Axiom

Overview

Axiom is a suspected Chinese cyber espionage group that has targeted the aerospace, defense, government, manufacturing, and media sectors since at least 2008. Some reporting suggests a degree of overlap between Axiom and Winnti Group but the two groups appear to be distinct based on differences in reporting on TTPs and targeting.[1][2][3]

Tactics

Group 72(Axiom) compromised high-value intellectual property companies in manufacturing, defense, and media through phishing (T1566), watering hole attacks (T1071.001), and network vulnerability exploitation (T1203). They utilize remote administration tools such as ZxShell (T1219) to maintain persistence in the target network to further penetrate the intranet and steal sensitive data.

Techniques

ZxShell's main techniques include keylogging (T1056.001), remote desktop (T1021.001), network scanning (T1046), and encryption of data transfers (T1573.001).ZxShell hides its presence through service persistence (T1543.003) and Windows registry modifications (T1112) to prevent detection and ensures persistent access. In addition, ZxShell utilizes proxy and tunneling techniques to mask malicious traffic.

1. **Techniques Used:** Acquire Infrastructure: DNS Server, Acquire Infrastructure: Virtual Private Server, Archive Collected Data, Compromise Infrastructure: Botnet, Data from Local System, Data Obfuscation: Steganography, Drive-by Compromise, Event Triggered Execution: Accessibility Features, Exploit Public-Facing Application, Exploitation for Client Execution, OS Credential Dumping, Phishing, Remote Service Session Hijacking: RDP Hijacking, Remote Services: Remote Desktop Protocol, Subvert Trust Controls, Valid Accounts
2. **Software used:** Derusbi, gh0st RAT, Hikit, Hydraq, PlugX, PoisonIvy, Zox, ZxShell

Procedures

ZxShell injects SVCHOST processes through a complex injection and service creation process using malicious DLL files and modifies the Windows registry to create persistent backdoors.ZxShell hijacks the system's firewall configurations and uses disguised service names to bypass protection software. Its communication feature connects to remote C2 servers via encrypted IP lists and supports a variety of network attack tools, including SYN flooding attacks and ARP spoofing. In addition, ZxShell features keylogging and remote desktop capabilities that allow

attackers to steal user login credentials, monitor victim activity, and move laterally across an intranet.