admin@338

Overview

admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors.

Tactics

The attack group targeted Hong Kong media organizations, gaining initial access via **spear phishing** emails to continuously monitor and steal data. They use persistence tactics to maintain long-term control over the victim's systems and defense circumvention and **command and control (C2)** through legitimate cloud services such as Dropbox. The main goal of the attackers is to stealthily steal sensitive information and circumvent security measures.

Techniques

1. **Spear Phishing (T1566.001):** Through a carefully crafted phishing email, an attacker exploits a Microsoft Office vulnerability (CVE-2012-0158) to execute malicious code.
2. **Exploitation of Vulnerabilities (T1203):** Through a known vulnerability, the attacker executes malicious code on the victim's device to install LOWBALL malware.
3. **Misuse of Cloud Services (T1071.001):** the legitimate Dropbox service was used as a communication channel to mask its malicious activities.
4. **Input Capture (T1056):** malware collects system information and user input for further infiltration and control.
5. **Exfiltration of data through web services (T1567.002):** the attacker utilizes Dropbox's secure channel to transmit stolen data and bypass security systems.

Procedures

The attacker first sends a carefully crafted spear phishing email to trick the target into opening a malicious Office attachment. Exploiting the CVE-2012-0158 vulnerability, the LOWBALL malware is installed and starts communicating with the Dropbox C2 server. The malware executes batch scripts that collect network and system information (e.g. netstat, ipconfig, etc.) from the victim. Next, the attacker sends further commands via the Dropbox API to upload the collected data. Once the target system is assessed to be of high value, they deploy a more advanced backdoor, BUBBLEWRAP, for deep control and continuous data theft. Command-and-control and data exfiltration is achieved through legitimate services, successfully bypassing most security monitoring.