SOL THREAT INTELLIGENCE

June 2026 Finance, Bank and Payment Regional Sector Brief

1 JUN TO 30 JUN 2026 ■ 3 REGIONS ■ PREPARED BY KAARTHEESWARAN RAVICHANDRAN

AMERICAS

EXECUTIVE SUMMARY

Ransomware concentration, browser credential theft and trusted-cloud delivery

The Americas finance, banking and payment sector was exposed to a ransomware-dominated threat environment during June 2026. The United States was the most targeted country globally in all four tracked weeks, ranging from 32.10 percent to 45.59 percent of global ransomware victims. Canada reached 7.35 percent in the first tracked week. The source set also identified DragonForce, Securotrop, 3AM ransomware and GoldenGh0stLoader as high-relevance threats to financial infrastructure and developer environments.

KEY INSIGHTS

1	**The United States led global ransomware victimization** during every tracked June week, with a range of 32.10 to 45.59 percent.
2	**DragonForce** targeted organizations with annual revenue of at least USD 15 million and used vulnerable drivers to disable endpoint protection.
3	**Securotrop, a Qilin affiliate**, deployed Chrome credential harvesting through Group Policy to all domain-joined systems.
4	**3AM ransomware** achieved full domain compromise through email bombing, IT vishing, Quick Assist and QEMU-based EDR evasion.
5	**GoldenGh0stLoader** used fake TurboVPN and WhatsApp installers, Google Cloud Storage, Amazon S3 and encrypted WebSocket traffic.

6 **SocGholish and XWorm** remained relevant as access and credential-theft tooling in the tracked period.

Top threat entities and June trend shifts

- **DragonForce / GOLD FLAME** RANSOMWARE

RaaS targeting organizations above USD 15 million annual revenue. Uses Log4Shell, SimpleHelp vulnerabilities, Truesight.sys, RentDrv.sys, Cobalt Strike, Mimikatz, SystemBC and PsExec.

- **Securotrop / Qilin affiliate** RANSOMWARE

Uses Group Policy to deploy Chrome credential theft across domain-joined hosts, followed by LSASS access, PsExec, RDP, VSS deletion and encryption.

- **3AM ransomware** SOCIAL ENGINEERING

Email bombing and Quick Assist initial access, QEMU-hosted QDoor, Duo removal attempts, GoodSync exfiltration to Backblaze and nine-day dwell.

- **GoldenGh0stLoader** RAT

Masquerades as TurboVPN or WhatsApp installers and retrieves encrypted payloads from Google Cloud Storage and Amazon S3 over WebSocket.

- **SocGholish** DRIVE-BY FRAMEWORK

Compromised websites used for downstream payload delivery.

- **XWorm** RAT AND STEALER

Broad credential theft and remote access through phishing and malicious downloads.

Trend shifts versus May 2026

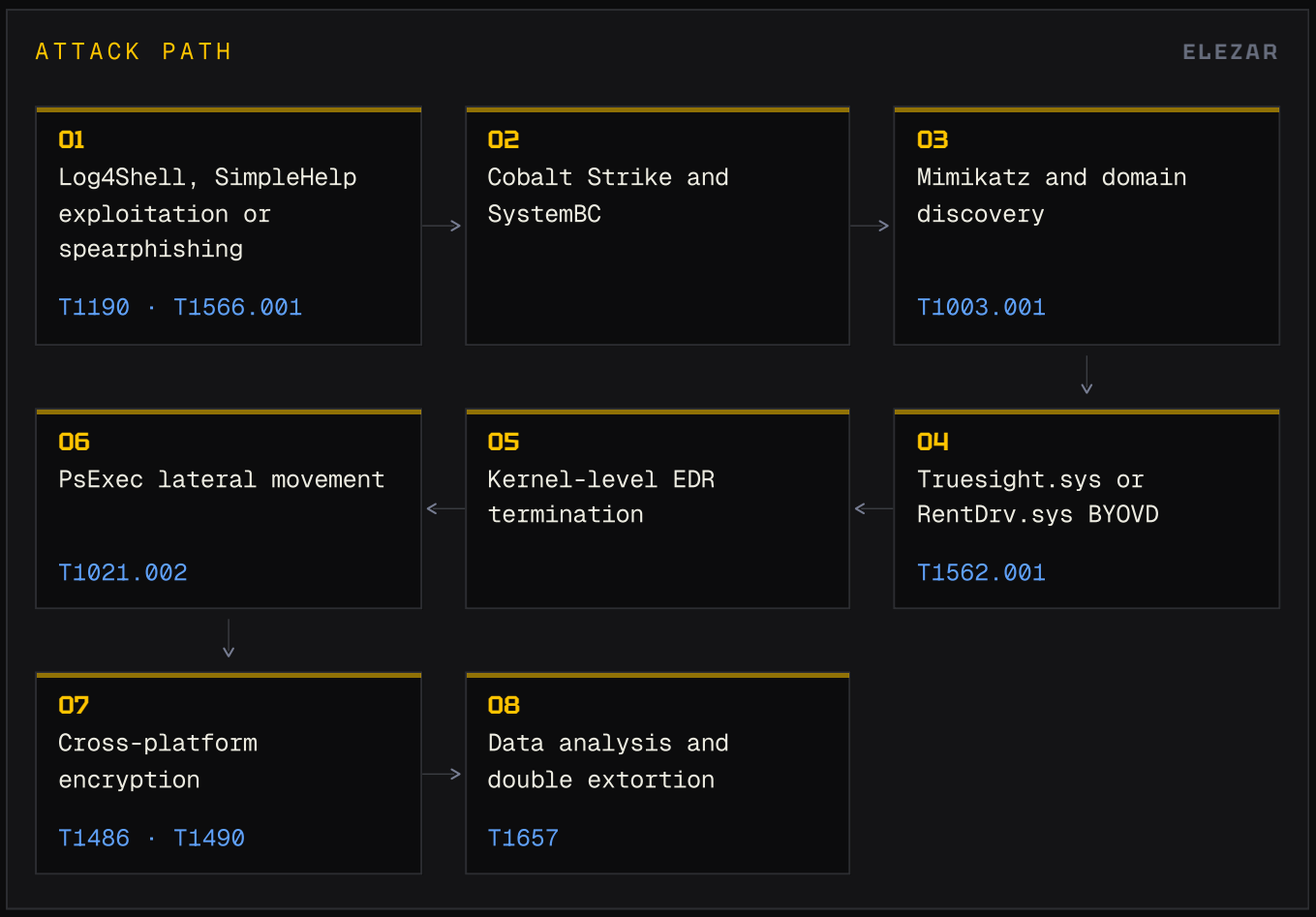
1 **June intelligence volume rose from 164 to 455 reports**, a 177 percent increase.

2	**BYOVD became a standard high-end ransomware capability** through DragonForce use of Truesight.sys and RentDrv.sys.
3	**Trusted cloud storage became a payload delivery channel** through GoldenGh0stLoader use of Google Cloud Storage and Amazon S3.
4	**IT helpdesk social engineering matured** through the 3AM email-bombing and Quick Assist chain.
5	**GPO-based browser credential harvesting appeared as a high-impact domain-wide post-exploitation technique** through Securotrop.

Attack chains, vulnerabilities and indicators

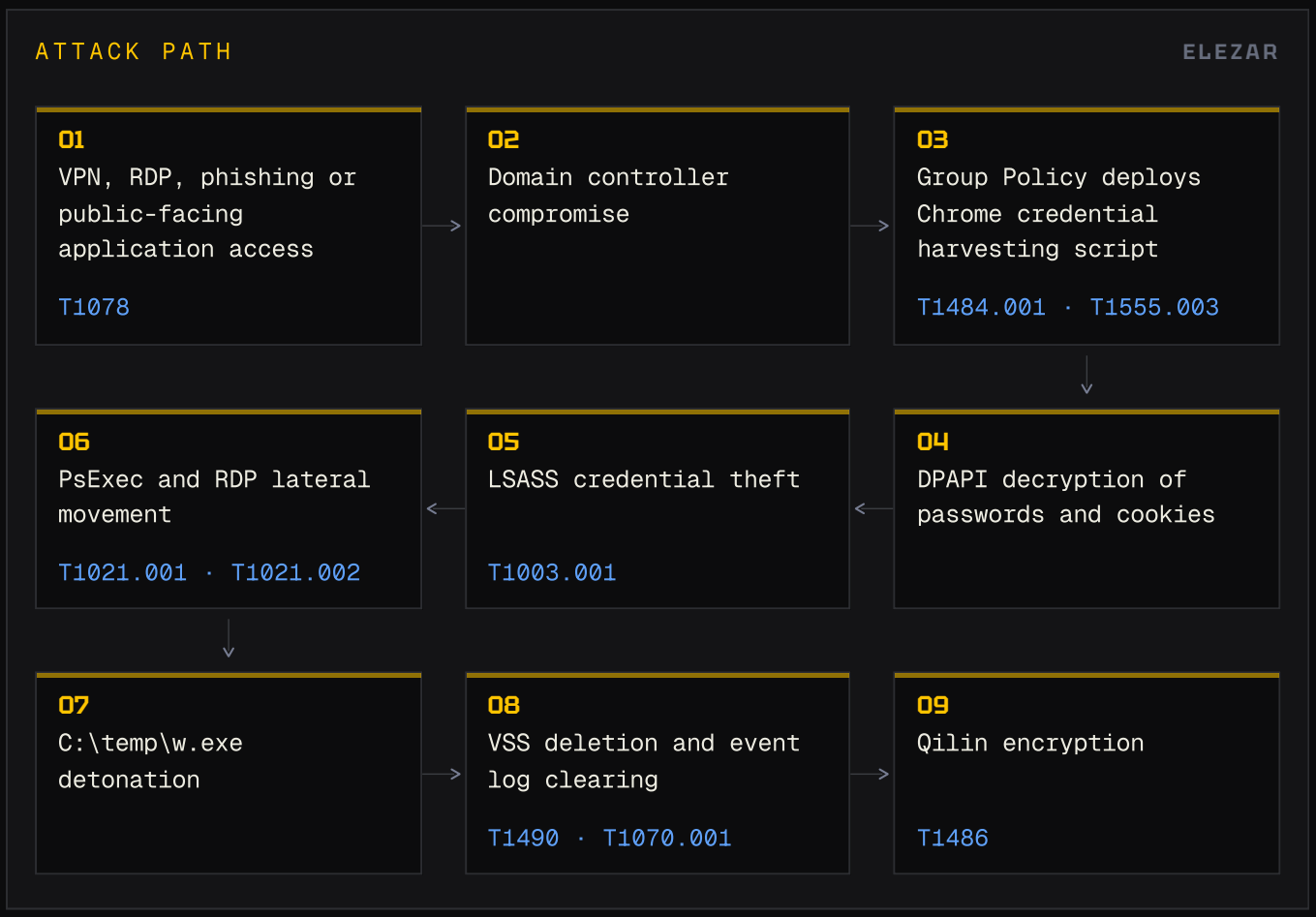
CVE	PRODUCT	IMPACT	JUNE CONTEXT
CVE-2021-44228	Apache Log4j	Remote code execution, CVSS 10.0	Actively exploited by DragonForce
CVE-2024-57726 / 57727 / 57728	SimpleHelp RMM	Authentication bypass, traversal and privilege escalation	Actively exploited by DragonForce
CVE-2026-20253	Splunk Enterprise	Unauthenticated RCE, CVSS 9.8	Risk to SIEM infrastructure
CVE-2026-0257	Palo Alto PAN-OS	Authentication bypass, CVSS 9.1	Perimeter risk

Attack Chain 1: DragonForce



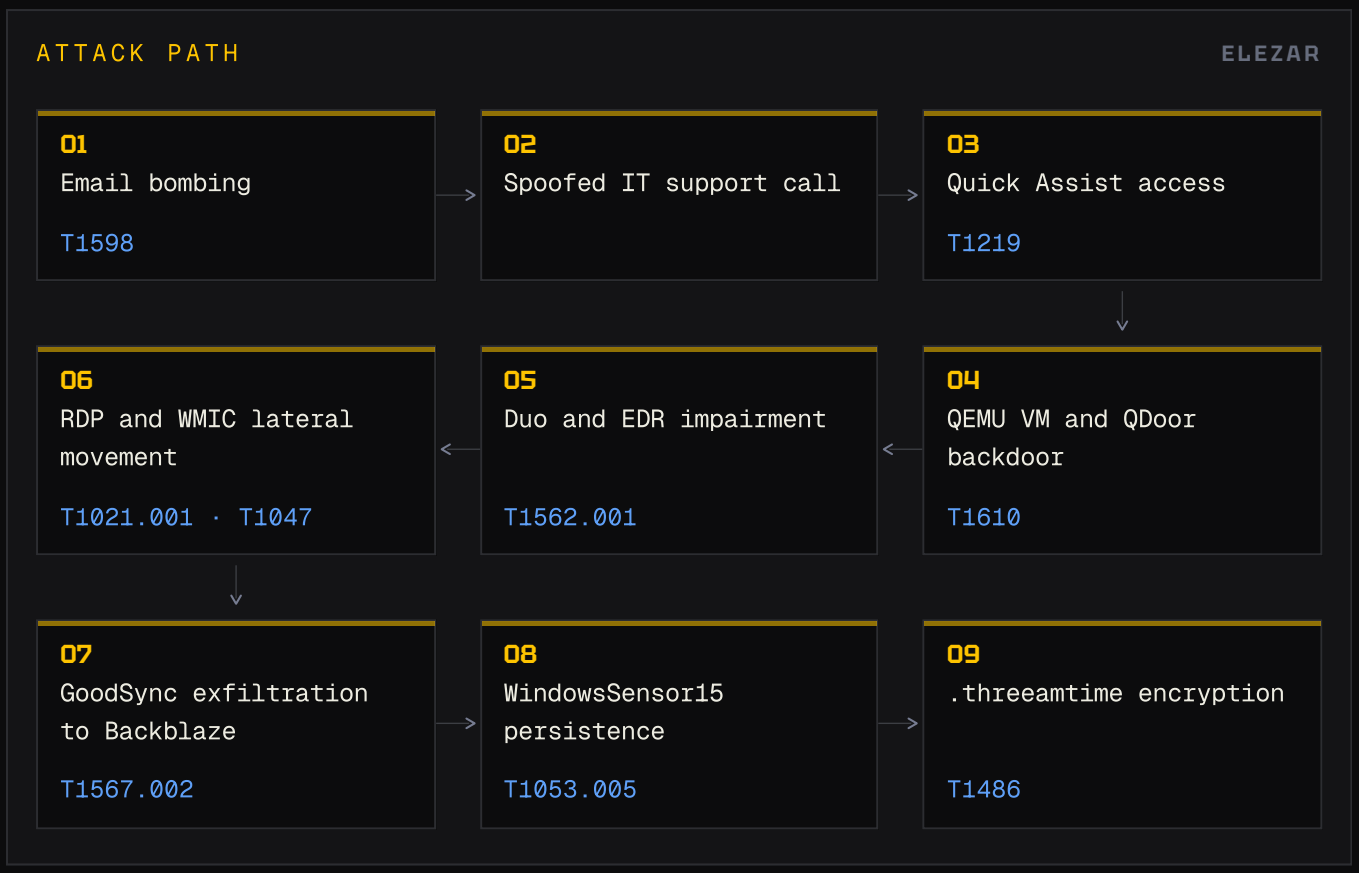
Source: Threat Intelligence Report ending 1 June 2026

Attack Chain 2: Securotrop



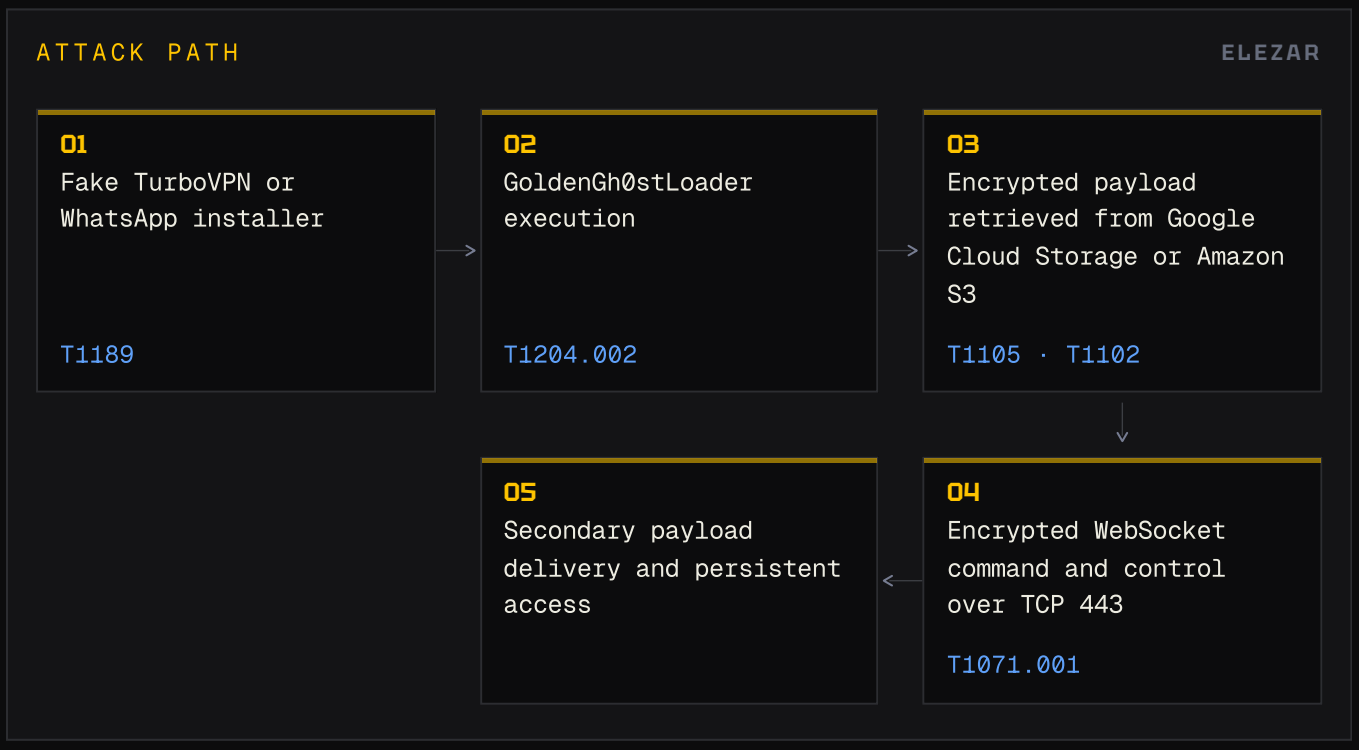
Source: Threat Intelligence Report June 2 to June 8, 2026

Attack Chain 3: 3AM ransomware



Source: Threat Intelligence Report June 9 to June 15, 2026

Attack Chain 4: GoldenGh0stLoader



Source: Threat Intelligence Report June 23 to June 29, 2026

Selected indicators

TYPE	INDICATOR	ASSOCIATION
SHA256	410db536a57c511b0ccac2639e0eb3320f303fc5c90242379ab43364c51ef321	DragonForce Truesight.sys
File	Truesight.sys / RentDrv.sys	DragonForce BYOVD drivers
File	C:\temp\w.exe	Securotrop staging
Task	WindowsSensor15	3AM persistence
File	Update_excic.acow2	3AM QEMU disk image
Process	qemu-system-* / wexe.exe	3AM EDR bypass

Prioritized defensive guidance

IMMEDIATE: ACT WITHIN 72 HOURS

1. Patch remaining Log4j exposure

Scan Java-based portals, middleware and payment systems for CVE-2021-44228 and isolate systems that cannot be patched.

2. Patch and restrict SimpleHelp

Apply fixes for CVE-2024-57726, CVE-2024-57727 and CVE-2024-57728. Restrict management access and verify MSP patch status.

3. Block vulnerable driver execution

Add Truesight.sys and RentDrv.sys to WDAC deny rules and enable the Microsoft Vulnerable Driver Blocklist.

URGENT: ACT WITHIN 1 TO 2 WEEKS

4. Detect GPO-based Chrome credential theft

Alert on Group Policy login script changes and PowerShell access to Chrome Login Data or Cookies.

5. Harden helpdesk processes

Restrict Quick Assist, implement callback verification and alert on more than 10 emails delivered to one mailbox within 60 seconds.

6. Enforce phishing-resistant MFA

Apply FIDO2, WebAuthn or certificate-based MFA to VPN, RDP and remote administration.

7. Detect trusted cloud payload delivery

Alert on WebSocket traffic and binary downloads from unapproved Google Cloud Storage and Amazon S3 buckets.

INVESTIGATE AND STRENGTHEN

8. Detect QEMU-based EDR evasion

Block or alert on qemu-system, wexe.exe and .acow2 or .qcow2 files outside approved IT use.

9. Protect immutable backups

Use offline or immutable storage that domain administrators cannot modify. Test clean recovery regularly.

10. Patch Splunk and PAN-OS

Prioritize CVE-2026-20253 and CVE-2026-0257 because compromise would remove security visibility or bypass the perimeter.

June source reports: Threat Intelligence Report ending 1 Jun 2026 · Threat Intelligence Reports for Jun 2 to 8, Jun 9 to 15, Jun 16 to 22 and Jun 23 to 29 2026

EMEA

EXECUTIVE SUMMARY

Credential theft, ransomware and regulatory extortion pressure

EMEA finance, banking and payment organizations faced a criminally driven threat environment in June 2026. The source set highlighted mass credential-stealer distribution, ransomware with GDPR and PDPL pressure tactics, and the temporary disruption of Amadey and StealC through Operation Endgame. Germany accounted for 5.15 percent of global ransomware victims during the week of 2 to 8 June. June report volume reached 455, up from 164 in May.

KEY INSIGHTS

1	**Operation Endgame** disrupted 47 domains and 182 command-and-control IPs associated with Amadey and StealC on 24 June.
2	**StealC v2** targeted Chromium and Firefox credentials, saved payment card data and Chrome App-Bound Encryption through APC injection.
3	**Brain Cipher** used double extortion and explicit GDPR notification threats against organizations exposed through RDP, VPN, phishing and initial access brokers.
4	**AiLock** introduced ChaCha20 plus NTRUEncrypt256 and laundering through Wasabi, FixedFloat and Monero.
5	**3AM ransomware** combined email bombing, IT vishing, Quick Assist abuse, a QEMU-hosted QDoor backdoor, 868 GB exfiltration and WindowsSensor15 persistence.
6	**RevStealer** used Polygon blockchain state to retrieve command-and-control configuration, reducing the value of static domain and IP blocklists.

Top threat entities and June trend shifts

- **Amadey and StealC** MAAS ECOSYSTEM

Mass browser credential theft, CVV2 harvesting, clipboard theft and downstream ransomware enablement. Operation Endgame reduced infrastructure but did not remove the source code or operator capability.

- **Brain Cipher** RANSOMWARE

LockBit 3.0-derived ransomware using exposed remote access, credential dumping, GPO deployment, service stopping and GDPR notification pressure.

- **AiLock** RANSOMWARE

New RaaS with post-quantum key encapsulation, operator-controlled detonation and cryptocurrency laundering designed to resist tracing.

- **3AM ransomware** SOCIAL ENGINEERING

Email bombing followed by spoofed IT support calls and Quick Assist. QDoor operated inside QEMU to evade host EDR.

- **RevStealer** INFOSTEALER

Credential and cryptocurrency wallet theft with EtherHiding-based C2 resolution through Polygon smart contract data.

- **FortiBleed** CREDENTIAL STUFFING

Used 110 million credentials against 430,000 FortiGate devices, creating a direct perimeter risk for financial institutions.

Trend shifts versus May 2026

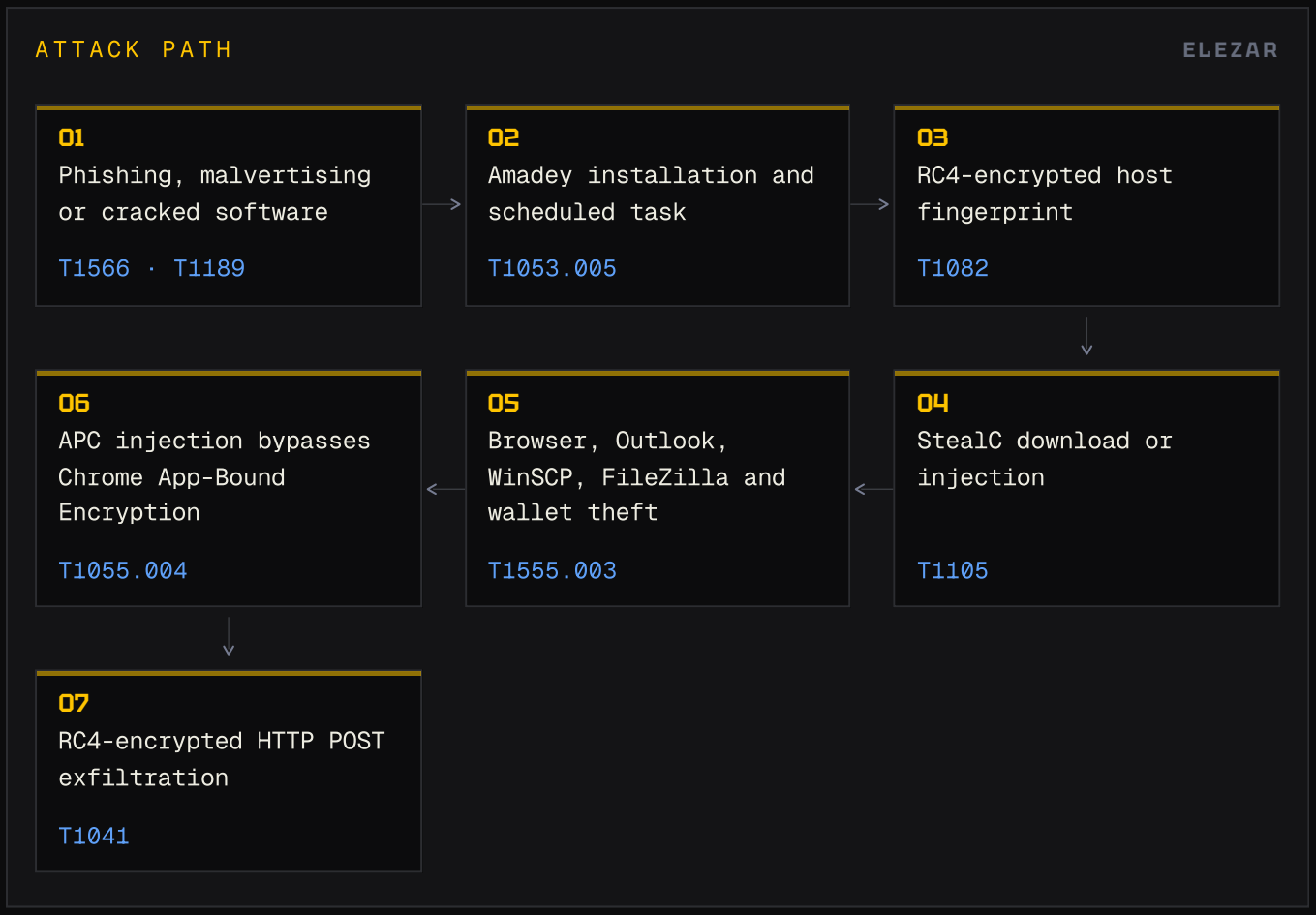
1 **MaaS disruption did not equal displacement**. StealC source code had already been sold and operators were expected to rebuild.

2	**Regulatory notification became an extortion lever** through GDPR and PDPL threats and time pressure.
3	**Blockchain-based command and control emerged** through RevStealer EtherHiding.
4	**QEMU-based EDR bypass expanded beyond one actor**, indicating broader adoption.
5	**Post-quantum ransomware encryption appeared in the tracked dataset** through AiLock.

Attack chains, vulnerabilities and indicators

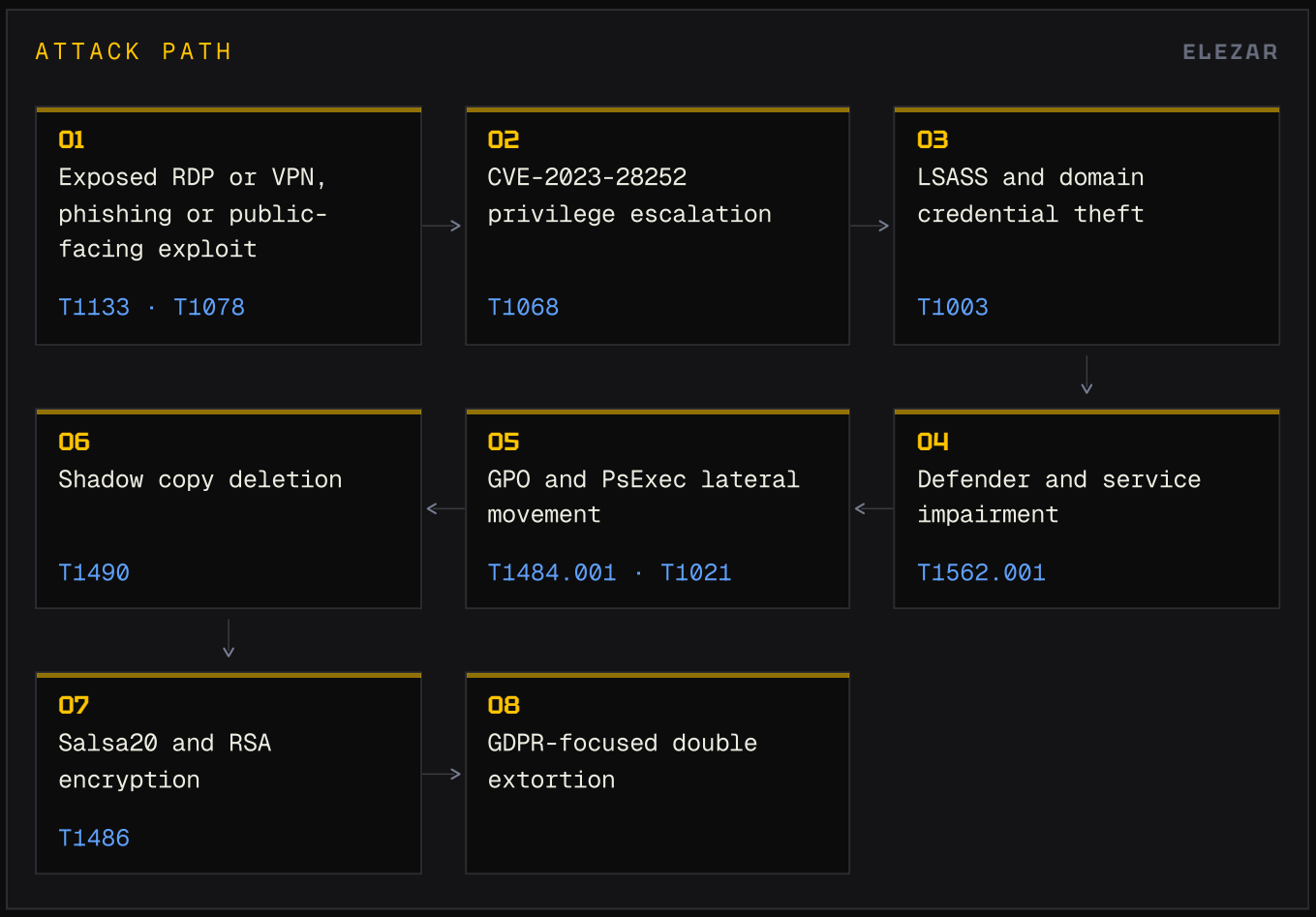
CVE	PRODUCT	IMPACT	JUNE CONTEXT
CVE-2023-28252	Windows CLFS driver	Privilege escalation	Actively used by Brain Cipher
CVE-2026-20253	Splunk Enterprise	Unauthenticated RCE, CVSS 9.8	Risk to SIEM infrastructure
CVE-2026-0257	Palo Alto PAN-OS	Authentication bypass, CVSS 9.1	Risk to network perimeter
CVE-2026-48907	Joomla Widget Factory	RCE, CVSS 9.8	Customer-facing portal risk
CVE-2026-35273	Oracle PeopleSoft	Zero-day RCE, CVSS 9.8	Enterprise HR and finance risk

Attack Chain 1: Amadey to StealC



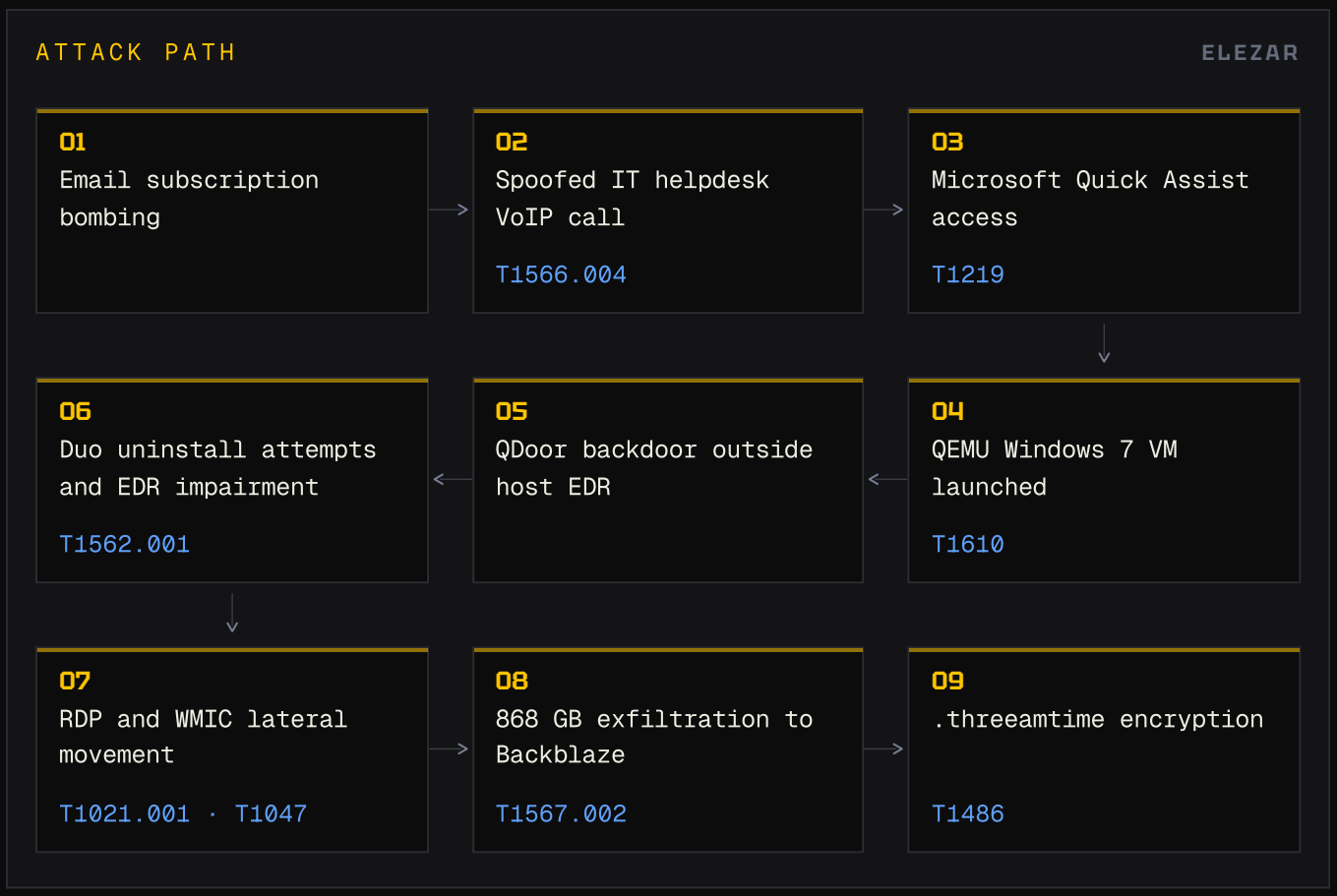
Source: Amadey and StealC: Malware-as-a-Service Unavailable; StealC and Amadey technical analysis

Attack Chain 2: Brain Cipher



Source: Threat Intelligence Report June 16 to June 22, 2026

Attack Chain 3: 3AM ransomware



Source: Threat Intelligence Report June 9 to June 15, 2026

Selected indicators

TYPE	INDICATOR	ASSOCIATION
IP	185[.]215[.]113[.]206	Amadey and StealC C2
IP	185[.]215[.]113[.]17	Amadey and StealC C2
IP	62[.]204[.]41[.]151	Shared C2 infrastructure
File	C:\Users\<user>\e079729711\nudwee.exe	Amadey persistence
IP	88[.]118[.]167[.]239:443	3AM QDoor C2
Task	WindowsSensor15	3AM persistence

Prioritized defensive guidance

IMMEDIATE: ACT WITHIN 72 HOURS

1. Block and hunt Amadey and StealC infrastructure

Block 185[.]215[.]113[.]206, 185[.]215[.]113[.]17 and 62[.]204[.]41[.]151. Hunt for nudwee.exe in user and temporary paths.

2. Detect the StealC APC injection sequence

Alert on CREATE_SUSPENDED followed by VirtualAllocEx, WriteProcessMemory, QueueUserAPC and ResumeThread from non-browser processes.

3. Patch CVE-2023-28252 and CVE-2026-20253

Prioritize Windows hosts and Splunk systems connected to financial operations.

URGENT: ACT WITHIN 1 TO 2 WEEKS

4. Harden IT support against Quick Assist abuse

Restrict Quick Assist, require out-of-band callback verification and alert on sudden mailbox flooding.

5. Detect QEMU and rogue VM execution

Alert on qemu-system processes, wexe.exe and .acow2 or .qcow2 images in C:\ProgramData.

6. Enforce phishing-resistant MFA on RDP and VPN

Use FIDO2 or certificate-based authentication for remote administration.

7. Prepare a GDPR and DORA double-extortion playbook

Pre-approve legal, compliance and incident reporting decision paths before an active ransomware event.

INVESTIGATE AND STRENGTHEN

8. Monitor blockchain RPC use

Alert on Polygon RPC traffic from non-trading systems and scripts decoding blockchain-sourced payloads.

9. Protect Outlook and WinSCP credentials

Restrict registry access to Outlook profile and WinSCP session paths from unapproved processes.

10. Rotate and harden FortiGate administration

Remove internet-exposed management, enforce certificates and rotate administrative credentials in response to FortiBleed.

June source reports: Amadey and StealC: Malware-as-a-Service Unavailable · StealC and Amadey technical analysis · Threat Intelligence Reports for Jun 2 to 8, Jun 9 to 15, Jun 16 to 22 and Jun 23 to 29 2026

APAC

EXECUTIVE SUMMARY

Localized phishing, supply chain compromise and cryptocurrency targeting

The APAC finance, banking and payment sector faced elevated multi-vector activity throughout June 2026. Chinese-speaking cybercrime and espionage operations targeted East and Southeast Asian financial institutions, payroll systems and tax-processing environments. North Korean-linked operators also targeted cryptocurrency and fintech development ecosystems through supply chain compromise and developer recruitment lures. June intelligence volume rose to 455 reports from 164 in May, while adversaries increased the use of localized Japanese, Hindi and Chinese pretexts.

KEY INSIGHTS

1	**TA4922** was the most operationally active Chinese-speaking actor in the source set, expanding tax, payroll and HR-themed phishing into Japan and Taiwan.
2	**Sapphire Sleet**, also tracked as BlueNoroff or UNC1069, compromised more than 140 npm packages and enumerated 166 cryptocurrency wallet browser extensions.
3	**Operation TaxShadow** impersonated Indian and Japanese tax authorities to deliver an obfuscated in-memory malware framework. Attribution to Chinese-speaking operators was assessed at moderate confidence.
4	**UNK_DeadDrop** targeted finance and cryptocurrency developers and quantitative analysts with recruitment lures, including impersonation of Ondo Finance.
5	No named APAC financial entity ransomware incident was confirmed in the ingested June reports. The period was instead dominated by phishing, credential theft, developer targeting and supply chain activity.

Top threat entities and June trend shifts

- **TA4922** CYBERCRIME

Japan and Taiwan tax, payroll and HR phishing. Uses RomulusLoader, Atlas RAT, SilentRunLoader, AnyDesk and SyncFuture. Atlas RAT injects into WeChat.exe and supports keylogging, screen capture, webcam and audio collection.

- **Sapphire Sleet** STATE-LINKED

Weaponized the **easy-day-js** npm dependency through compromised Mastra packages. The campaign targeted developer systems and cryptocurrency wallet extensions across Windows, macOS and Linux.

- **UNK_DeadDrop** DEVELOPER TARGETING

Used recruitment and repository lures against financial developers and quantitative analysts. Delivered the Overlord Go RAT and targeted cryptocurrency theft.

- **Operation TaxShadow** PHISHING CAMPAIGN

Used India and Japan tax authority impersonation, DLL search order hijacking, reflective loading and proxy-aware WebSocket command and control.

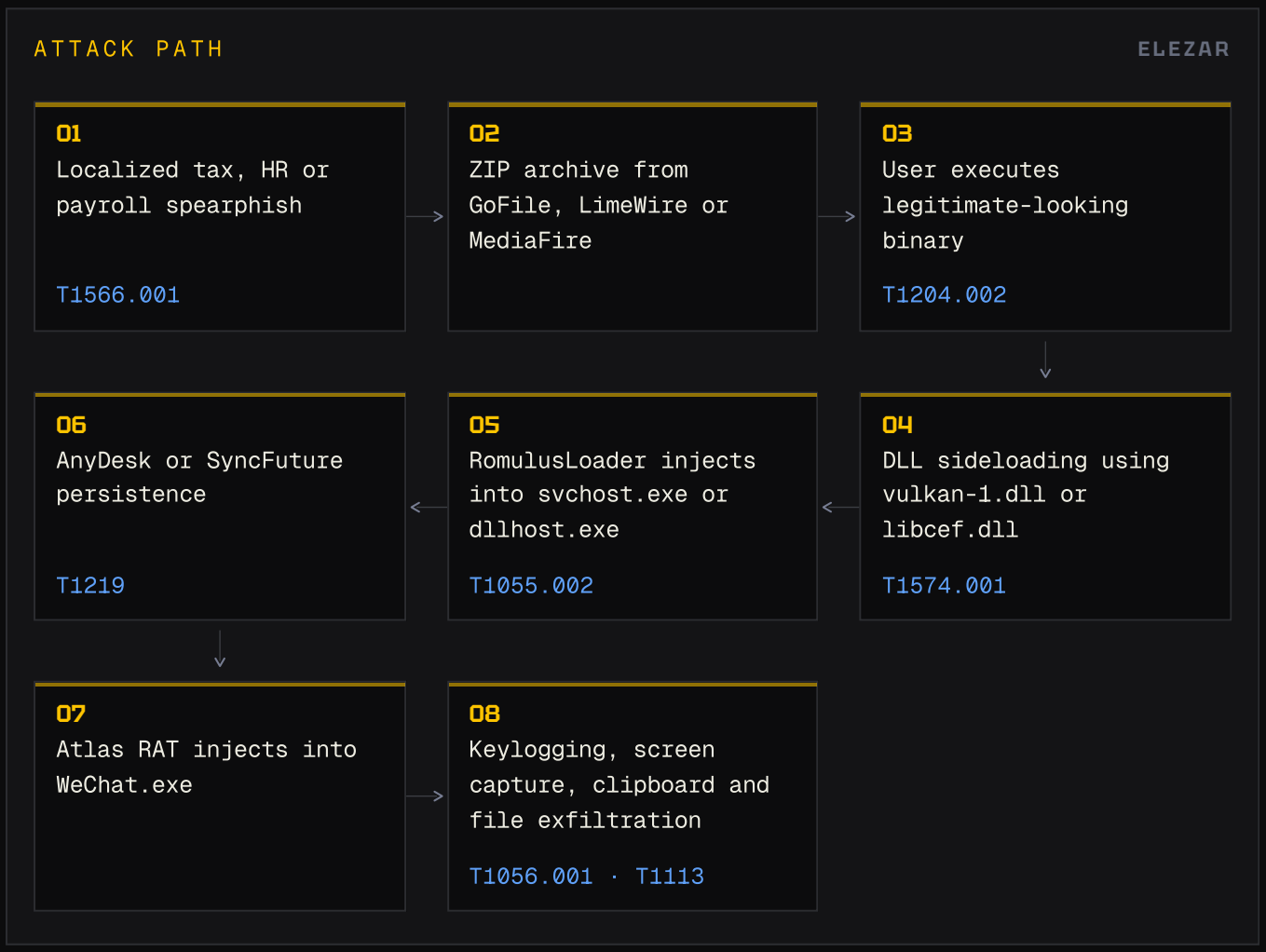
Trend shifts versus May 2026

1	**Report volume increased 177 percent**, from 164 reports in May to 455 in June.
2	**Localized lure quality improved**, including Japanese salary adjustment archives and Hindi tax-themed executables.
3	**Developer and supply chain vectors gained prominence** through the Sapphire Sleet npm compromise and UNK_DeadDrop recruitment operations.
4	**LLM-assisted development and localization appeared in the source set**, particularly around SilentRunLoader and TA4922 campaign production.

Attack chains, vulnerabilities and indicators

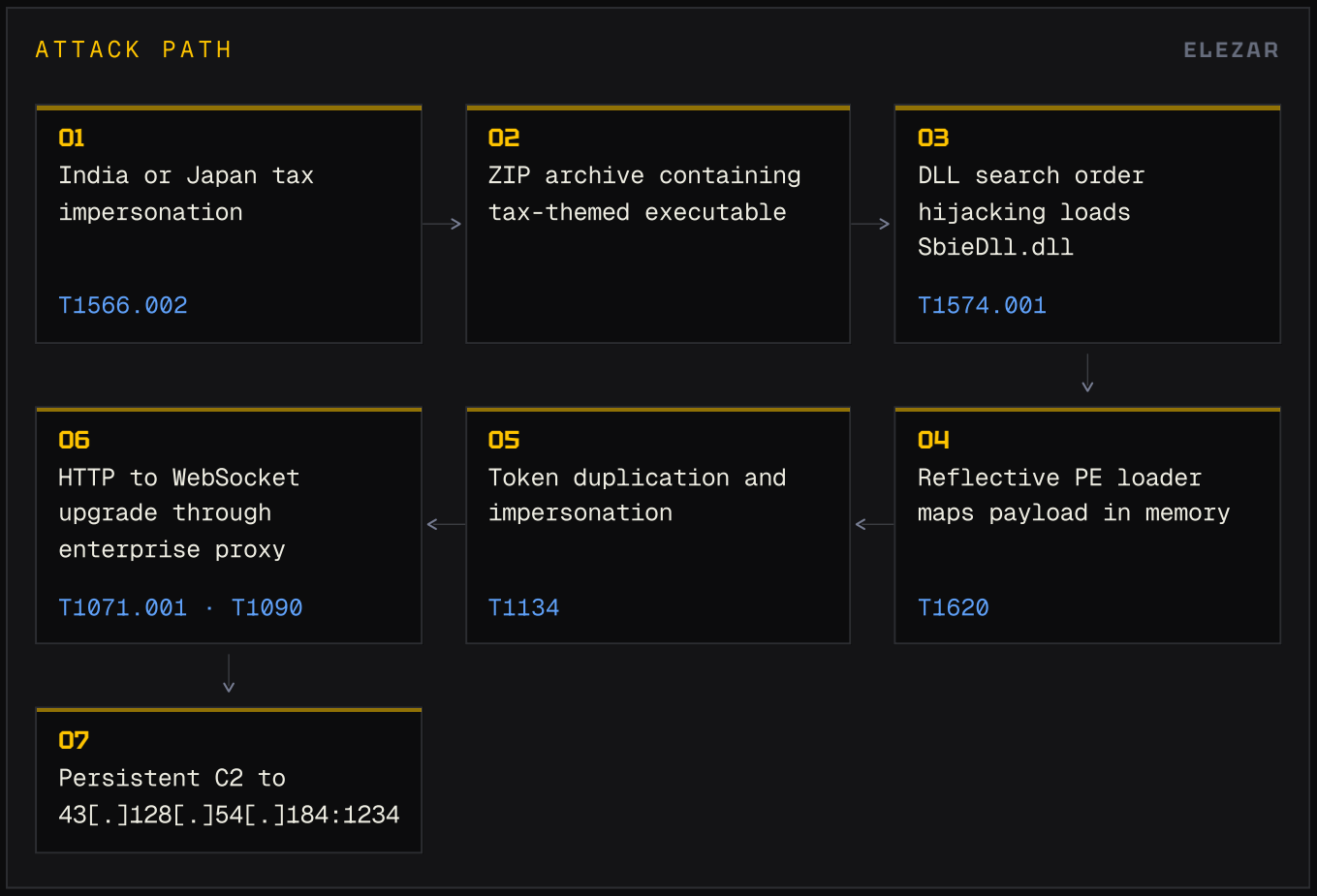
CVE	PRODUCT	IMPACT	JUNE RELEVANCE
CVE-2026-20245	Cisco Catalyst SD-WAN Manager	Root-level backdoor	Emergency patch priority for financial network infrastructure
CVE-2026-20253	Splunk Enterprise	Unauthenticated RCE, CVSS 9.8	Direct risk to SIEM infrastructure
CVE-2026-0257	Palo Alto PAN-OS	Authentication bypass, CVSS 9.1	Direct risk to perimeter access

Attack Chain 1: TA4922 localized phishing to Atlas RAT



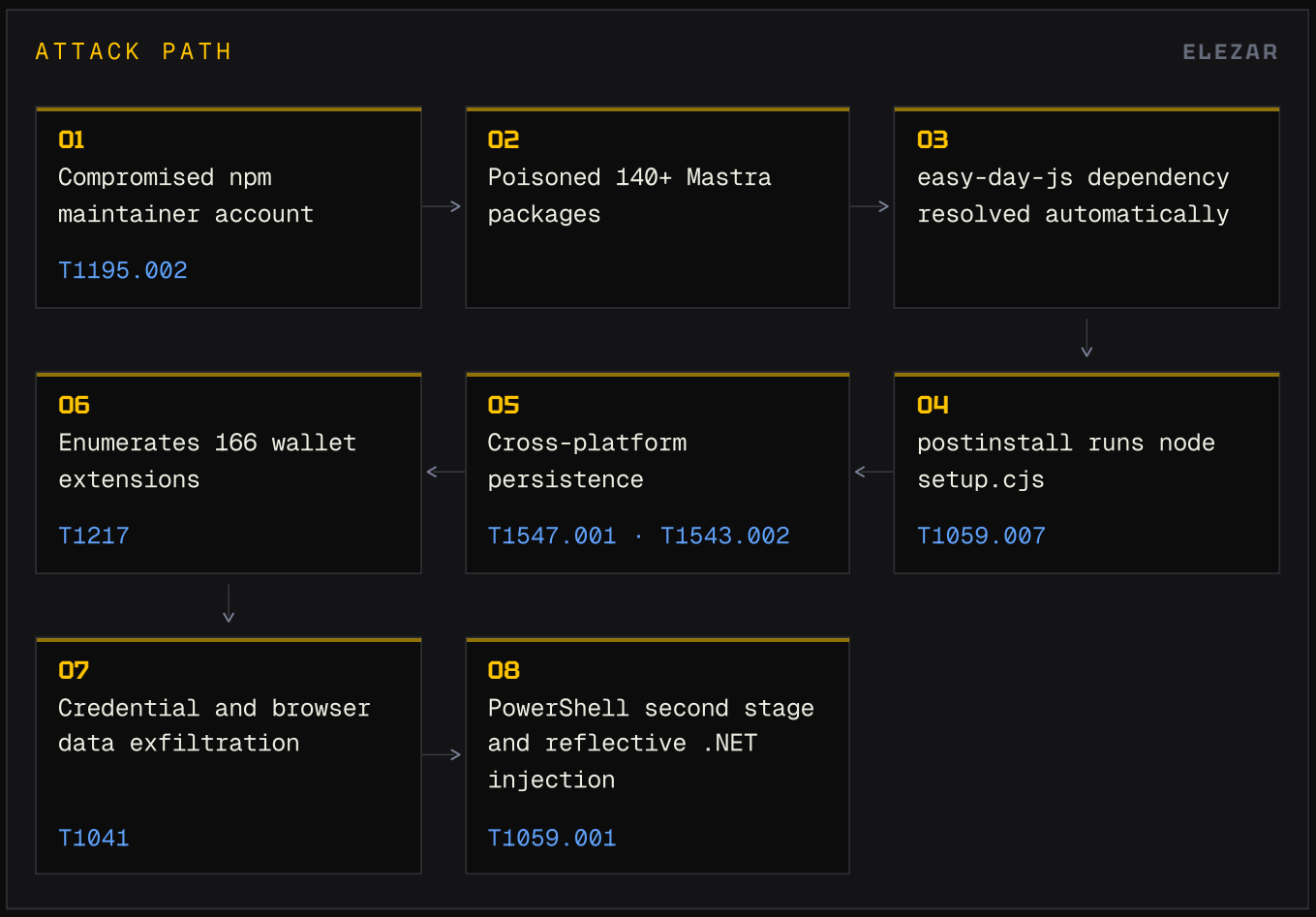
Source: TA4922: The Suspected Chinese Crime Group is Going Global

Attack Chain 2: Operation TaxShadow



Source: Operation TaxShadow: Multi-Region Tax Phishing and In-Memory Malware Campaign

Attack Chain 3: Sapphire Sleet npm supply chain



Source: From package to postinstall payload: Inside the Mastra npm supply chain compromise by Sapphire Sleet

Selected indicators

TYPE	INDICATOR	ASSOCIATION
IP	43[.]128[.]54[.]184:1234	TaxShadow C2
IP	206[.]238[.]115[.]58	Atlas RAT C2
IP	154[.]211[.]86[.]110	Atlas RAT C2
IP	23[.]254[.]164[.]92	Sapphire Sleet stage two
Domain	teams[.]onweblive[.]org	Sapphire Sleet PowerShell C2
Domain	ws[.]ztts88[.]cyou	SilentRunLoader C2 and exfiltration
Registry	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\NvmProtocal	Sapphire Sleet persistence

Prioritized defensive guidance

IMMEDIATE: ACT WITHIN 72 HOURS

1. Block confirmed June C2 infrastructure

Add 43[.]128[.]54[.]184, 23[.]254[.]164[.]92, teams[.]onweblive[.]org, ws[.]ztts88[.]cyou and related indicators to perimeter blocklists and SIEM watchlists.

2. Audit npm and CI/CD integrity

Search package-lock files and SBOMs for easy-day-js versions 1.11.21 and later. Hunt for the NvmProtocal Run key and com.nvm.protocal.plist.

3. Hunt Atlas RAT execution patterns

Alert on user-space processes spawning svchost.exe or dllhost.exe, non-system loading of vulkan-1.dll or libcef.dll, outbound TCP 886 and injection into WeChat.exe.

URGENT: ACT WITHIN 1 TO 2 WEEKS

4. Control RMM use

Allowlist approved RMM tools and alert on AnyDesk or SyncFuture installs without a valid service ticket.

5. Tune phishing controls for localized lures

Flag Japanese salary or tax ZIP attachments, Hindi tax impersonation and links to GoFile, LimeWire, MediaFire and srt.tw.

6. Protect browser sessions

Use phishing-resistant MFA and managed browser profiles. Hunt for Chrome_Live_Backup_*.zip and C:\WSBF_ALL.

7. Patch June-exploited infrastructure

Prioritize CVE-2026-20245, CVE-2026-20253 and CVE-2026-0257.

INVESTIGATE AND TUNE DETECTIONS

8. Validate fileless malware coverage

Confirm behavioral detection for reflective assembly loading, unusual ZwAllocateVirtualMemory use and unexpected WebSocket upgrades.

9. Review proxy-aware C2 visibility

Alert on HTTP 101 Switching Protocols responses to unapproved destinations and inspect HTTP CONNECT tunnelling.

10. Treat developer workstations as privileged assets

Apply least privilege to CI/CD credentials, audit package installation events and monitor VS Code or Cursor extension installation.

June source reports: TA4922: The Suspected Chinese Crime Group is Going Global · From package to postinstall payload: Inside the Mastra npm supply chain compromise by Sapphire Sleet · Operation TaxShadow: Multi-Region Tax Phishing and In-Memory Malware Campaign · Don’t Fear the Repo: UNK_DeadDrop Phishing Campaign Targets Developers to Steal Cryptocurrency · Threat Intelligence Report Jun 2 to Jun 8 2026