Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

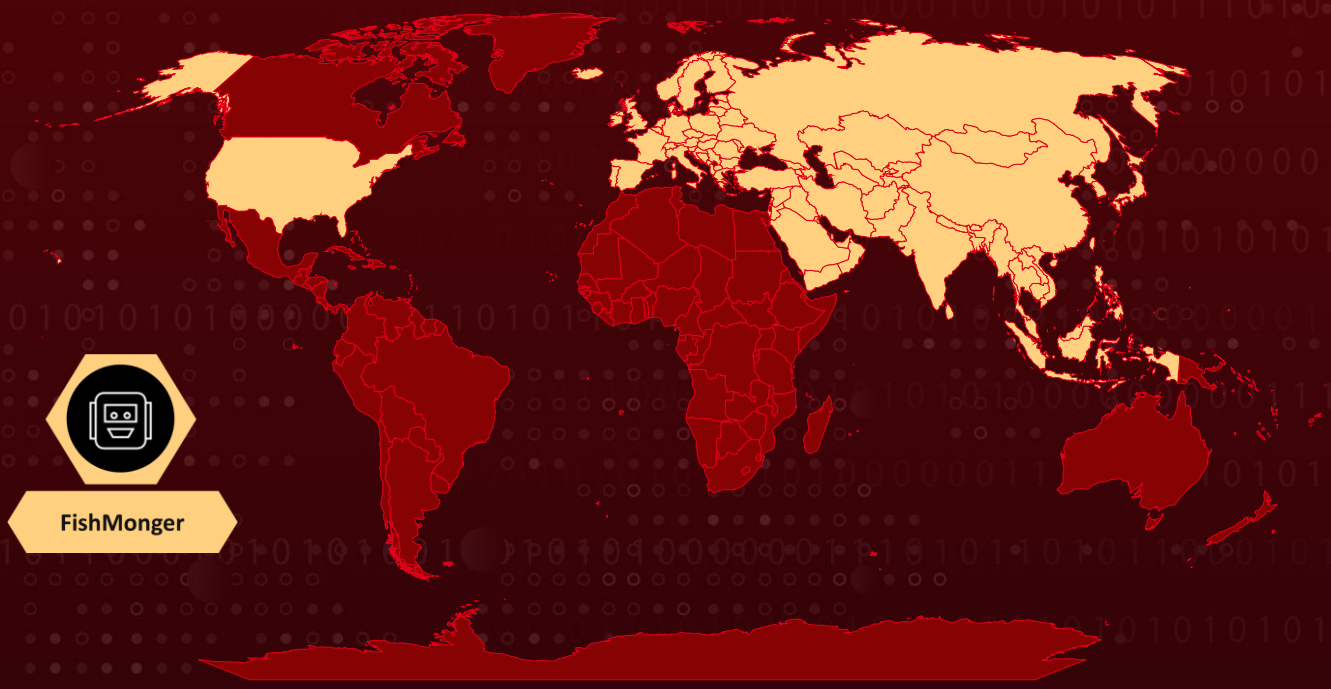
FishMonger the Espionage Group Behind Operation FishMedley

Date of Publication	Admiralty Code	TA Number
March 21, 2025	A1	TA2025088

Summary

Attack Commenced: January 2022
Threat Actor: FishMonger (alias Earth Lusca, TAG-22, RedHotel, Bronze University, Red Scylla, Chromium, AQUATIC PANDA, Charcoal Typhoon, ControlX, Red Dev 10)
Malware: ShadowPad, SodaMaster, Spyder
Campaign: Operation FishMedley
Targeted Regions: Asia, Europe, and the United States
Targeted Industries: Government, NGOs, Think Tank, Religion
Attack: In a shadowy game of cyber espionage, the elusive group FishMonger, also known as Earth Lusca, launched Operation FishMedley in January 2022, striking governments, NGOs, and think tanks across Asia, Europe, and the United States. Believed to be operated by the Chinese contractor I-SOON, FishMonger is armed with sophisticated malware, allowing the attackers to move stealthily, exploit credentials, and infiltrate networks with chilling precision.

Attack Regions



Attack Details

#1 In January 2022, a global cyber-espionage campaign known as Operation FishMedley was launched by the advanced persistent threat (APT) group FishMonger. Also referred to as **Earth Lusca**, TAG-22, Aquatic Panda, or Red Dev 10, FishMonger targeted governments, non-governmental organizations (NGOs), and think tanks across Asia, Europe, and the United States.

#2 Notable victims included a Taiwanese government agency, a Catholic organization in Hungary, a charity in the United States, and a French think tank. The group is believed to be operated by I-SOON, a Chinese contractor based in Chengdu, which faced a significant document leak in 2024 exposing its malicious operations.

#3 FishMonger is notorious for employing watering-hole attacks and using compromised websites to infect unsuspecting visitors. Their arsenal of malware includes ShadowPad, a modular backdoor frequently used for persistent access; Spyder, an encrypted communication tool for post-compromise activities; and SodaMaster, a backdoor used for data extraction and remote command execution.

#4 These tools are typically delivered through PowerShell commands and DLL side-loading techniques, often disguised using legitimate software such as Bitdefender executables to evade detection. The attackers commonly gained initial access by compromising administrative credentials or exploiting vulnerable systems.

#5 In several instances, they hijacked administrative consoles to deploy implants across networks. Impacket, a widely used lateral movement framework, was deployed to navigate through compromised environments. Additionally, credential dumping techniques using *comsvcs.dll* allowed attackers to capture sensitive information and maintain further access.

#6 FishMonger's reliance on such sophisticated, well-maintained tools, combined with their calculated attack methods, reflects a consistent pattern of state-sponsored cyber espionage. Their activities emphasize the ongoing threat to organizations and the critical importance of implementing robust cybersecurity measures.

Recommendations

Strengthen Access Controls: Implement multi-factor authentication (MFA) across all administrative and user accounts. Enforce least privilege access to limit the impact of compromised credentials. Monitor for unauthorized use of administrative consoles and restrict access using role-based access controls (RBAC).

Enhance Network Security: Segment networks to minimize lateral movement in case of a breach. Deploy network intrusion detection systems (NIDS) and intrusion prevention systems (IPS) to identify suspicious activities. Regularly update firewalls and ensure rules prevent unauthorized remote access.

Network Segmentation & Zero Trust Implementation: Segment critical infrastructure to isolate sensitive data and limit lateral movement. Implement Zero Trust Network Access (ZTNA) by enforcing identity-based policies rather than traditional perimeter security.

Harden Administrative Console: Limit access to admin consoles and ensure they are accessible only from secure, dedicated devices. Enable audit logging to detect unauthorized access attempts. Monitor for anomalous activity like suspicious commands executed on admin consoles.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0011 Command and Control	T1583 Acquire Infrastructure	T1583.004 Server	T1583.001 Domains
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.003 Windows Command Shell	T1072 Software Deployment Tools
T1543 Create or Modify System Process	T1543.003 Windows Service	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading

T1140 Deobfuscate/Decode Files or Information	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1556** Modify Authentication Process
T1556.002 Password Filter DLL	**T1003** OS Credential Dumping	**T1003.001** LSASS Memory	**T1003.002** Security Account Manager
T1087 Account Discovery	**T1087.001** Local Account	**T1016** System Network Configuration Discovery	**T1007** System Service Discovery
T1057 Process Discovery	**T1021** Remote Services	**T1021.002** SMB/Windows Admin Shares	**T1095** Non-Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	junlper[.]com, api[.]googleauthenticatoronline[.]com
File Names	log.dll, task.exe, DeElevator64.dll, DrsSDK.dll, safestore64.dll, libmaxminddb-0.dll, libvlc.dll, sasetup.dll
File Paths	C:\Users\Public\task.exe, C:\windows\temp\guid.dat, C:\Windows\system32\sasetup.dll, C:\Windows\debug\svhost.tmp, C:\nb.exe, C:\Users\public\drop.zip
IPv4	213[.]59[.]118[.]124, 61[.]238[.]103[.]165, 162[.]33[.]178[.]23, 78[.]141[.]202[.]70, 192[.]46[.]223[.]211, 168[.]100[.]10[.]136

TYPE	VALUE
SHA1	3c08c694c222e7346bd8633461c5d19eae18b661, d8b631c551845f892ebb5e7d09991f6c9d4facad, 3a702704653ec847cf9121e3f454f3dbe1f90afd, 3630f62771360540b66701abc8f6c868087a6918, a4f68d0f1c72c3ac9d70919c17dc52692c43599e, 5401e3ef903afe981cfc2840d5f0ef2f1d83b0bf, d61a4387466a0c999981086c2c994f2a80193ce3, 918ddd842787d64b244d353bfc0e14cc037d2d97, f12c8cec813257890f4856353abd9f739deed890, 3f5f6839c7dcb1d164e4813af2e30e9461ab35c1
URLs	hxxp[:]//5[.]188[.]230[.]47/log[.]dll, hxxp[:]//<a_victim's_web_server_IP_address>/Images/menu/aa[.]doc

References

https://www.welivesecurity.com/en/eset-research/operation-fishmedley/

https://hivepro.com/threat-advisory/earth-luscas-sneaky-moves-unleashes-new-linux-backdoor/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

REPORT GENERATED ON

March 21, 2025 • 4:00 AM

More at www.hivepro.com