SOL THREAT INTELLIGENCE

June 2026 Energy, Gas, Oil and Utilities Regional Sector Brief

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

AMERICAS

EXECUTIVE SUMMARY

VOLTZITE pre-positioning and FortiBleed compound the world's highest ransomware exposure

The Americas, led by the United States, carried the highest ransomware burden in every June reporting week. The United States accounted for 32.10 to 45.59 percent of global ransomware victims, while Canada reached 7.35 percent in the week of 2 to 8 June. Energy and utilities also faced a distinct nation-state threat through VOLTZITE pre-positioning against electric and water infrastructure, plus FortiBleed, a Russian-speaking initial-access campaign that compromised more than 430,000 FortiGate devices and captured over 110 million credentials. No source report named a specific Americas energy victim, so the brief separates region-wide exposure from confirmed sector targeting.

KEY INSIGHTS

1	VOLTZITE was confirmed conducting slow, low-noise reconnaissance and pre-positioning against US electric, water and utility infrastructure.
2	FortiBleed affected more than 430,000 FortiGate devices, with 10.1 percent of compromised devices located in the United States.
3	The United States represented between 32.10 and 45.59 percent of all global ransomware victims across June reporting weeks.
4	DragonForce explicitly targeted organizations above USD 15 million revenue and used SimpleHelp exploitation plus BYOVD EDR termination.
5	The 3AM chain used email flooding, IT-helpdesk vishing, Quick Assist, a QEMU-hosted backdoor and 868 GB of pre-encryption exfiltration.

6	Operation Endgame disrupted Amadey and StealC, but already-stolen remote-access and browser credentials remained available to access brokers.

Top threat entities and June trend shifts

- **VOLTZITE / Volt Typhoon** NATION-STATE

Confirmed pre-positioning against electric, water and utility systems through edge-device exploitation, valid accounts and living-off-the-land execution.

- **FortiBleed operator** INITIAL ACCESS BROKER

Mass FortiGate compromise, passive authentication capture and distributed cracking infrastructure with a major US victim share.

- **DragonForce** RANSOMWARE

Revenue-based targeting, MSP exploitation, cross-platform encryption and BYOVD EDR termination.

- **3AM Ransomware** RANSOMWARE

Helpdesk social engineering, Quick Assist abuse, QEMU-based EDR evasion and extended pre-encryption dwell.

- **Securotrop / Qilin** RANSOMWARE

GPO-based Chrome credential collection and domain-wide propagation.

- **Amadey / StealC** INFOSTEALER ECOSYSTEM

Credential harvesting for VPN, browser, Outlook, WinSCP and crypto environments.

Trend shifts versus May 2026

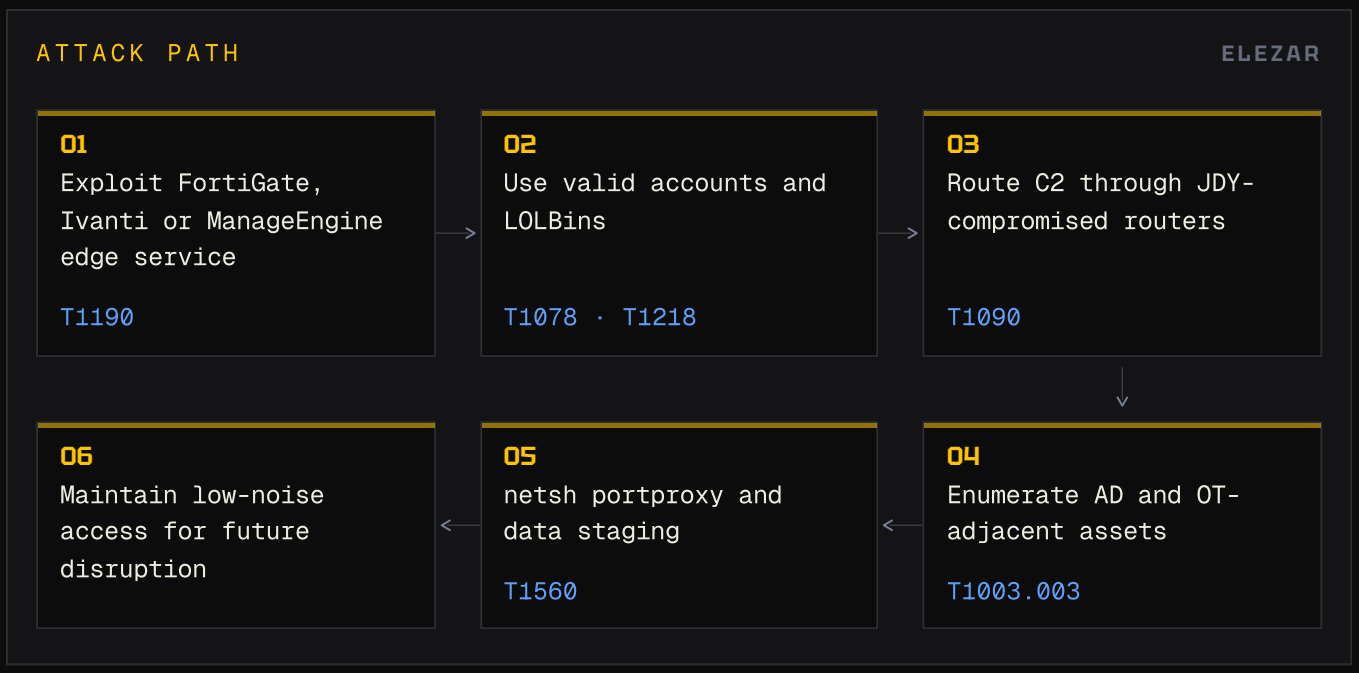
1	US ransomware concentration remained globally dominant throughout the month.

2	Nation-state pre-positioning against electric and utility infrastructure was directly documented.
3	FortiBleed introduced mass passive credential capture from FortiGate devices without installing conventional malware.
4	QEMU-based EDR evasion appeared as a practical ransomware technique.
5	Post-disruption credential exposure persisted because stolen logs were already available in criminal markets.

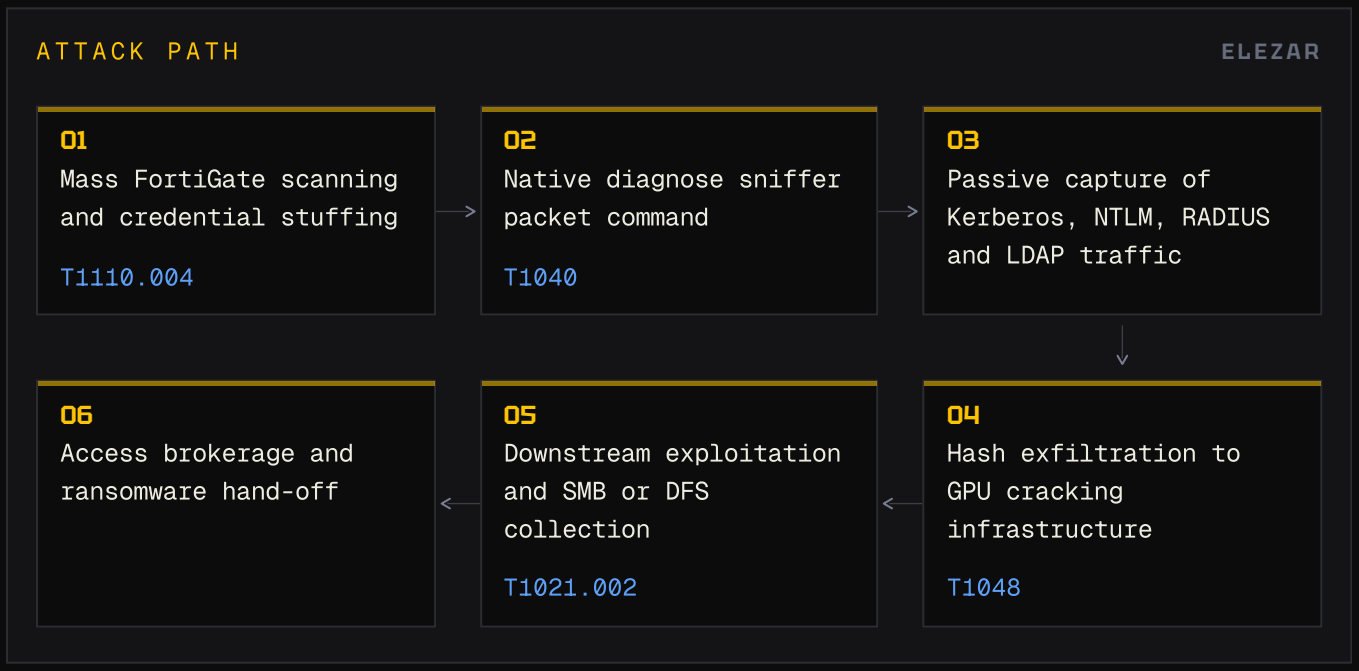
Attack chains, vulnerabilities and indicators

CVE	PRODUCT	CVSS	JUNE CONTEXT
CVE-2026-0257	Palo Alto PAN-OS	9.1	Widely deployed perimeter technology
CVE-2026-20253	Splunk Enterprise	9.8	SIEM and monitoring risk
CVE-2024-57726/27/28	SimpleHelp RMM	High	MSP and remote substation support
CVE-2023-28252	Windows CLFS	High	Ransomware privilege escalation
CVE-2023-46805 / CVE-2024-21887	Ivanti Connect Secure	Critical	Remote-access exploitation
CVE-2022-42475	FortiGate SSL VPN	Critical	VOLTZITE edge access and FortiGate exposure
CVE-2021-44228	Apache Log4j	10.0	Persistent public-application risk

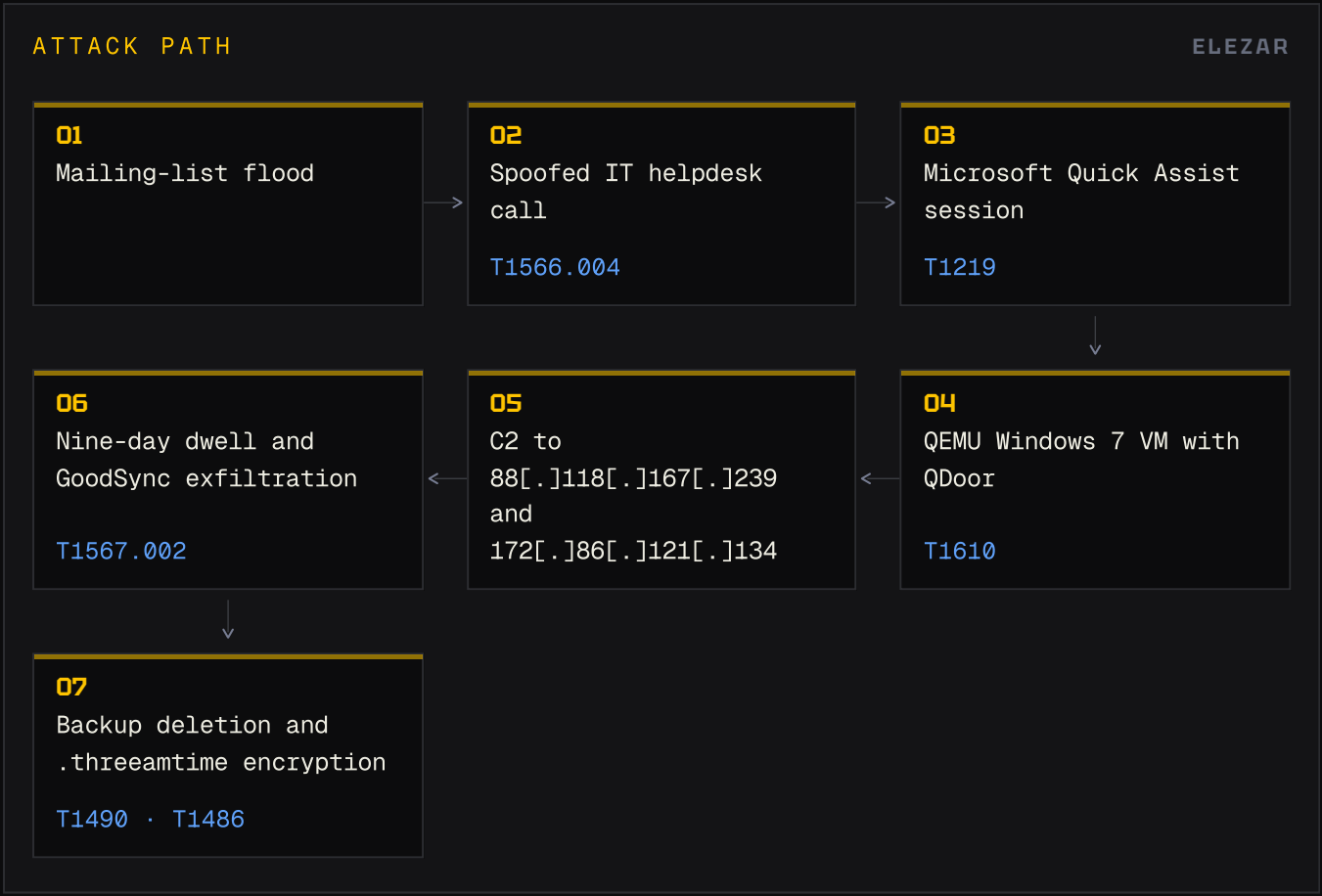
VOLTZITE OT pre-positioning



FortiBleed credential harvesting



3AM helpdesk compromise



Selected indicators

TYPE	INDICATOR	ATTRIBUTION
IP	149[.]248[.]3[.]38:13339	VOLTZITE / JDY
Process	auditdy	JDY botnet
IP	88[.]118[.]167[.]239:443 / 172[.]86[.]121[.]134	3AM QDoor
Task	WindowsSensor15	3AM persistence
Driver	Truesight.sys / RentDrv.sys	DragonForce
IP	185[.]215[.]113[.]206 / 185[.]215[.]113[.]17 / 62[.]204[.]41[.]151	Amadey / StealC
Command	wbadmin.exe delete systemstatebackup -keepVersions:0 -quiet	3AM backup destruction

Prioritized defensive guidance

Recommendations are calibrated for distributed utility operations, OT and ICS estates, remote-access infrastructure, MSP dependencies and high-impact service continuity requirements.

IMMEDIATE: ACT WITHIN 7 DAYS

1. Treat FortiGate credentials that traversed exposed devices as potentially compromised and rotate them.
2. Patch PAN-OS and Ivanti gateways or isolate them behind allowlisted management paths.
3. Block and hunt DragonForce BYOVD drivers across Windows and OT-adjacent systems.

URGENT: ACT WITHIN 30 DAYS

1. Deploy VOLTZITE living-off-the-land hunting for netsh portproxy, csvde, certutil, 7-Zip and ntds.dit access.
2. Detect QEMU processes, ACOW2 or QCOW2 files and WindowsSensor15 scheduled tasks.
3. Patch SimpleHelp and review all MSP sessions into substations and OT-support networks.
4. Rotate VPN, WinSCP and browser-stored credentials exposed through infostealer ecosystems.
5. Audit GPO changes and prevent domain-wide Chrome credential harvesting.

ONGOING DETECTION AND RESILIENCE

1. Maintain offline immutable backups for historians, SCADA databases and engineering files.

2. Deploy TLS certificate hunting for AsyncRAT-family C2 infrastructure.

3. Use OT NDR to identify slow reconnaissance and anomalous IT-to-OT communication.

4. Map response procedures to NERC CIP and relevant utility-sector reporting obligations.

June source reports: DomainTools and Dragos VOLTZITE reporting, Lumen JDY analysis, SOCRadar FortiBleed reporting, Red Piranha weekly reports, and Operation Endgame reporting from June 2026.

EMEA

EXECUTIVE SUMMARY

Ransomware, credential theft and RAT infrastructure dominate the sector risk

EMEA energy and utilities faced a criminally dominated threat environment in June 2026. No source report named a specific EMEA energy victim, but Europe was heavily represented in global ransomware activity, with Germany accounting for 5.15 percent of victims during the week of 2 to 8 June. The most important sector risks were LockBit-derived ransomware families, the Amadey and StealC credential ecosystem, a broad AsyncRAT family infrastructure footprint and the emergence of AiLock with post-quantum key encapsulation and GDPR-focused extortion pressure.

KEY INSIGHTS

1	Deadlock, Qilin, The Gentlemen, Brain Cipher and DragonForce maintained broad European reach through RaaS affiliate structures.
2	AiLock explicitly weaponized GDPR notification pressure and used ChaCha20 with NTRUEncrypt256.
3	Securotrop, a Qilin affiliate, deployed a GPO-based PowerShell script to steal Chrome credentials across domain-joined hosts before encryption.
4	DragonForce used SimpleHelp exploitation and BYOVD drivers, creating direct risk for energy operators dependent on MSPs.
5	Operation Endgame removed 47 domains and actioned 182 Amadey and StealC C2 IPs, but the source code and replacement infrastructure remained available.
6	Censys identified 13 live AsyncRAT descendants, including VenomRAT, DCRat and Gh0st RAT variants.

Top threat entities and June trend shifts

- **DragonForce / GOLD FLAME** RANSOMWARE

Targets organizations above USD 15 million revenue, exploits public apps and RMM, and uses kernel-level BYOVD EDR termination.

- **Brain Cipher** RANSOMWARE

Uses exposed remote access, Windows CLFS privilege escalation, domain-wide propagation and LockBit-derived encryption.

- **Securotrop / Qilin affiliate** RANSOMWARE

Harvests Chrome credentials through GPO and deploys ransomware after domain-wide credential collection.

- **AiLock** RANSOMWARE

Uses operator-controlled detonation, network-share encryption and GDPR-focused coercion.

- **Amadey / StealC** INFOSTEALER ECOSYSTEM

Provides stolen VPN, browser, Outlook and WinSCP credentials to access brokers and ransomware affiliates.

- **AsyncRAT family** RAT ECOSYSTEM

Thirteen active descendants identified through reusable TLS certificate patterns and non-standard C2 ports.

Trend shifts versus May 2026

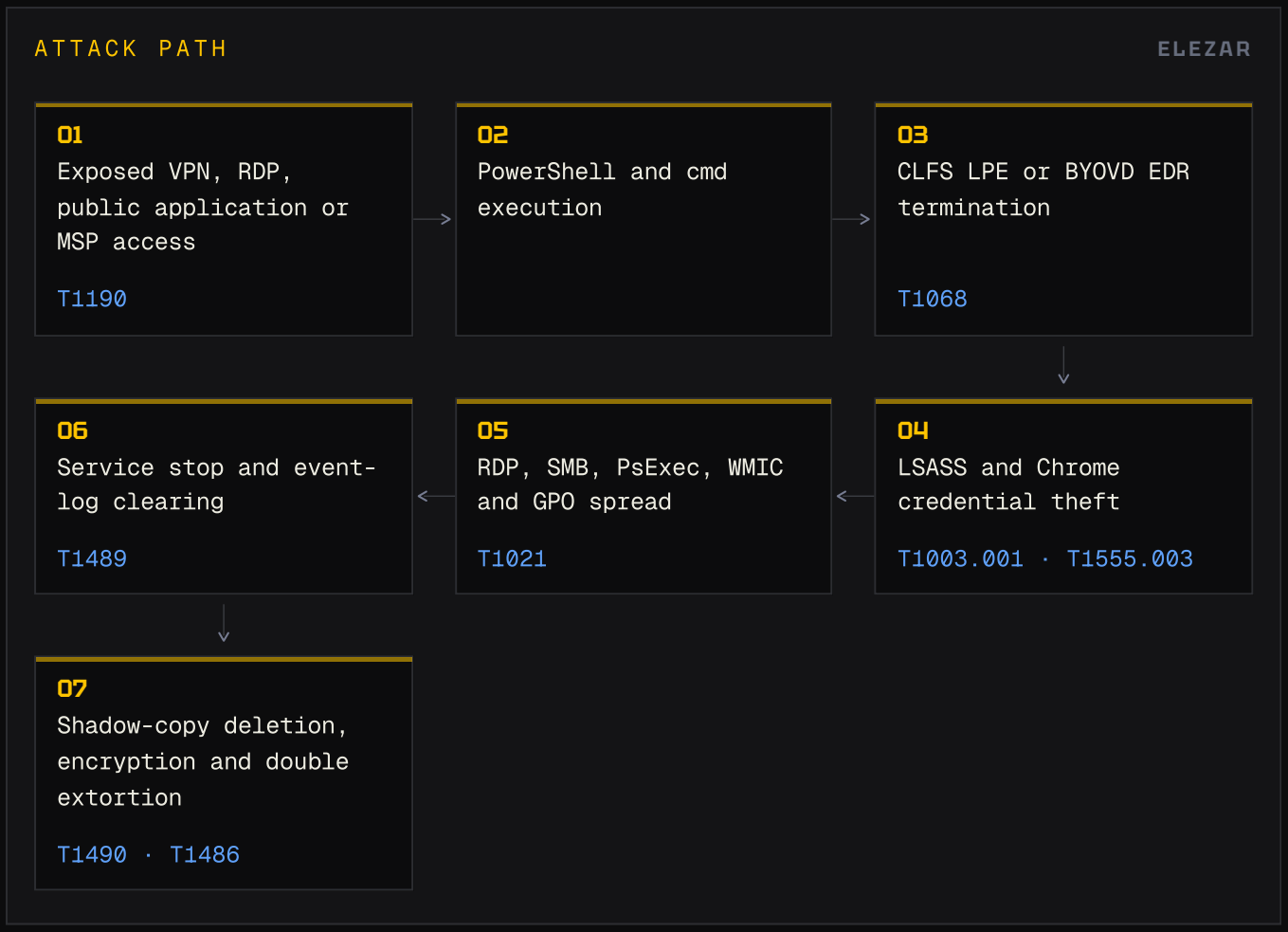
1	Germany entered the top three ransomware victim countries during June.
2	GDPR became an explicit extortion lever through AiLock.
3	GPO-based browser credential theft created a domain-wide pre-encryption collection technique.
4	Operation Endgame disrupted infrastructure but did not remove the underlying malware capability.

5 TLS certificate patterns became a practical cross-family hunting method for active RAT infrastructure.

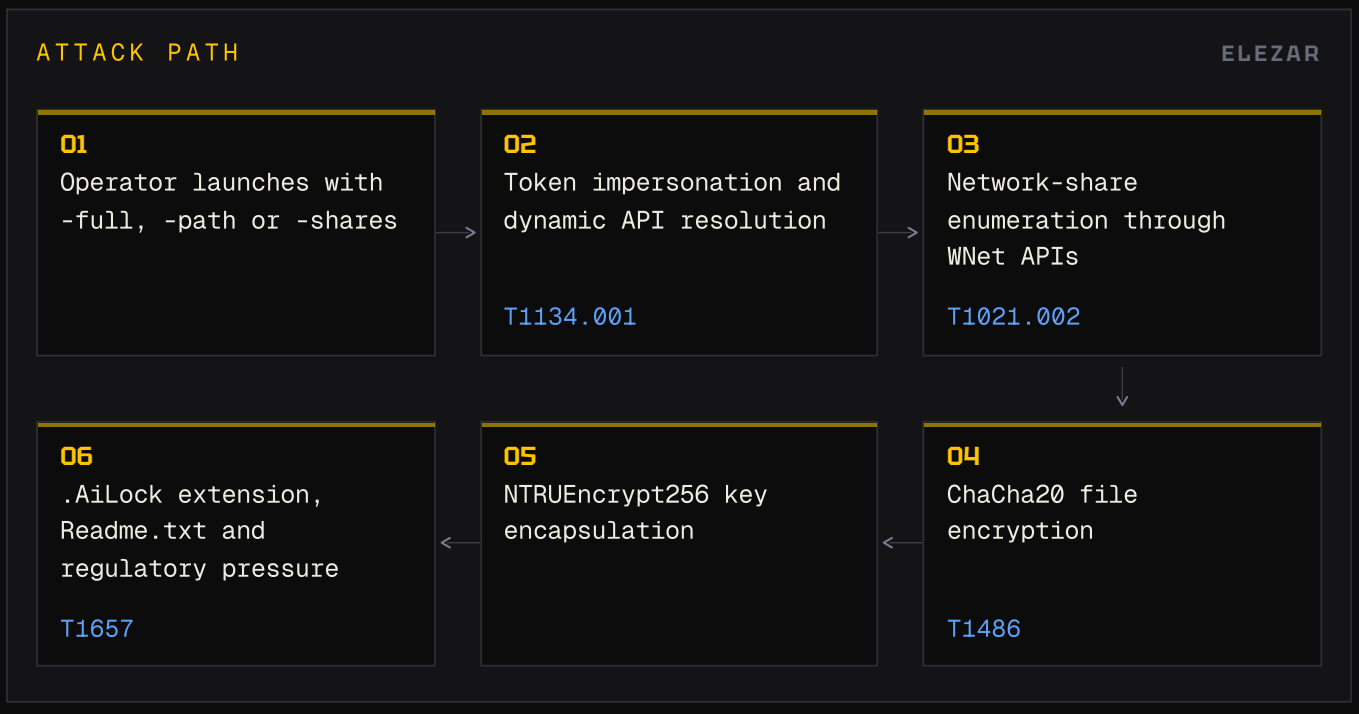
Attack chains, vulnerabilities and indicators

CVE	PRODUCT	CVSS	JUNE CONTEXT
CVE-2026-0257	Palo Alto PAN-OS	9.1	Perimeter VPN and firewall exposure
CVE-2026-20253	Splunk Enterprise	9.8	Monitoring platform compromise
CVE-2024-57726/27/28	SimpleHelp RMM	High	MSP supply-chain access
CVE-2023-28252	Windows CLFS	High	Ransomware privilege escalation
CVE-2023-46805 / CVE-2024-21887	Ivanti Connect Secure	Critical	Remote access gateway exploitation
CVE-2021-44228	Apache Log4j	10.0	Persistent initial-access vector
CVE-2025-5777	Citrix NetScaler	Critical	Session theft and remote access risk

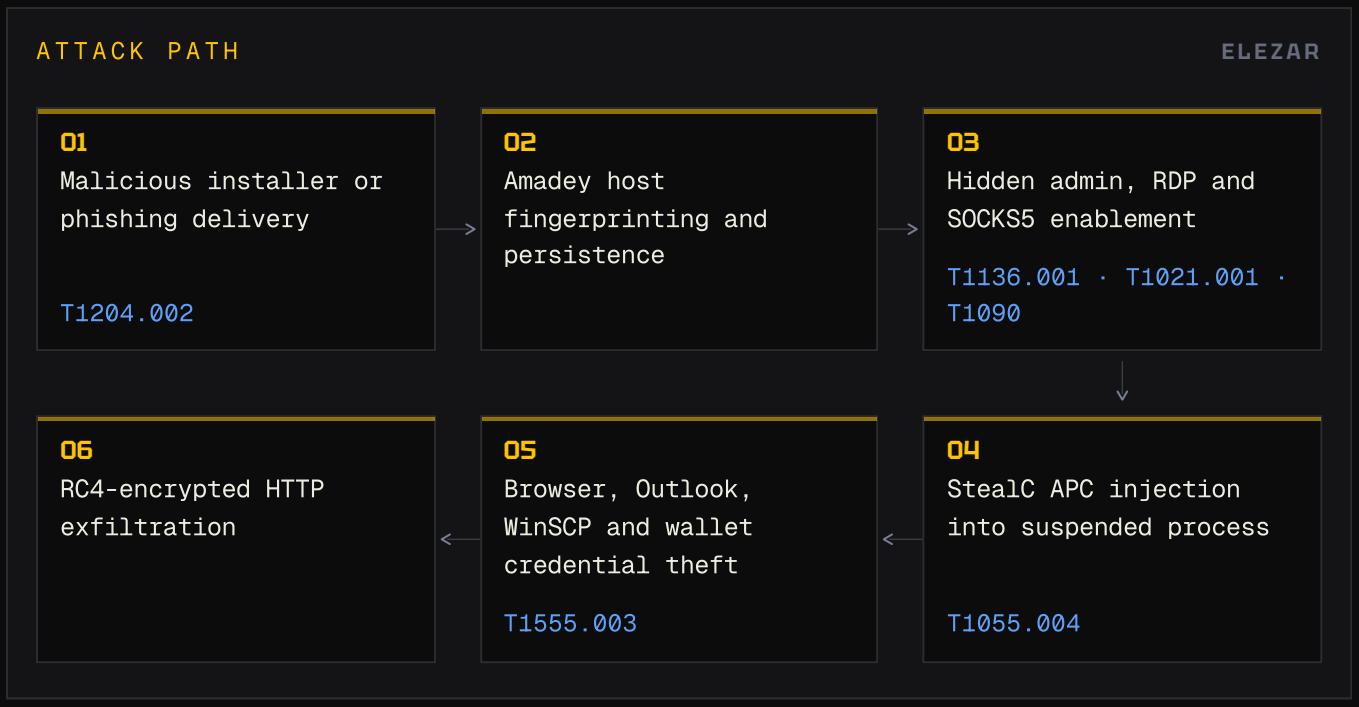
LockBit-derived ransomware



AiLock post-quantum RaaS



Amadey to StealC



Selected indicators

TYPE	INDICATOR	ATTRIBUTION
SHA256	410db536a57c511b0ccac2639e0eb3320f303fc5c90242379ab43364c51ef321	DragonForce
Driver	Truesight.sys / RentDrv.sys	DragonForce
File	C:\temp\w.exe	Securotrop staging
Mutex	FAUST	AiLock
IP	185[.]215[.]113[.]206 / 185[.]215[.]113[.]17 / 62[.]204[.]41[.]151	Amadey / StealC
IP	192[.]229[.]116[.]23 / 192[.]238[.]134[.]73 / 107[.]175[.]159[.]134	AsyncRAT family
Task	WindowsSensor15	3AM persistence

Prioritized defensive guidance

Recommendations are calibrated for distributed utility operations, OT and ICS estates, remote-access infrastructure, MSP dependencies and high-impact service continuity requirements.

IMMEDIATE: ACT WITHIN 7 DAYS

1. Patch PAN-OS and Ivanti gateways or isolate them behind trusted source restrictions.
2. Block Truesight.sys and RentDrv.sys with HVCI or WDAC and hunt Sysmon driver-load events.
3. Predefine GDPR and NIS2 incident-notification decisions before ransomware extortion occurs.

URGENT: ACT WITHIN 30 DAYS

1. Audit GPO modifications and disable Chrome password storage on OT-adjacent workstations.
2. Patch SimpleHelp and require MSP remote-access controls and evidence of compliance.
3. Detect QEMU, QCOW2 or ACOW2 artifacts used to run backdoors outside EDR visibility.
4. Block Quick Assist where not required and train distributed helpdesks against vishing.
5. Rotate privileged credentials potentially exposed through Amadey and StealC infections.

ONGOING DETECTION AND RESILIENCE

1. Hunt AsyncRAT TLS certificate patterns on non-standard ports.
2. Maintain air-gapped or immutable backups resilient to network-share encryption.
3. Protect backups from in-guest shadow-copy deletion using hypervisor or cloud immutability.
4. Evaluate AS-level blocking for repeat bulletproof-hosting infrastructure.

June source reports: Red Piranha weekly reports, Bitsight and Microsoft Operation Endgame reporting, and Censys AsyncRAT family infrastructure analysis from June 2026.

APAC

EXECUTIVE SUMMARY

State-sponsored OT pre-positioning meets a high-tempo ransomware ecosystem

APAC energy, gas, oil and utilities faced two parallel threat streams during June 2026. Chinese state-sponsored groups focused on long-term access to utility and OT-adjacent environments, while criminal operators maintained pressure through ransomware, credential theft and edge-device exploitation. VOLTZITE was the most strategically significant actor because its confirmed targeting scope includes Australia, New Zealand, Singapore, Taiwan and India. Earth Lusca also expanded its capability by deploying a Windows version of SrySOCKS with rootkit functionality. No source report named a specific APAC energy victim during the month, so this brief distinguishes confirmed actor targeting from inferred sector exposure.

KEY INSIGHTS

1	VOLTZITE, also tracked as Volt Typhoon, continued pre-positioning against water, electric and utility infrastructure using compromised edge devices and living-off-the-land techniques.
2	The JDY botnet exceeded 1,500 compromised SOHO and IoT devices and scanned Fortinet and other edge services used across distributed utility environments.
3	Earth Lusca released SrySOCKS for Windows with a RawWNPF kernel rootkit capable of hiding processes, files, registry keys and network connections.
4	DragonForce, Brain Cipher, AiLock and 3AM remained active ransomware risks with APAC reach, although no named APAC energy victim was confirmed in the source set.
5	Operation Endgame disrupted Amadey and StealC infrastructure, but replacement loader and credential-theft capability appeared during the same reporting window.
6	The June corpus rose from 164 to 455 reports, a 177 percent increase from May, indicating a materially more active threat environment.

Top threat entities and June trend shifts

- **VOLTZITE** NATION-STATE

Pre-positioning in water and energy environments through FortiGate, Ivanti, SOHO routers and valid-account abuse. Uses LOLBins and compromised routers for proxying.

- **Earth Lusca / FishMonger** NATION-STATE

Targeted oil, gas and energy organizations across Asia with SprySOCKS for Windows, multi-protocol C2 and a kernel rootkit.

- **DragonForce** RANSOMWARE

LockBit 3.0 derivative using BYOVD drivers Truesight.sys and RentDrv.sys to terminate EDR before cross-platform encryption.

- **Brain Cipher** RANSOMWARE

LockBit-derived ransomware using CVE-2023-28252 for privilege escalation and exposed RDP or VPN services for entry.

- **AiLock** RANSOMWARE

New RaaS using ChaCha20 with NTRUEncrypt256 and explicit regulatory-notification pressure.

- **GoldenGh0stLoader** LOADER / RAT

Used trusted Google Cloud Storage and Amazon S3 paths for secondary payload delivery over encrypted WebSocket traffic.

Trend shifts versus May 2026

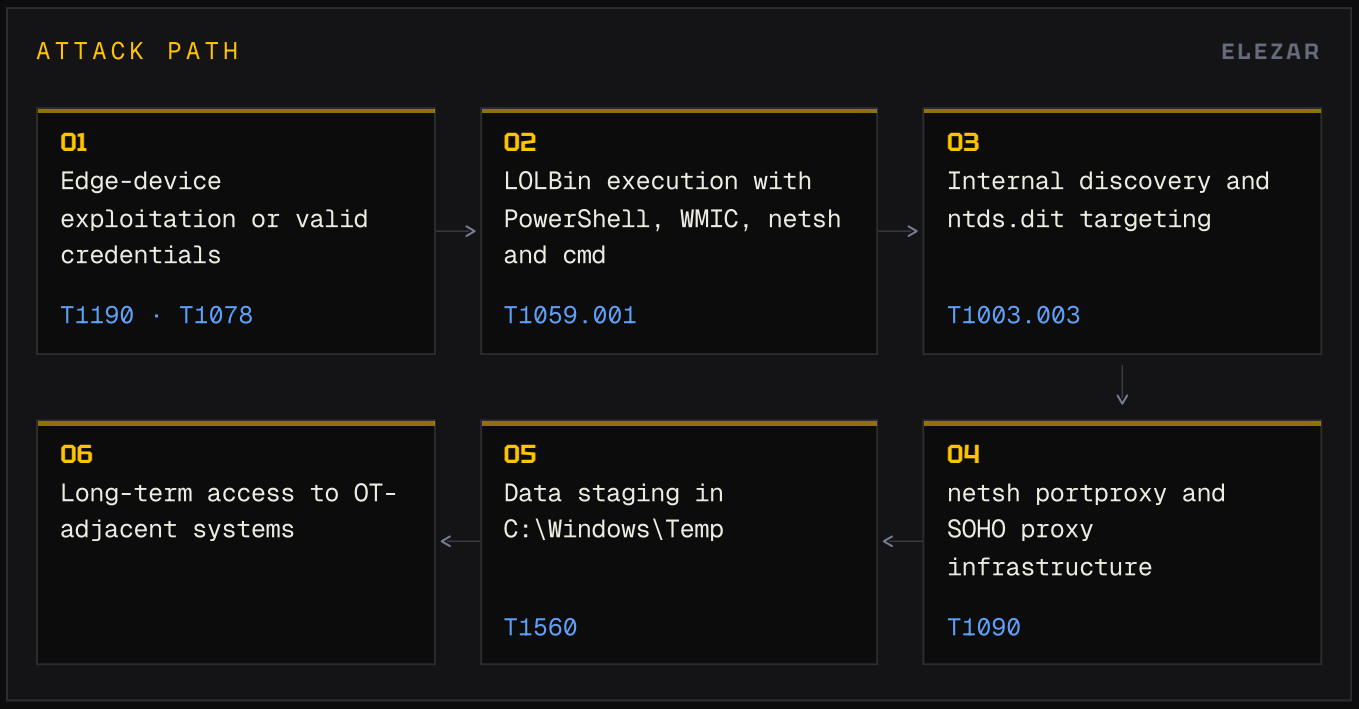
1 State-sponsored utility targeting moved from general strategic concern to directly documented June reporting through VOLTZITE water-sector pre-positioning.

2	Windows rootkit capability increased through SprySOCKS, expanding Earth Lusca beyond its earlier Linux-focused tooling.
3	BYOVD EDR termination became a repeatable ransomware technique rather than an isolated observation.
4	Post-quantum key encapsulation appeared in active ransomware through AiLock.
5	Disruption of credential-stealing infrastructure did not remove access risk because replacement tooling emerged immediately.

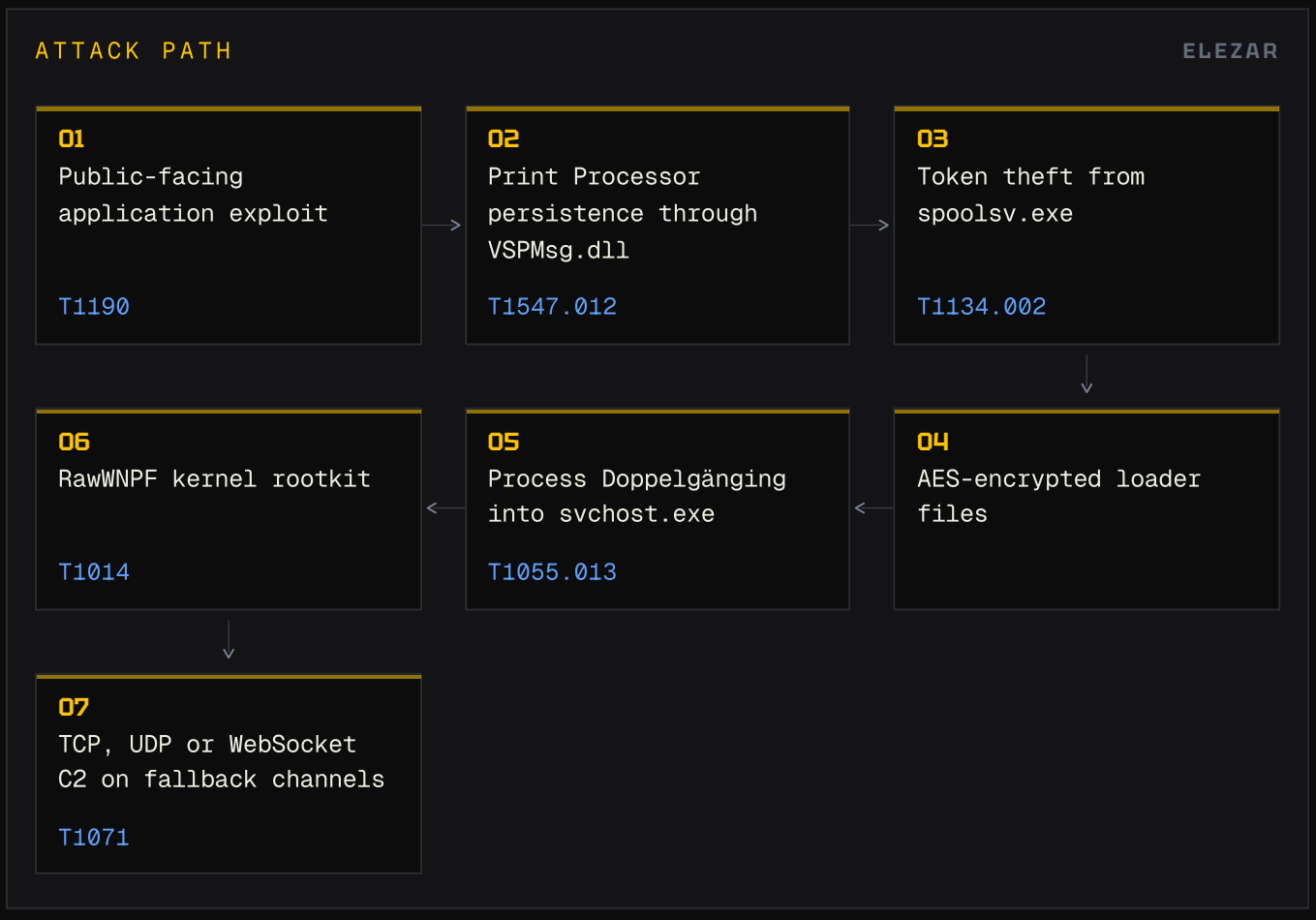
Attack chains, vulnerabilities and indicators

CVE	PRODUCT	CVSS	JUNE CONTEXT
CVE-2026-0257	Palo Alto PAN-OS	9.1	Perimeter authentication bypass risk
CVE-2026-20253	Splunk Enterprise	9.8	Unauthenticated RCE against monitoring infrastructure
CVE-2024-57726/27/28	SimpleHelp RMM	High	MSP and remote-management supply-chain access
CVE-2023-28252	Windows CLFS	High	Brain Cipher privilege escalation
CVE-2023-46805 / CVE-2024-21887	Ivanti Connect Secure	Critical	VOLTZITE and ransomware entry vector
CVE-2022-42475	FortiGate SSL VPN	Critical	VOLTZITE edge-device exploitation
CVE-2021-44228	Apache Log4j	10.0	Earth Lusca and ransomware exploitation

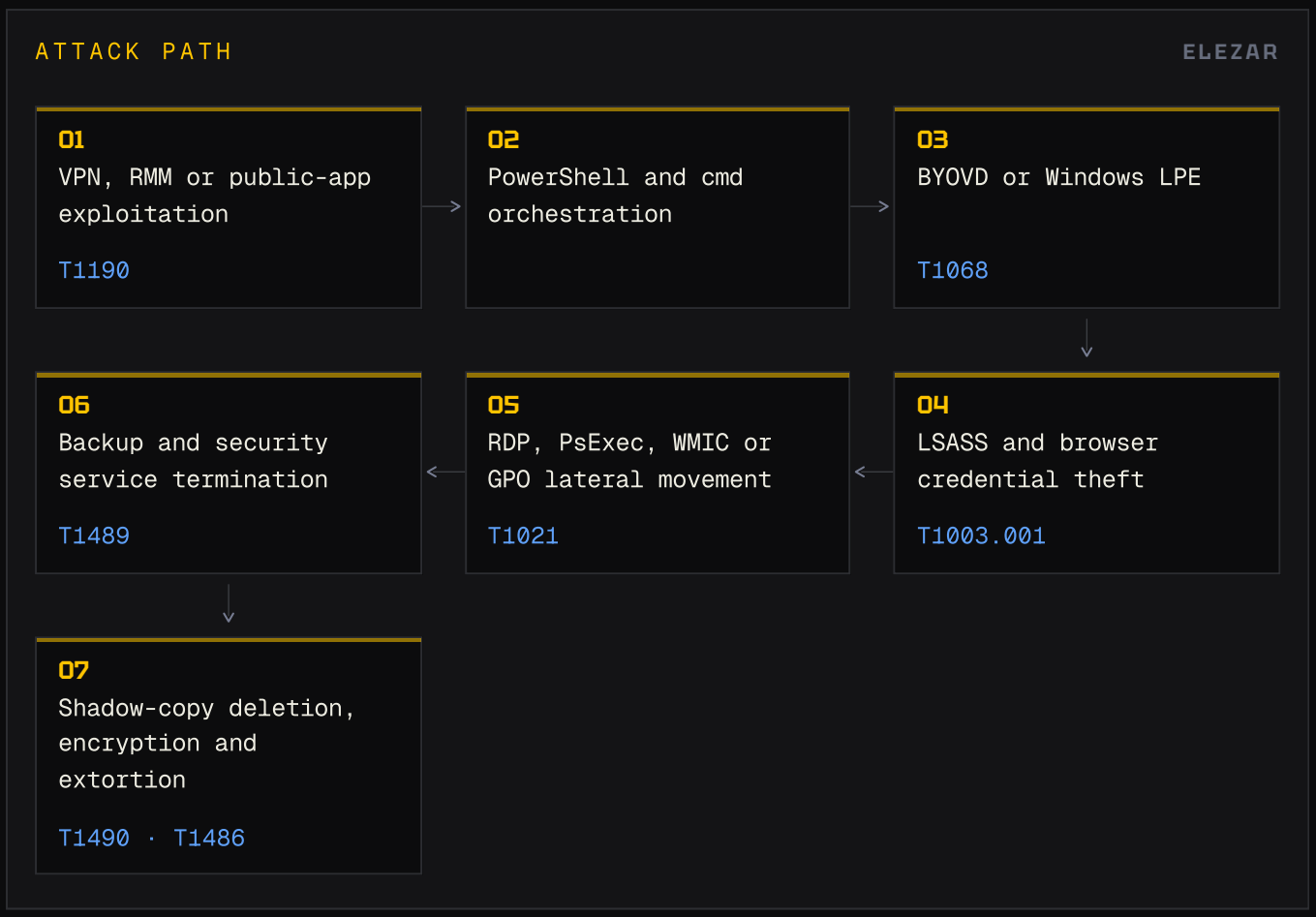
VOLTZITE utility pre-positioning



Earth Lusca SprySOCKS



Ransomware double extortion



Selected indicators

TYPE	INDICATOR	ATTRIBUTION
IP	149[.]248[.]3[.]38:13339	VOLTZITE / JDY payload server
Process	auditdy	JDY botnet process
Driver	Truesight.sys / RentDrv.sys	DragonForce BYOVD
SHA256	410db536a57c511b0ccac2639e0eb3320f303fc5c90242379ab43364c51ef321	DragonForce
IP	88[.]118[.]167[.]239:443 / 172[.]86[.]121[.]134	3AM QDoor C2
File	X1B5206BDC1743DD.dat	SprySOCKS encrypted payload
Registry	HKLM\SYSTEM\ControlSet001\Control\Print\Environments\Windows x64\Print Processors\VSPMsg	SprySOCKS persistence

Prioritized defensive guidance

Recommendations are calibrated for distributed utility operations, OT and ICS estates, remote-access infrastructure, MSP dependencies and high-impact service continuity requirements.

IMMEDIATE: ACT WITHIN 7 DAYS

1. Patch or isolate PAN-OS, Ivanti and FortiGate edge systems under active exploitation.

2. Block and hunt Truesight.sys and RentDrv.sys driver loads across Windows estates.

3. Remove public exposure from PLC, HMI and SCADA management interfaces, and rotate default credentials.

URGENT: ACT WITHIN 30 DAYS

1. Replace or harden SOHO and IoT devices used at remote substations and utility sites.

2. Disable unnecessary Print Spooler services and audit new Print Processor registry entries.

3. Detect SrySOCKS at the network layer because RawWNPF hides host-level indicators.

4. Restrict Quick Assist and train helpdesks against email-flood plus vishing attacks.

5. Patch SimpleHelp and require MSP attestation for remote-management security.

ONGOING DETECTION AND RESILIENCE

1. Hunt VOLTZITE living-off-the-land patterns including csvde, netsh portproxy, certutil and 7-Zip staging.

2. Control executable downloads from public cloud storage and inspect unexpected WebSocket traffic.

3. Maintain offline immutable backups for historians, engineering shares and OT-support systems.

4. Prepare legal and incident-response procedures for regulatory-notification extortion.

June source reports: DomainTools nation-state targeting of water systems reports, Lumen Black Lotus Labs JDY botnet analysis, ESET SrySOCKS for Windows, and Red Piranha weekly reports for June 2026.