APT12

Overview

APT12 is a threat group that has been attributed to China. The group has targeted a variety of victims including but not limited to media outlets, high-tech companies, and multiple governments. APT12 used a variety of malware tools in its recent attacks, including RIPTIDE, HIGHTIDE, THREEBYTE, and WATERSPOUT. APT12 quickly adapts its attack tools and continues its cyber espionage activities after each public exposure.

Tactics

APT12's tactics are focused on cyber espionage with the goal of obtaining sensitive information and taking control of victim networks. Tactics include using spear phishing for Initial Access, Privilege Escalation through known vulnerabilities (e.g., CVE-2012-0158), and using persistent backdoors such as HIGHTIDE to maintain long-term access to victim systems (Persistence).

Techniques

APT12 techniques include sending a malicious Word document (T1566.001) using spear phishing emails, executing code (T1203) by exploiting vulnerabilities in the document (e.g., CVE-2012-0158), and subsequently communicating with hard-coded C2 servers over HTTP (T1071.001) and encrypting the communication (T1573.001) to evade Detection. The backdoor program is stored under a specific path to perform persistent control.

1. **Techniques Used:** Dynamic Resolution: DNS Calculation, Exploitation for Client Execution, Phishing: Spearphishing Attachment, User Execution: Malicious File, Web Service: Bidirectional Communication
2. **Software used:** HTRAN, Ixeshe, RIPTIDE

Procedures

APT12 first attacks target organizations using spear phishing emails with malicious documents that exploit the CVE-2012-0158 vulnerability to execute code and install backdoor programs such as RIPTIDE, HIGHTIDE, and THREEBYTE.RIPTIDE first establishes communication with a command-and-control (C2) server and obtains encryption keys through HTTP GET requests. encryption key, and all subsequent communications are encrypted via RC4.HIGHTIDE is an upgraded version of RIPTIDE, which performs protocol and communication string changes to evade detection after encountering public exposure.APT12 also conducts attacks using different backdoor programs (e.g., THREEBYTE and WATERSPOUT), which are usually stored in specific system paths and achieve persistent access through encrypted communication with C2 servers.