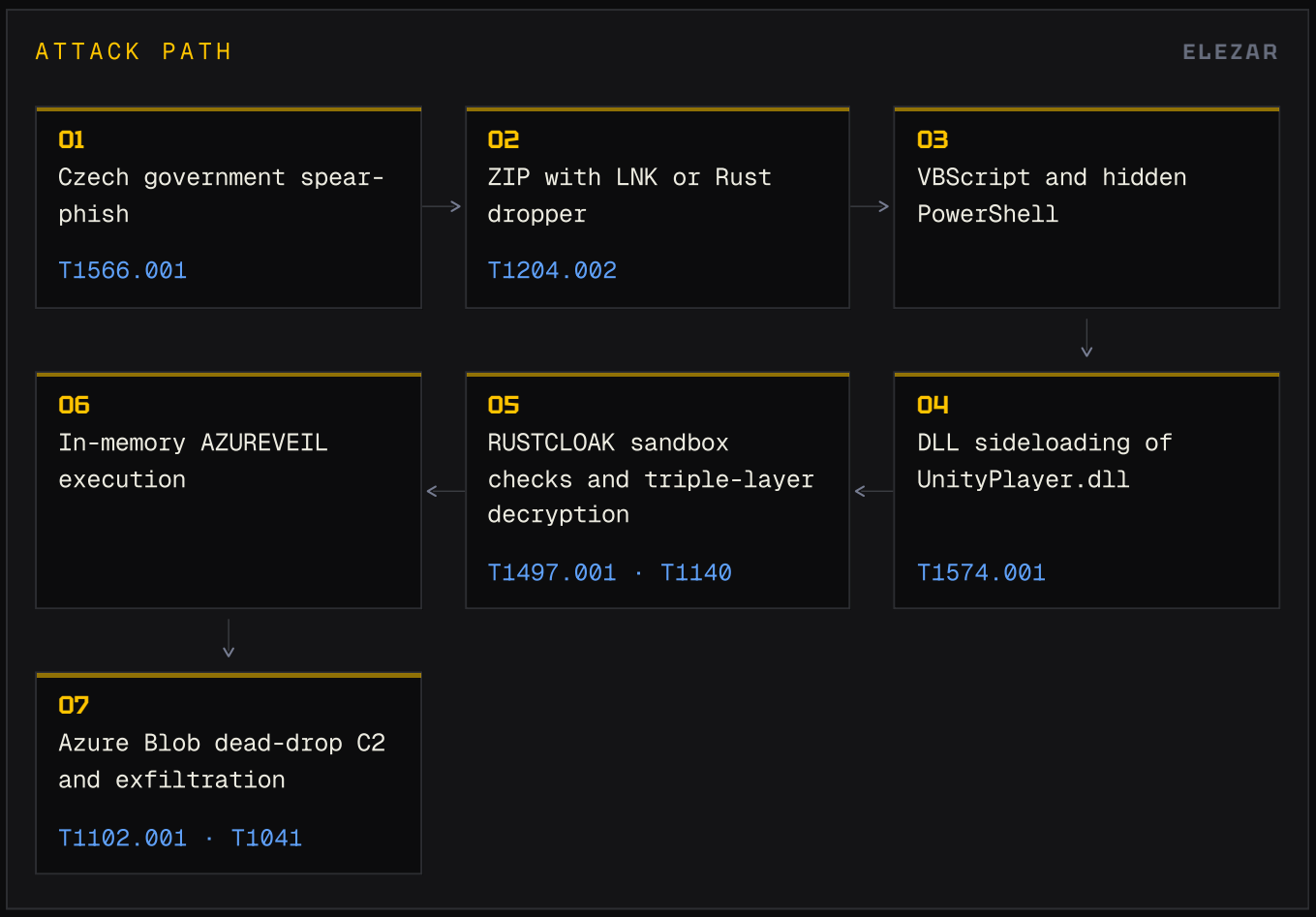
1	Azure Blob Storage, Cloudflare Workers, Heroku and public DoH resolvers were used to blend C2 with legitimate traffic.
2	Czech government targeting became directly confirmed in June.
3	LinkedIn-based intelligence collection against military and government personnel received a Five Eyes warning.
4	Regional infrastructure mapping established a new baseline of 3,923 active C2 servers.

5 ESXi-targeting ransomware and bootkit persistence expanded the government data-center risk.

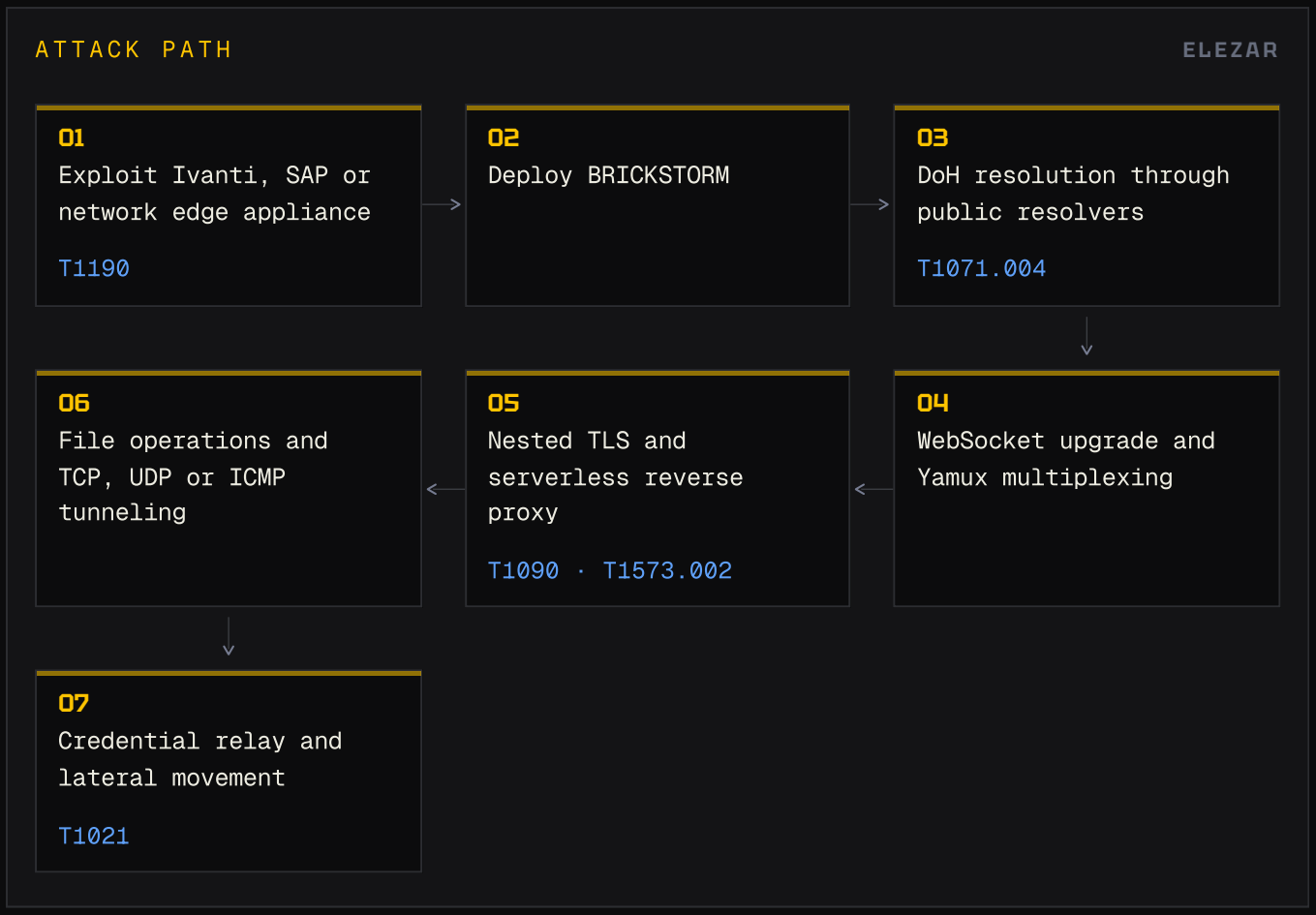
Attack chains, vulnerabilities and indicators

CVE	PRODUCT	SEVERITY	JUNE CONTEXT
CVE-2026-0257	Palo Alto GlobalProtect	Critical	PARISITE exploitation
CVE-2025-22457	Ivanti Connect Secure	Critical	UNC5221 initial access
CVE-2025-31324	SAP NetWeaver	Critical	Chinese-nexus exploitation
CVE-2026-35273	Oracle PeopleSoft	Critical	Government and public-sector exposure
CVE-2026-8936	Docker Desktop	8.2	Government DevOps relevance

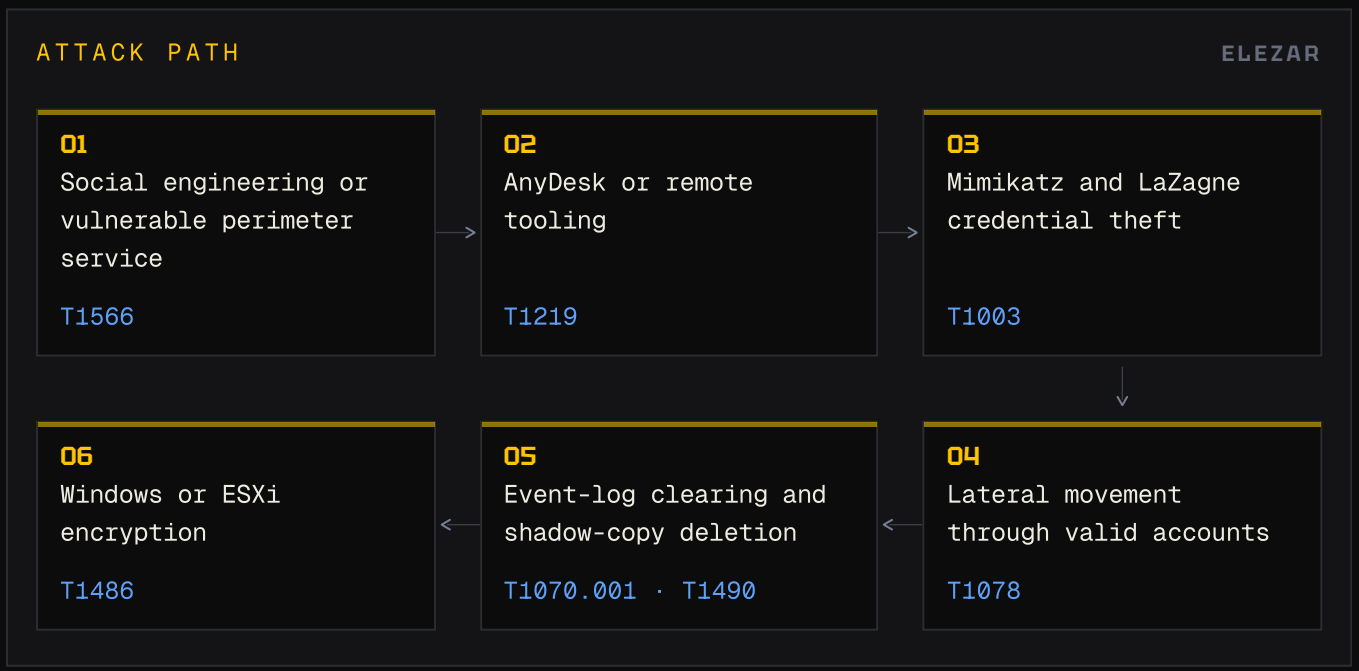
Operation Dragon Weave



UNC5221 BRICKSTORM



Eastern European ransomware access



Selected indicators

TYPE	INDICATOR	ATTRIBUTION
Domain	note1ggbbhggdwa1[.]blob[.]core[.]windows[.]net	AZUREVEIL C2
File	UnityPlayer.dll / RuntimeBroker_update.exe	Dragon Weave
Path	%LOCALAPPDATA%\WebViewFixUtility	Dragon Weave staging
Domain	ms-azure[.]azdatastore[.]workers[.]dev	BRICKSTORM proxy
Domain	ms-azure[.]herokuapp[.]com	BRICKSTORM proxy
IP	64[.]176[.]166[.]79 / 194[.]48[.]199[.]121	BRICKSTORM
Network	application/dns-message over HTTPS	BRICKSTORM DoH

Prioritized defensive guidance

Recommendations are calibrated for government identity systems, public-service platforms, defense-adjacent networks, cloud services, remote-access infrastructure and high-impact operational continuity requirements.

IMMEDIATE: ACT WITHIN 72 HOURS

1. Revoke long-lived Azure Blob SAS tokens and block the Dragon Weave C2 container.

2. Patch GlobalProtect and Ivanti edge devices as emergency priorities.

3. Block BRICKSTORM IOCs and detect DoH traffic from unauthorized endpoints.

URGENT: ACT WITHIN 2 WEEKS

1. Detect DLL sideloading from user-writable paths and WebViewFixUtility artifacts.

2. Hunt Yamux-over-WebSocket and nested TLS patterns.

3. Brief government and military personnel on LinkedIn-based intelligence approaches.

4. Audit PeopleSoft and SAP NetWeaver deployments for exploitation artifacts.

STRATEGIC UPLIFT

1. Restrict external Teams contacts and detect unauthorized remote-access tools.

2. Harden ESXi management and test isolated recovery from ransomware.

3. Apply CASB controls to Azure Blob and other legitimate cloud repositories.

4. Enforce monitored DNS resolution and prevent unmanaged DoH.

June source reports: Operation Dragon Weave reporting, CYFIRMA Weekly Intelligence Report dated 12 June 2026, NVISO BRICKSTORM analysis and Hunt.io Eastern European C2 infrastructure mapping.

APAC

EXECUTIVE SUMMARY

Supply-chain compromise and novel espionage tooling reshape government risk

APAC Government, Public Administration and Defense organizations faced sustained espionage activity in June 2026. Reporting identified three concurrent nation-state campaigns: APT32's domestic targeting pivot through the FireAnt MetaKit supply chain, APT37's NarwhalRAT operation against South Korean personnel, and CL-STA-1062's TinyRCT campaign against Southeast Asian government and state-owned networks. Amaranth-Dragon also weaponized CVE-2025-8088 against Indonesian government and law-enforcement targets. Total reporting rose from 164 reports in May to 455 in June, a 177 percent increase across the wider corpus.

KEY INSIGHTS

1	APT32 shifted from primarily external espionage to domestic Vietnamese targeting through a compromised MetaKit update channel.
2	APT37 introduced NarwhalRAT with keylogging, screen capture, audio recording, USB collection and dual-channel C2.
3	CL-STA-1062 deployed TinyRCT against Southeast Asian government and state-owned networks and exfiltrated source code and MSSQL data.
4	Amaranth-Dragon became the first observed actor to weaponize WinRAR CVE-2025-8088 against Indonesian government targets.
5	Supply-chain compromise, dead-drop cloud C2 and custom malware all increased compared with May.
6	Four government-focused actor clusters were confirmed active in the June intelligence corpus.

Top threat entities and June trend shifts

- **APT32 / OceanLotus** NATION-STATE

  Compromised FireAnt MetaKit update infrastructure to deliver SPECTRALVIPER to Vietnamese domestic targets.

- **APT37 / ScarCruft** NATION-STATE

  Used Microsoft Account security lures to deliver NarwhalRAT against South Korean government and defense-adjacent personnel.

- **CL-STA-1062 / UAT-7237** NATION-STATE

  Targeted Southeast Asian government and state-owned networks with TinyRCT and tunneling tools.

- **Amaranth-Dragon** NATION-STATE

  APT41-linked cluster targeting Indonesian government and law enforcement with CVE-2025-8088, TGAmaranth RAT and Havoc.

- **SPECTRALVIPER** BACKDOOR

  HTTPS C2, named-pipe orchestration, process injection and encrypted Cookie-header beaconing.

- **NarwhalRAT** RAT

  Python-based surveillance malware with pCloud dead-drop fallback and broad collection capability.

Trend shifts versus May 2026

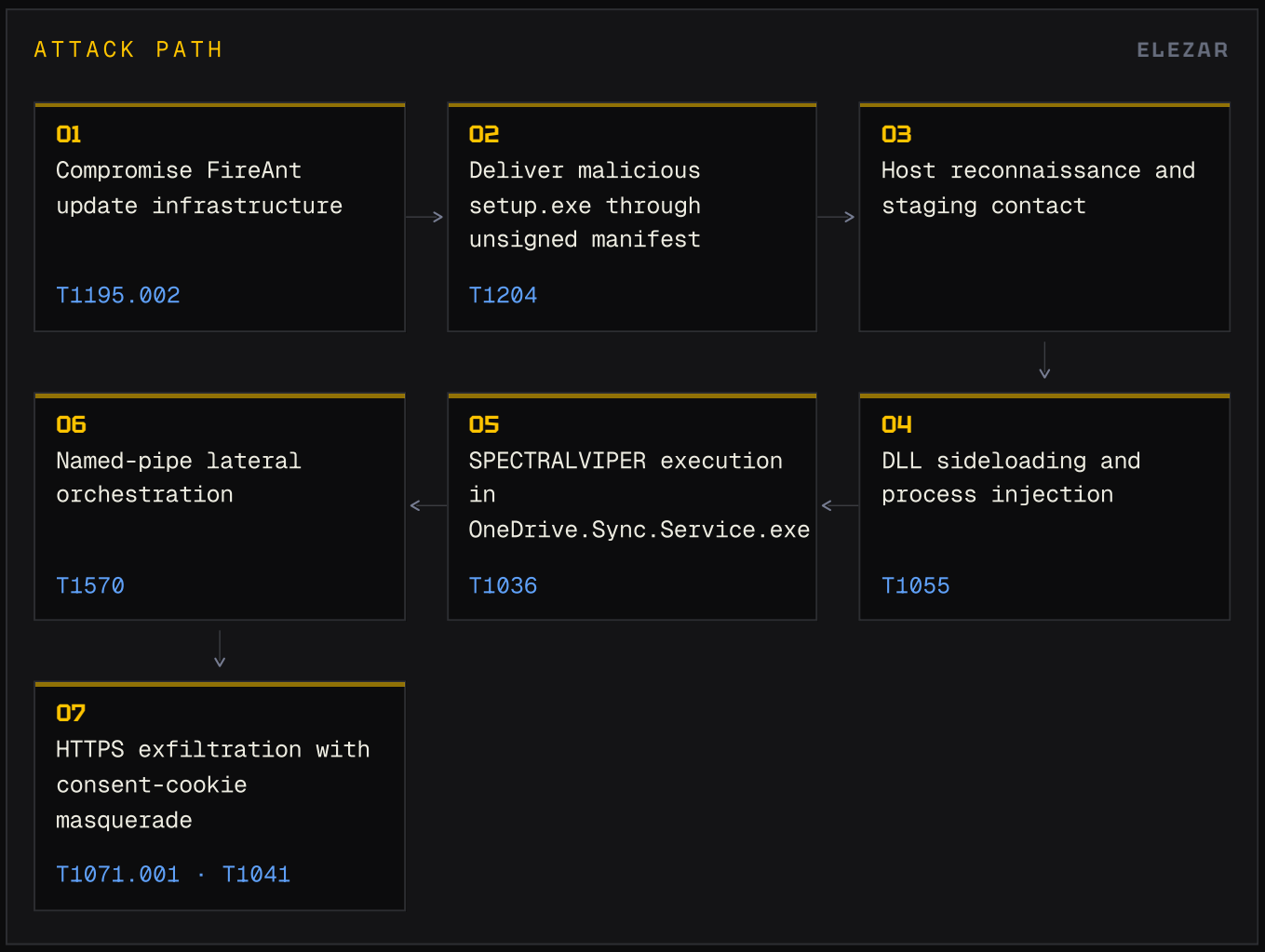
1	Software supply-chain compromise became a confirmed initial-access method against government-adjacent targets.
2	APT32 demonstrated a domestic-targeting pivot rather than only external collection.

3	Three novel malware families appeared in sector reporting: NarwhalRAT, TinyRCT and TGAmaranth RAT.
4	Cloud and dead-drop services were increasingly used for resilient C2.
5	Politically themed and trusted-platform lures remained effective against government personnel.

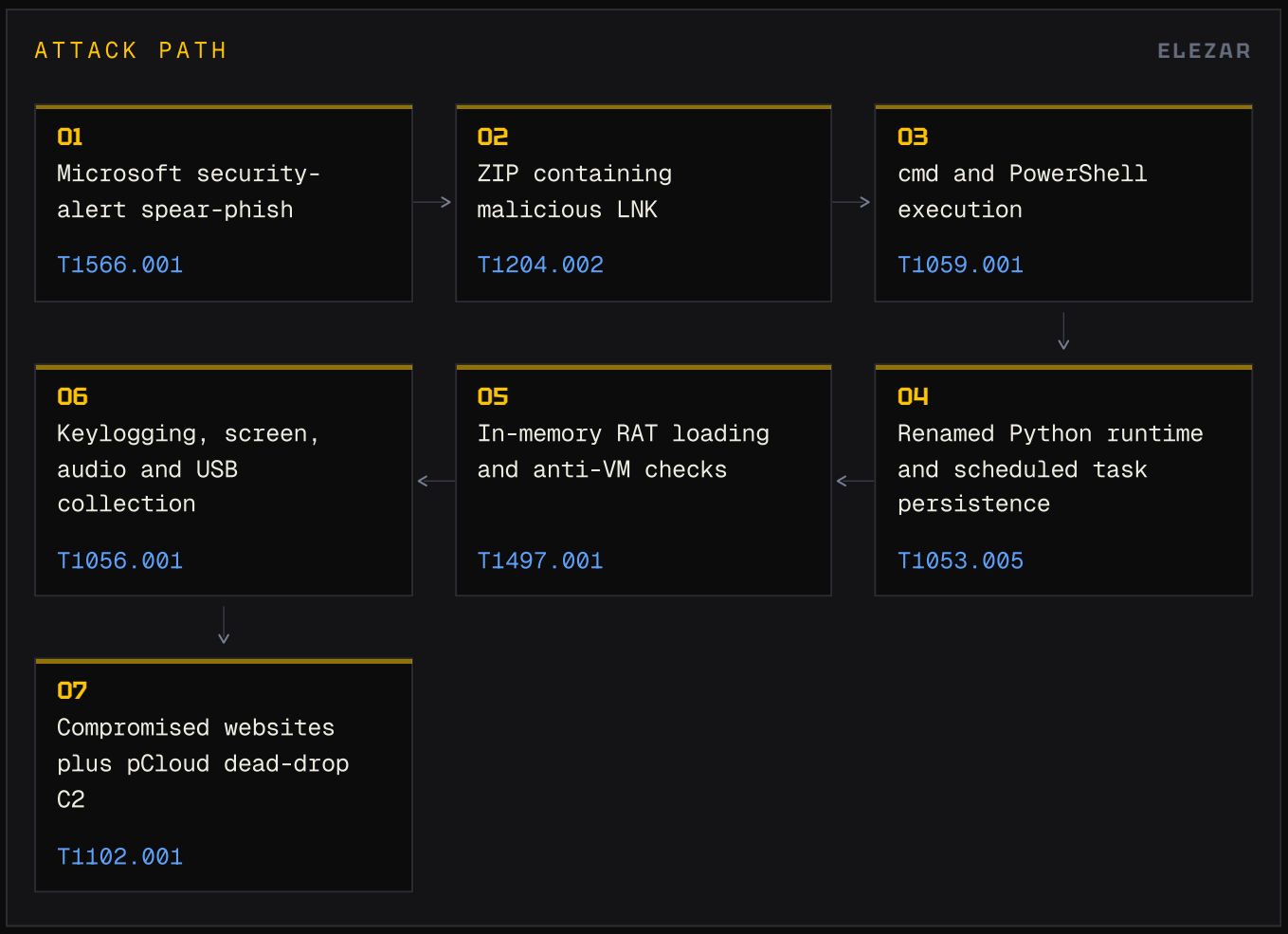
Attack chains, vulnerabilities and indicators

CVE	PRODUCT	SEVERITY	JUNE CONTEXT
CVE-2025-8088	WinRAR	High	Actively weaponized by Amaranth-Dragon
CVE-2021-44228	Apache Log4j	10.0	Used by Chinese-nexus actors for initial access
CVE-2022-40684	Fortinet FortiOS	Critical	Relevant to public-facing government infrastructure
CVE-2022-39952	FortiNAC	Critical	Remote code execution risk
Public-facing MS SQL RCE	Microsoft SQL Server	N/A	Observed against government-linked infrastructure

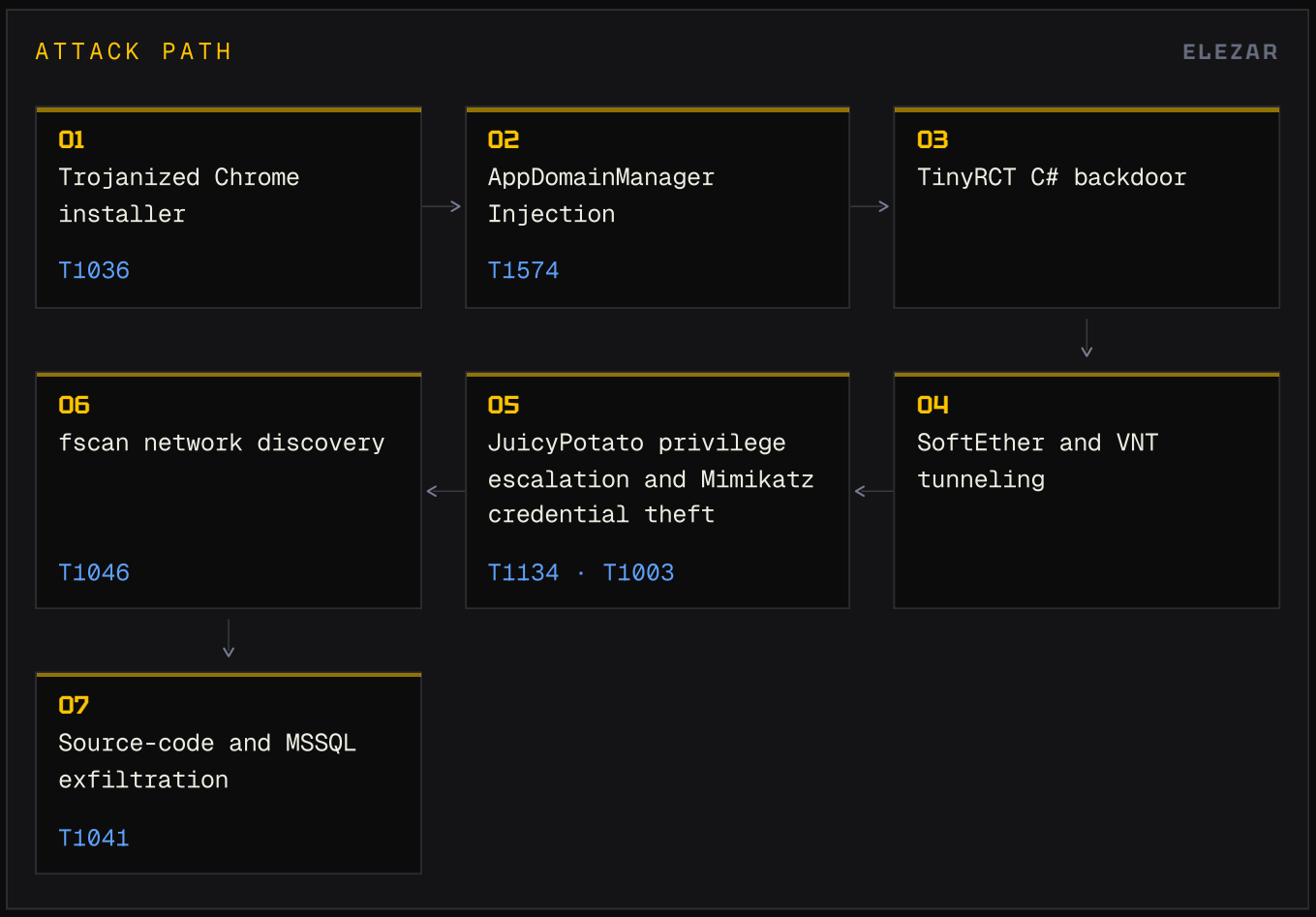
APT32 MetaKit supply chain



APT37 NarwhalRAT



TinyRCT government compromise



Selected indicators

TYPE	INDICATOR	ATTRIBUTION
Domain	financemachinelearning[.]com	SPECTRALVIPER C2
IP	139[.]162[.]11[.]152 / 142[.]91[.]98[.]77	APT32 staging
File	DtlCrashCatch.dll	SPECTRALVIPER loader
Domain	daehoat[.]com / webhostingkorea[.]com	NarwhalRAT C2 and staging
File	userscreen.exe / config.cat	NarwhalRAT
Mutex	i5zJH9FL10cVd3sSW9eyWWErPJ	NarwhalRAT
Path	%APPDATA%\naverwhale	NarwhalRAT staging

Prioritized defensive guidance

Recommendations are calibrated for government identity systems, public-service platforms, defense-adjacent networks, cloud services, remote-access infrastructure and high-impact operational continuity requirements.

IMMEDIATE: ACT WITHIN 72 HOURS

1. Block and hunt SPECTRALVIPER infrastructure and masquerade filenames.
2. Patch WinRAR against CVE-2025-8088 across government endpoints.
3. Isolate software-update mechanisms that lack code signing or transport integrity.

URGENT: ACT WITHIN 2 WEEKS

1. Detect NarwhalRAT scheduled-task and hidden-directory artifacts.
2. Remove public exposure from MSSQL servers and monitor xp_cmdshell activity.
3. Restrict SoftEther, VNT and other unapproved tunneling tools.
4. Sandbox ZIP archives containing LNK files and brief staff on OTP-security lures.

STRATEGIC UPLIFT

1. Formalize third-party software supply-chain security reviews.
2. Monitor SPECTRALVIPER named pipes and unusual OneDrive process behavior.
3. Hunt AppDomainManager Injection artifacts in .NET environments.

4. Add Havoc-specific detection coverage to SIEM and EDR.

June source reports: CYFIRMA OceanLotus reporting, Korean NarwhalRAT analysis, CyberPress TinyRCT reporting and CYFIRMA Weekly Intelligence Report dated 19 June 2026.