FishMonger (Aquatic Panda)

[/fɪʃˈmʌŋgər (əˈkwætɪk ˈpændə)/]

FishMonger (aka AQUATIC PANDA) is a China-aligned APT active since around 2015, focused on long-term cyber espionage targeting governments, academia, research institutions, and technology sectors. Assessed as a high-risk threat, the group continues operations through 2024–2025, evolving into sophisticated, multi-stage intrusions against internet-facing and academic infrastructure.

IDENTITY

Attribution : Commonly assessed as a China-linked advanced persistent threat actor operating in support of political, diplomatic, and strategic intelligence goals.

Active Since : ~2015 (earliest campaigns publicly attributed; operational scale increased from 2018).

Aliases : AQUATIC PANDA; BRONZE UNIVERSITY; BountyGlad; CHROMIUM; Charcoal Typhoon; ControlX; Earth Lusca; Red Dev 10; Red Scylla; RedHotel; TAG-22.

Motivation : Espionage-focused — collection of sensitive government, academic, and technology-related intelligence.

TTPs

Initial Access

- Exploitation of internet-facing applications and servers shortly after vulnerability disclosure.
- Web server compromise via known but unpatched vulnerabilities.
- Targeted spear-phishing against academics, researchers, and policy professionals.

Execution

- Deployment of custom loaders and lightweight backdoors.
- Use of web shells for command execution on compromised servers.
- Abuse of legitimate system utilities to evade detection.

Persistence

- Long-lived web shells embedded in compromised web infrastructure.
- Scheduled tasks and service installation for endpoint persistence.
- Reuse of compromised servers as staging nodes.

Command & Control (C2)

- HTTP/HTTPS-based C2 communications.
- Domains impersonating legitimate academic, cloud, or technology services.
- Regular rotation of infrastructure to reduce attribution and takedown risk.

Lateral Movement & Collection

- Credential harvesting from application configuration files and memory.
- Discovery and collection of research data, policy documents, and internal communications.
- Selective lateral movement within high-value segments of victim networks.

Exfiltration & Impact

- Staged data exfiltration over encrypted web traffic.
- Operations focused on covert intelligence theft rather than disruption or monetization.

Malware & Tools Observed

- Custom backdoors and loaders associated with FishMonger operations.
- Multiple web shell variants used across campaigns.
- Modified open-source utilities repurposed for post-exploitation.

TARGET PROFILE

Primary Sectors : Government (foreign affairs, diplomacy), universities and academic research institutions, think tanks, technology and telecommunications companies.

Secondary Sectors : Public research bodies, policy advisory organizations.

Geographic Focus : Europe (strong emphasis on academic sector), East and Southeast Asia, South Asia, selective Middle East expansion.

THREAT ASSESSMENT

Risk Level : HIGH — persistent exploitation of exposed infrastructure, disciplined operational security, and strategic target selection.

Recent Activity : Active throughout 2024–2025, with campaigns observed against European universities and government-affiliated research bodies.

Evolution : Progressed from opportunistic web compromises to coordinated, intelligence-driven intrusion campaigns with improved tooling and infrastructure hygiene.

NOTABLE OPERATIONS

2018–2019: Initial large-scale campaigns targeting European universities via vulnerable web servers and web shells.

2020: Increased focus on government-linked research and public policy institutions during global geopolitical shifts.

2021–2022: Expansion into technology and telecommunications sectors; refinement of post-exploitation tooling.

2023–2025: Sustained exploitation of edge devices and enterprise applications; continued focus on academia and policy-oriented targets with mature operational discipline.