**NSPX30 Analysis Report**

In my ongoing research project, I've come across a significant threat that sheds light on the activities of a new China-aligned Advanced Persistent Threat (APT) group named Blackwood. This APT group, which we believe has been operating since at least 2018, employs a sophisticated implant known as NSPX30. The NSPX30 implant is delivered through adversary-in-the-middle (AitM) attacks, specifically hijacking update requests from legitimate software.

The color-coded MITRE ATT&CK Navigator I've developed serves as a comprehensive framework to categorize and analyze various aspects of this threat. Each color assigned to different elements in the MITRE ATT&CK Navigator reflects a careful evaluation based on factors such as relevance, frequency, risk impact, severity impact, historical data, and adversary Tactics, Techniques, and Procedures (TTPs). The color spectrum ranges from green (level 1, lowest severity/impact) to red (level 5, highest severity/impact).

Key findings from my analysis of the NSPX30 threat include its deployment via the update mechanisms of well-known software such as Tencent QQ, WPS Office, and Sogou Pinyin. The implant has been identified in targeted attacks against Chinese and Japanese entities, as well as individuals in China, Japan, and the United Kingdom. NSPX30, a multistage implant, traces its evolution back to a smaller backdoor known as Project Wood, dating as far back as 2005.

The MITRE ATT&CK Navigator color system helps to emphasize critical points in the report, such as the attribution of this activity to the Blackwood APT group. This China-aligned group engages in cyberespionage operations with a focus on utilizing AitM attacks to deliver NSPX30 implants through legitimate software updates, concealing the location of its command and control servers by intercepting implant-generated traffic.

The timeline of NSPX30's evolution, originating from Project Wood, reveals the historical depth of almost two decades of development and malicious activities by an undisclosed number of threat actors. The report also highlights the geographical distribution of Blackwood's targets, emphasizing the global impact of this APT group.

Additionally, the technical analysis unveils NSPX30's capabilities, including packet interception, allowlisting in Chinese antimalware solutions, and the ability to conduct HTTP and UDP interception. The orchestrator's actions, plugin functionalities, and backdoor commands are thoroughly examined, providing a comprehensive understanding of the threat landscape.

In conclusion, the NSPX30 threat, orchestrated by Blackwood, represents a significant cybersecurity challenge with a historical context dating back to 2005. The MITRE ATT&CK Navigator color-coded framework serves as a visual aid to convey the severity, impact, and relevance of various aspects of this threat, providing a valuable tool for cybersecurity professionals to understand and respond effectively to this evolving APT.