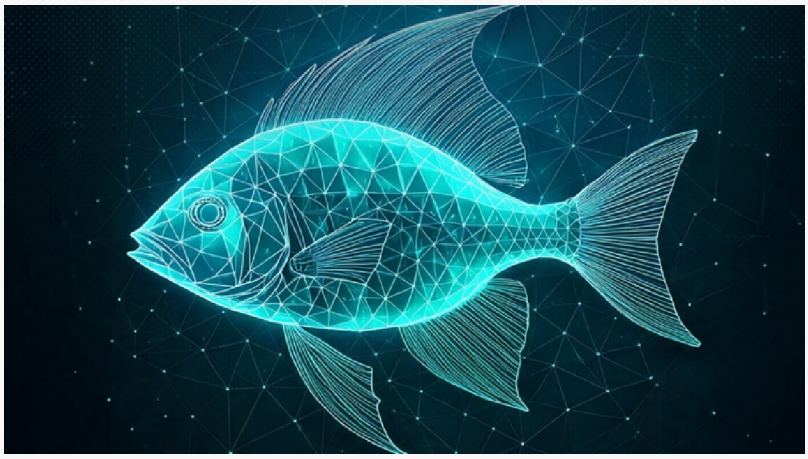
ESET Research reveals Operation FishMedley — global espionage operation by China's FishMonger and I-SOON



DUBAI , DUBAI, UNITED ARAB EMIRATES, March 24, 2025 /EINPresswire.com/ -- The US Department of Justice (DOJ) recently unsealed an indictment against employees of the Chinese contractor I SOON for their involvement in multiple global espionage operations. Those include attacks that ESET Research previously documented in its Threat Intelligence reports and attributed to the FishMonger group — I-SOON's operational arm — including one involving seven organizations ESET identified as being targeted in a 2022 campaign that ESET named Operation FishMedley. Alongside the indictment, the FBI (which refers to FishMonger as Aquatic Panda) added those named to its Most Wanted list. The indictment describes several attacks that are strongly related to what we published in a private APT intelligence report in early 2023. Today, ESET Research shares technical knowledge about this global campaign that targeted governments, nongovernmental organizations (NGOs), and think tanks across Asia, Europe, and the United States.

"During 2022, ESET investigated several compromises where implants such as ShadowPad and SodaMaster, which are commonly employed by China-aligned threat actors, were used. We were able to cluster seven independent incidents for Operation FishMedley," says ESET researcher Matthieu Faou, who investigated FishMonger's operation. "During our research, we were able to independently confirm that FishMonger is an espionage team operated by I SOON, a Chinese contractor based in Chengdu that suffered an infamous document leak in 2024." adds Faou.

During 2022, in Operation FishMedley, FishMonger attacked governmental organizations in Taiwan and Thailand, Catholic charities in Hungary and the United States, an NGO in the United States, a geopolitical think tank in France, and an unknown organization in Turkey. These verticals and countries are diverse, but most are of obvious interest to the Chinese government.

In most cases, the attackers seemed to have privileged access inside the local network, such as domain administrator credentials. Operators used implants, such as ShadowPad, SodaMaster, and Spyder, that are common or exclusive to China-aligned threat actors. Among other tools used by FishMonger in FishMedley are a custom password exfiltrating passwords; a tool used to interact with Dropbox, likely used to exfiltrate data from the victim's network; the fscan network scanner; and a NetBIOS scanner.

FishMonger — a group operated by the Chinese contractor I SOON — falls under the Winnti Group umbrella and is most likely operating out of China, from the city of Chengdu, where I-SOON's office remains likely to be located. FishMonger is also known as Earth Lusca, TAG 22, Aquatic Panda, or Red Dev 10. ESET published an analysis of this group in early 2020 when it heavily targeted universities in Hong Kong during the civic protests that started in June 2019. The group is known to operate watering-hole attacks. FishMonger's toolset includes ShadowPad, Spyder, Cobalt Strike, FunnySwitch, SprySOCKS, and the BIOPASS RAT.

For a more detailed analysis and technical breakdown of FishMonger's operation, FishMedley, check out the latest ESET Research blog post, "Operation FishMedley," on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of known and emerging cyberthreats — securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. An ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and X.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here

in today's world. Please see our Editorial Guidelines for more information.