ESET releases latest APT report: China-aligned groups expand targeting; Iran advances diplomatic espionage

DUBAI , DUBAI, UNITED ARAB EMIRATES, November 13, 2024 /EINPresswire.com/ -- ESET Research has released its latest APT Activity Report, which highlights activities of select advanced persistent threat (APT) groups that were documented by ESET researchers from April 2024 until the end of September 2024. ESET observed a notable expansion in targeting by China-aligned MirrorFace. Typically focused on Japanese entities, it extended its operations to include a diplomatic organization in the European Union for the first time, while continuing to prioritize its Japanese targets. Additionally, China-aligned APT groups have been increasingly relying on the open-source and multiplatform SoftEther VPN to maintain access to victims' networks. Researchers also observed indications that Iran-aligned groups might be leveraging their cybercapabilities to support diplomatic espionage and, potentially, kinetic operations.

"With regard to China-aligned threat groups, we detected extensive use of the SoftEther VPN by Flax Typhoon, observed Webworm switching from its full-featured backdoor to using the SoftEther VPN Bridge on machines belonging to governmental organizations in the EU, and noticed GALLIUM deploying SoftEther VPN servers at telecommunications operators in Africa," says Director of Threat Research at ESET, Jean-Ian Boutin. "For the first time, we observed MirrorFace targeting a diplomatic organization within the EU, a region that remains a focal point for several China-, North Korea-, and Russia-aligned threat actors. Many of these groups are particularly focused on governmental entities and the defense sector," he adds.

Iran-aligned groups, on the other hand, compromised several financial services firms in Africa – a continent geopolitically important to Iran, conducted cyberespionage against Iraq and Azerbaijan, neighboring countries with which Iran has complex relationships, and increased their stake in the transport sector in Israel. Despite this seemingly narrow geographical targeting, Iran-aligned groups maintained a global focus, further pursuing diplomatic envoys in France and

educational organizations in the United States.

North Korea-aligned threat actors persisted with their pursuit of stolen funds – both traditional currencies and cryptocurrencies. We observed these groups continuing their attacks on defense and aerospace companies in Europe and the US, as well as targeting cryptocurrency developers, think tanks, and NGOs. One such group, Kimsuky, began abusing Microsoft Management Console files, which are typically used by system administrators but can execute any Windows command. Additionally, several North Korea-aligned groups frequently misused popular cloud-based services.

And finally, ESET Research detected Russia-aligned cyberespionage groups frequently targeting webmail servers such as Roundcube and Zimbra, usually with spearphishing emails that trigger known XSS vulnerabilities. Besides Sednit targeting governmental, academic, and defense-related entities worldwide, ESET identified another Russia-aligned group, GreenCube, stealing email messages via XSS vulnerabilities in Roundcube. Other Russia-aligned groups continued to focus on Ukraine, with Gamaredon deploying large spearphishing campaigns while reworking its tools using and abusing both Telegram and Signal messaging apps. Additionally, Sandworm utilized its new Windows backdoor named WrongSens. ESET also analyzed the public hack-and-leak of data from the Polish Anti-Doping Agency, which was likely compromised by an initial access broker who then shared access with the Belarus-aligned FrostyNeighbor APT group, an entity behind cyber-enabled disinformation campaigns critical of NATO.

In Asia, ESET observed that campaigns continued to focus primarily on governmental organizations. However, research also noticed an increased emphasis on the education sector, particularly targeting researchers and academics focused on the Korean peninsula and Southeast Asia. This shift was driven by threat actors aligned with China and North Korea's interests. Lazarus, one of the North Korea-aligned groups, continued to attack entities around the globe in the financial and technology sectors. In the Middle East, several Iran-aligned APT groups continued to attack governmental organizations, with Israel being the most affected country.

Over the past two decades, Africa has become a significant geopolitical partner for China, and we have seen China-aligned groups expand their activities on that continent. In Ukraine, Russia-aligned groups continued to be the most active, heavily impacting governmental entities, the defense sector, and essential services such as energy, water, and heat supply.

The highlighted operations are representative of the broader landscape of threats ESET investigated during this period. ESET products protect our customers' systems from the malicious activities described in this report. Intelligence shared here is based mostly on proprietary ESET telemetry data. These threat intelligence analyses, known as ESET APT Reports PREMIUM, assist organizations tasked with protecting citizens, critical national infrastructure, and high-value assets from criminal and nation-state-directed cyberattacks. More information about ESET APT Reports PREMIUM and its delivery of high-quality, strategic, actionable, and

tactical cybersecurity threat intelligence is available at the ESET Threat Intelligence page.

You can read the full ESET APT Activity Report 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
email us here