ESET Research discovers China-aligned APT group Blackwood that uses advanced implant to attack within China, Japan & UK

DUBAI , DUBAI, UNITED ARAB EMIRATES, January 30, 2024 /EINPresswire.com/ -- ESET researchers have discovered NSPX30, a sophisticated implant used by a new China-aligned APT group, named Blackwood by ESET. Blackwood leverages adversary-in-the-middle techniques to hijack update requests from legitimate software to deliver the implant. It has carried out cyberespionage operations against individuals and companies from China, Japan, and the United Kingdom. ESET mapped the evolution of NSPX30 back to an earlier ancestor – a simple backdoor we have named Project Wood. The oldest sample found was compiled in 2005.

ESET Research named Blackwood and the backdoor Project Wood based on a recurring theme in a mutex name. A mutex, or mutual exclusion, is a synchronization tool used to control access to a shared resource. The Project Wood implant from 2005 appears to be the work of developers with experience in malware development, given the techniques implemented. ESET believes that the China-aligned threat actor we have named Blackwood has been operating since at least 2018. In 2020, ESET detected a surge of malicious activity on a targeted system located in China. The machine had become what is commonly referred to as a “threat magnet,” as ESET Research detected attempts by attackers to use malware toolkits associated with multiple APT groups.

According to ESET telemetry, the NSPX30 implant was recently detected on a small number of systems. The victims include unidentified individuals located in China and Japan, an unidentified Chinese-speaking individual connected to the network of a high-profile public research university in the United Kingdom, a large manufacturing and trading company in China, and China-based offices of a Japanese corporation in the engineering and manufacturing vertical. ESET has also observed that the attackers attempt to re-compromise systems if access is lost.

NSPX30 is a multistage implant that includes several components, such as a dropper, an installer, loaders, an orchestrator, and a backdoor. Both of the latter components have their own sets of plugins that implement spying capabilities for several applications, such as Skype, Telegram, Tencent QQ, and WeChat, among others. It is also capable of allowlisting itself in several Chinese antimalware solutions. Using ESET telemetry, ESET Research determined that machines are compromised when legitimate software attempts to download updates from legitimate servers using the (unencrypted) HTTP protocol. Hijacked software updates include those for popular Chinese software, such as Tencent QQ, Sogou Pinyin, and WPS Office. The basic purpose of the backdoor is to communicate with its controller and exfiltrate collected data; it is capable of taking screenshots, keylogging, and collecting various information.

The attackers' capability for interception also allows them to anonymize their real infrastructure, as the orchestrator and the backdoor contact legitimate networks owned by Baidu to download new components or exfiltrate collected information. ESET believes that the malicious but legitimate-looking traffic generated by NSPX30 is forwarded to the real attackers' infrastructure by the unknown interception mechanism that also performs adversary-in-the-middle attacks.

"How exactly the attackers are able to deliver NSPX30 as malicious updates remains unknown to us, as we have yet to discover the tool that enables the attackers to compromise their targets initially," says ESET researcher Facundo Muñoz, who discovered NSPX30 and Blackwood. "However, based on our own experience with China-aligned threat actors who exhibit these capabilities, as well as recent research on router implants attributed to another China-aligned group, MustangPanda, we speculate that the attackers are deploying a network implant within the networks of the victims, possibly on vulnerable network appliances, such as routers or gateways," explains Muñoz.

For more technical information about the new China-aligned APT group Blackwood and its latest NSPX30 implant, check out the blog post "NSPX30: A sophisticated AitM-enabled implant evolving since 2005." Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and X (Twitter).

Sanjeev Kant

Vistar Communications
+971 55 972 4623
email us here