FIELD CONTACT REPORT

CLASSIFIED DOCUMENT
PROJECT NIGHTINGALE
TEMPORARY CODE NAME: NIGHTSHADE-12

EVENT DATE: 2024-08-30
DOCUMENT CREATION DATE: 2022-03-14
TARGET ENTITY: People's Republic of China
CLASSIFICATION LEVEL: Top Secret
MISSION PRIORITY: 2
ORIGINATING DIVISION: Covert Operations

SUBJECT: Encounter with PRC Asset "Night Owl" at Shanghai Safe House

SUMMARY: On 2024-08-30, I made contact with PRC asset "Night Owl" at Shanghai Safe House #4 (Latitude: 31.2286° N, Longitude: 121.4547° E). The encounter provided technical insights into PRC's recent advances in cyber warfare capabilities.

TECHNICAL DETAILS:

1. **Communication Protocol:** Night Owl utilized an encrypted communication protocol based on the ECDH (Elliptic Curve Diffie-Hellman) key exchange algorithm, with a 256-bit key size. The protocol exhibited a 2-3 second delay, indicating potential use of a proxy server or a compromised node in the communication chain.
2. **Device Identification:** Night Owl's device, a custom-built smartphone (Model: "Aurora"), featured a 4.7-inch OLED display, a Qualcomm Snapdragon 888 processor, and 12 GB of RAM. The device's operating system (OS) was an unnamed, custom-built Android variant (Version: 12.1.0).
3. **Encryption Method:** Night Owl's device employed an AES-256-GCM (Advanced Encryption Standard with Galois/Counter Mode) encryption method for data at rest and in transit. The encryption key was derived from a 2048-bit RSA key pair, with the private key stored securely on the device.
4. **Data Transmission:** Night Owl transmitted 2.4 GB of data to our servers using a custom-built, proprietary communication protocol (TCP/IP-based). The data transfer rate averaged 10 Mbps, indicating potential use of a high-speed internet connection or a compromised network.

ANALYSIS:

Based on the technical details collected, it is clear that the PRC has made significant advancements in cyber warfare capabilities. The use of a custom-built OS, encryption method, and communication protocol suggests a high level of sophistication and coordination among PRC cyber warfare units.

The ECDH key exchange algorithm used by Night Owl's device indicates a potential vulnerability to quantum computer-based attacks. Furthermore, the use of a 256-bit key size, while currently considered secure, may be compromised in the near future as quantum computers become more powerful.

MEASUREMENTS & METRICS:

- **Device Specifications:** Aurora smartphone (Dimensions: 157.5 x 75.2 x 7.9 mm, Weight: 180 g)
- **Communication Protocol Delay:** 2-3 seconds (indicating potential use of a proxy server or compromised node)
- **Data Transfer Rate:** 10 Mbps (averaged over 2.4 GB of data transmission)

RECOMMENDATIONS:

1. **Immediate Action:** Conduct a thorough analysis of the custom-built OS and encryption method used by Night Owl's device to identify potential vulnerabilities.
2. **Long-Term Strategy:** Develop a comprehensive counter-cyber warfare plan to address the PRC's advancements in this area.
3. **Asset Management:** Continuously monitor and evaluate the performance of asset Night Owl to ensure optimal effectiveness and minimize risk.

AUTHENTICATION:

This Field Contact Report has been verified through multiple sources and is considered a reliable representation of the events described. The report has been reviewed and approved by the Covert Operations Division and is classified Top Secret.

**