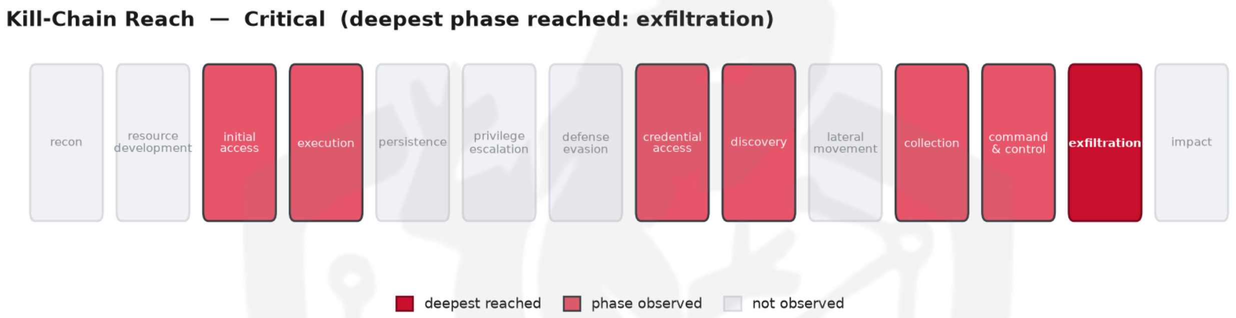
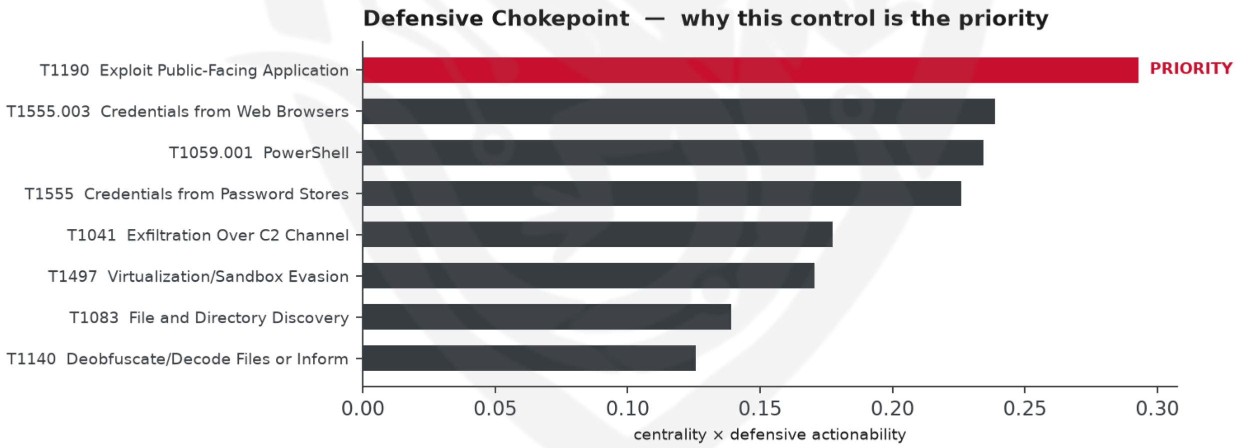
THREAT REPORT: ENERGY SECTOR TARGETED BY EKZ STEALER EXPLOITING FORTINET CVE-2026-35616

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

An observed cluster of activity leveraged the EKZ Stealer malware family to exploit the Fortinet vulnerability identified as CVE-2026-35616. The campaign focused on organizations within the energy sector. Defensive priority should be to patch the vulnerable public-facing services immediately, apply a virtual patch via a web-application firewall, and restrict management interfaces to VPN-only access, while also ensuring the CVE is patched on all affected systems.

Threat Overview

The threat actor is not identified in the source. The activity employed the EKZ Stealer malware family and exploited the Fortinet CVE-2026-35616 flaw. Victims were energy-sector entities, though no specific country was disclosed.

Attack Chain and Priority Control

The observed techniques follow a typical intrusion sequence:
1. **T1190 – Exploit Public-Facing Application** – initial compromise of the Fortinet service.
2. T1082 – System Information Discovery.
3. T1083 – File and Directory Discovery.
4. T1027 – Obfuscated Files or Information, including T1027.002 Software Packing.
5. T1059.001 – PowerShell execution.
6. T1105 – Ingress Tool Transfer.
7. T1005 – Data from Local System.
8. T1041 – Exfiltration Over C2 Channel.
9. T1070.004 – File Deletion.

Priority technique: T1190 Exploit Public-Facing Application.
Concrete control (as stated in the source): *Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only. In parallel, patch CVE-2026-35616 on all affected systems.*

Infrastructure and Corroboration

The enrichment data did not reveal any hosting providers or autonomous system numbers linked to the malicious infrastructure. AbuseIPDB reported no indicators with a confidence level of 80 % or higher. No additional malware families were corroborated by abuse.ch.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1036.005 Match Legitimate Resource Name or Location
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1555 Credentials from Password Stores
- T1555.003 Credentials from Web Browsers
- T1083 File and Directory Discovery
- T1497 Virtualization/Sandbox Evasion
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1027 Obfuscated Files or Information

- T1070.004 File Deletion
- T1027.002 Software Packing
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.2928).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4167; 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
APT39	0.4167
Patchwork	0.4157
APT3	0.3973
APT18	0.3889
Volt Typhoon	0.381

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
URL	hxxp://83[.]138[.]53[.]110/service/save[.]php
Hash	0da123adf9251957a4b850a3f6bd6a753dd4892be176a84a18450e899534cc5e
Hash	338662fd0c4d750a0ba203a32b59f081
Hash	17e771c78430cc67e71d4547f8996a1a488e9d3f

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:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** T1190 Exploit Public-Facing Application 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:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 22+ groups that use Exploit Public-Facing Application, this pairing runs 2.0x above base rate, a disproportionately-coupled move rather than the obvious one.

With T1190 Exploit Public-Facing Application blocked, the threat actor could preserve the same objective by pivoting to T1047 Windows Management Instrumentation, a technique disproportionately paired with it across tracked groups. Defensive countermeasure: Monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=23, lift 1.5), T1569 System Services (n=8, lift 1.8)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command