DomainTools

THREAT BRIEF

The Knownsec Leak

China’s Contractor Driven Cyber Espionage Ecosystem

Background

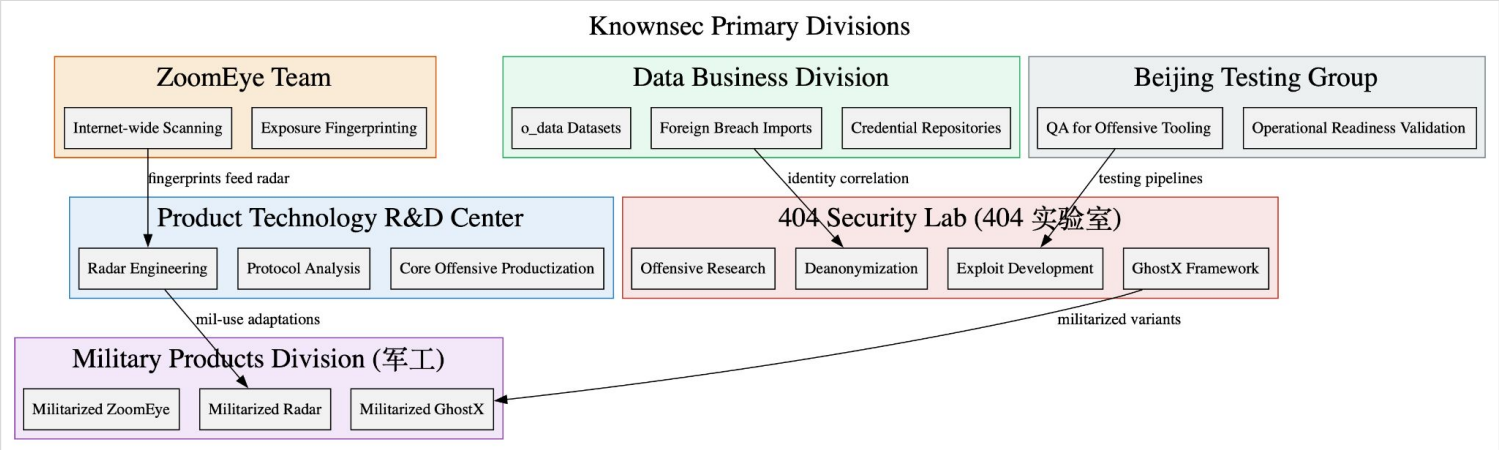
In November 2025, data from Chinese security firm Knownsec (知道创宇) was leaked on Github. Prior to the leak, Knownsec was considered a “white-hat” pillar in China’s cybersecurity landscape, focused on patching security gaps and strengthening networks. However, the leaked internal documents, product manuals, work breakdown structure (WBS) project sheets, personnel directories, and vast infrastructure datasets show Knownsec operates as an offensive intelligence contractor whose day-to-day work aligns directly with the operational needs of China’s security and military apparatus.

The leaked materials reveal that Knownsec maintains some of the most extensive foreign targeting datasets yet seen in a contractor leak, covering Taiwan, Japan, South Korea, India, and multiple Western nations. Its clients include Public Security Bureaus at the provincial and national levels, defense research institutes, and intelligence-adjacent technical units.

Organizational Structure

Knownsec's internal structure is optimized for the production of offensive cyber capabilities.

Organization	Purpose
404 Security Lab (404 实验室)	Offensive research, exploitation development, and deanonymization, including stewardship of the GhostX tooling family.
Product Technology R&D Center	Transforms raw offensive ideas into stable, deployable products (most notably Passive Radar), protocol-analysis frameworks, and related reconnaissance systems.
Data Business Division	Curates massive datasets, foreign breach archives, and credential repositories, effectively forming the human intelligence layer of Knownsec's cyber operations.
Military Products Division (军工)	Adapts and reconfigures Knownsec's core technologies – ZoomEye, Radar, GhostX – into militarized variants suitable for defense research institutes and specialized units.
ZoomEye Team	Maintains the company's most publicly recognizable asset: a continuous internet-wide scanning and exposure fingerprinting platform.
Beijing Testing Group	Ensures products meet stability and operational-readiness requirements before deployment to customers.



DomainTools

Offensive Tooling Pipeline

- **ZoomEye** is the company's internet-wide scanning and fingerprinting platform that functions as a persistent intelligence sensor grid. A global cyberspace search engine equivalent to Shodan/FOFA.

- **TargetDB (关基目标库)** is the analytical backbone of its reconnaissance capability, an immense, curated intelligence repository that transforms raw internet data into a structured map of global critical infrastructure.

- **Data Lake (o_data_*)** is a carefully indexed archive of global breach data, sourced from criminal markets, prior compromises, open leaks, and internal acquisitions.

- **GhostX** operates at the intersection of browser exploitation, network manipulation, and host persistence. It begins with browser fingerprinting, gathering granular details, plugins, fonts, extensions, power telemetry, and rendering quirks to create a durable identity signature that follows a user across VPNs, proxies, and devices. Once a target is profiled, GhostX can be set to escalate into active compromise.

- **Un-Mail platform** is the company's dedicated engine for webmail takeover and long-term communications exploitation, effectively turning inboxes into intelligence feeds.

- **Passive Radar (无源雷达)** is designed for the phase immediately following initial access, when the operational priority shifts from intrusion to comprehension. It relies on ingestion and analysis of packet capture (PCAP) data. This passive approach allows operators to observe a network as it actually behaves, without altering traffic patterns or triggering defensive controls, the system then automatically extracts and classifies the network's technical structure.

Supply Chain Intelligence

Knownsec's operational footprint is supported by a sophisticated and multilayered supply chain, one that mirrors the procurement logic of government-backed defense contractors. They utilize European hosting infrastructure, including services from companies such as EDIS and Impreza. These foreign VPS and storage nodes provide staging grounds for scanning operations, payload delivery, redirection infrastructure, and exfiltration endpoints. Their geographic dispersion reduces attribution risk and increases operational reach.

DATA ACQUISITION ECOSYSTEM

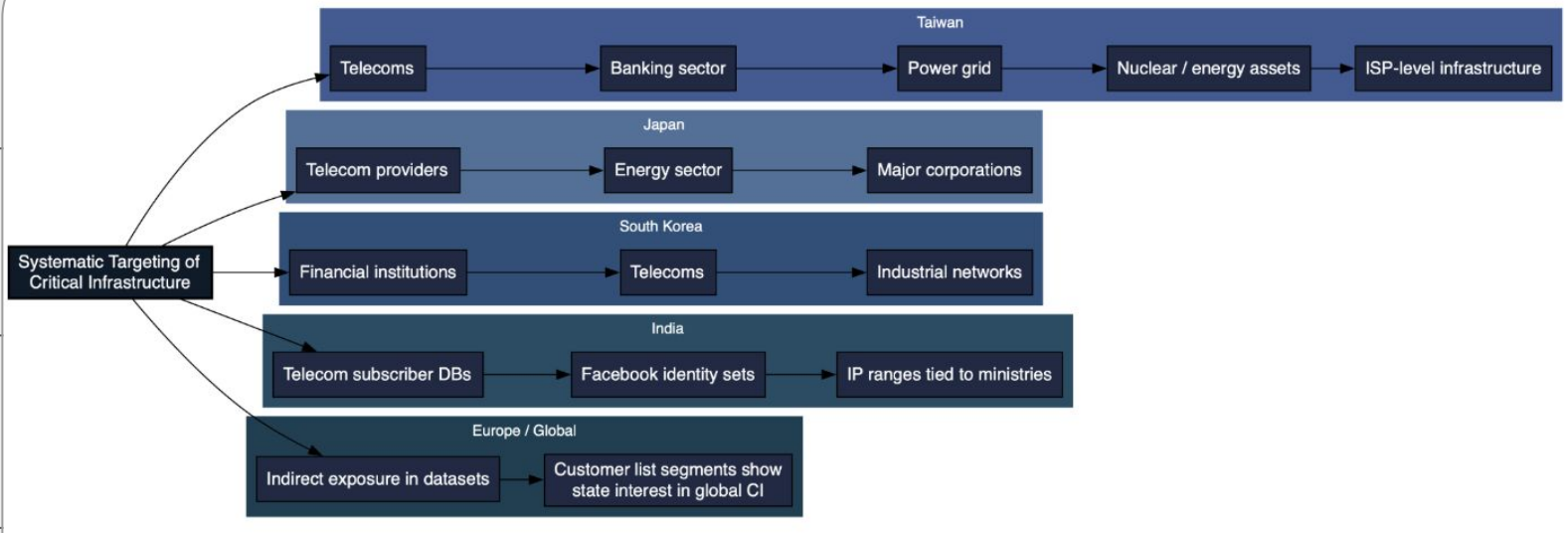
Knownsec's massive o_data_* archives encompassing foreign breach dumps, credential collections, telecom subscriber databases, and national-ID repositories come from a mix of purchases, criminal-market harvesting, and internal scraping operations.

EVIDENCE FROM INTERNAL DOCUMENTS SHOWS:

- Internal cost centers for offensive tooling.
- WBS projects show formal funding lines with project sponsors.
- External datasets are purchased or harvested from criminal markets.
- Infrastructure procurement mirrors government-funded contractor operations.

Global Targeting

Knownsec's targeting is strategic, multi-regional, and overtly political, aligning with the geopolitical interests of the PRC. Indicators of compromise (IOCs) point to a deliberate and methodical mapping of Taiwan's financial, telecommunications, and energy sectors. The sample extracted entries illustrate this well: exposed Fortinet firewalls at Nan Shan Life Insurance and Hua Nan Commercial Bank, publicly reachable Sophos XG appliances at Chunghwa Telecom, and a vulnerable Check Point service tied to Taipower, Taiwan's national energy provider.



DomainTools

Detect and Respond in Real-Time with DomainTools

While Knownsec presents itself as a standard cybersecurity vendor, these leaked materials reveal a state-aligned offensive contractor deeply embedded in the PRC's cyberespionage ecosystem.

DomainTools provides SOC teams with near real-time detection, investigation, and enrichment capabilities to disrupt adversaries like Knownsec swiftly and efficiently. DomainTools is a critical layer and essential piece in the security stack of elite enterprises and performance-driven security teams.

THREAT INTELLIGENCE

Detect relevant indicators earlier in their lifecycle to identify and disrupt incipient attacks.

PHISHING & FRAUD PREVENTION

Know if and when malicious domains and infrastructure are spoofing your assets before they cause damage.

THREAT HUNTING

Discover IOCs and malicious infrastructure that may be hiding inside your network.

BRAND PROTECTION

Monitor lookalike domain names and protect your brand against cybercriminals.

FORENSICS & INCIDENT RESPONSE

Respond to and triage potential incidents with confidence and speed.

APPLICATION ENRICHMENT

Empower your homegrown or third-party security applications with the world's best Internet intelligence.

THE DOMAINTOOLS DIFFERENCE

Why is DomainTools the trusted source for Internet intelligence?

- Built on over 20 years of engineering experience
- and threat knowledge
- Reaches into 97% of the full Internet
- Access to billions of open-source data points
- Updated in near-real-time

DomainTools