Deep Panda

Overview

Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. [1] The intrusion into healthcare company Anthem has been attributed to Deep Panda. [2] This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. [3] Deep Panda also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. [4] Some analysts track Deep Panda and APT19 as the same group, but it is unclear from open source information if the groups are the same. [5]

Tactics

Deep Panda enters the victim's network by exploiting public vulnerabilities (e.g., Log4Shell, T1190) and network backdoors (T1505.003) and executes commands via hijacked services (T1569.002). The attack targets a wide range of areas, including financial and academic, with the goal of obtaining sensitive information and persistent access.

Techniques

They use command line and script interpreters (T1059.001) for malicious command execution, hiding their activities through masquerading (T1036) and reflective code loading (T1620). In addition, they use DLL side-loading (T1574.002) and root kits (T1014) to avoid detection and pass data back to the C2 server via encrypted communication (T1041).

1. **Techniques Used:** Command and Scripting Interpreter: PowerShell, Event Triggered Execution: Accessibility Features, Hide Artifacts: Hidden Window, Obfuscated Files or Information: Indicator Removal from Tools, Process Discovery, Remote Services: SMB/Windows Admin Shares, Remote System Discovery, Server Software Component: Web Shell, System Binary Proxy Execution: Regsvr32, Windows Management Instrumentation
2. **Software used:** Derusbi, Mivast, Net, Ping, Sakula, StreamEx, Tasklist

Procedures

Deep Panda first compromises the VMware Horizon server through the Log4Shell vulnerability by launching a PowerShell script that downloads and executes multiple files, including the malicious DLL, named Milestone, whose source code is based on the Gh0st RAT with file reading, system information discovery, session enumeration, and more. features, and was shelled by Themida to avoid detection. They then used the Fire Chili rootkit signed with a stolen digital certificate to hide malicious files, processes, registry entries, and network connections. The rootkit dynamically manages the hidden list via IOCTL to ensure persistence and stealth, and protects against malware manipulation.