APT3

Overview

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security.[1][2] This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap.[1][3] As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.[4]

Tactics

APT3's tactics focus on attacking corporate and government organizations through spear phishing emails and vulnerability exploits. They often use zero-day and known vulnerabilities for remote code execution and elevation of privilege, and maintain long-term access to the target network through persistence mechanisms and backdoor programs while disguising their command-and-control (C2) communications.

Techniques

APT3 utilizes spear phishing emails (T1566.001) to direct users to malicious webpages using known vulnerabilities (e.g., CVE-2014-6332 and CVE-2014-4113) for remote code execution (T1203). They use PowerShell (T1059.001) to download and execute malicious loads and create scheduled tasks (T1053.005) for persistence, while using the SOCKS5 agent for communication (T1090.003).

1. **Techniques Used:** Account Discovery: Local Account, Account Manipulation, Archive Collected Data: Archive via Utility, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Brute Force: Password Cracking, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Windows Command Shell, Create Account: Local Account, Create or Modify System Process: Windows Service, Credentials from Password Stores: Credentials from Web Browsers, Data from Local System, Data Staged: Local Data Staging, Event Triggered Execution: Accessibility Features, Exfiltration Over C2 Channel, Exploitation for Client Execution, File and Directory Discovery, Hide Artifacts: Hidden Window, Hijack Execution Flow: DLL Side-Loading, Indicator Removal: File Deletion, Ingress Tool Transfer, Input Capture: Keylogging, Multi-Stage Channels, Non-Application Layer Protocol, Obfuscated Files or Information, Software Packing, Indicator Removal from Tools, OS Credential Dumping: LSASS Memory, Permission Groups Discovery, Phishing: Spearphishing Link, Process Discovery, Proxy: External Proxy, Remote Services: Remote Desktop Protocol, Remote Services: SMB/Windows Admin Shares, Remote System Discovery, Scheduled Task/Job: Scheduled Task, System Binary Proxy Execution: Rundll32, System Information Discovery, System Network Configuration

Discovery, System Network Connections Discovery, System Owner/User Discovery, Unsecured Credentials: Credentials In Files, User Execution: Malicious Link, Valid Accounts: Domain Accounts

2. **Software used:** LaZagne, OSInfo, PlugX, RemoteCMD, schtasks, SHOTPUT

Procedures

APT3 sends emails containing malicious links or attachments to targets via spear-phishing emails that exploit vulnerabilities such as CVE-2014-6332 to execute malicious code. Malicious web pages invoke PowerShell via VBScript to download and execute malicious files (e.g. install.exe), which in turn drop other malicious files (e.g. doc.exe and test.exe). doc.exe leverages CVE-2014-4113 for elevation of privilege, which then launches test.exe, test. exe communicates with the C2 server via the SOCKS5 proxy to establish a persistent connection and receive commands to execute.APT3's C2 server issues a variety of commands, including downloading files, deleting files, or executing commands. The organization will also use custom backdoor programs such as Pirpi and SHOTPUT to maintain control of the victim network and quickly move laterally through the target network via zero-day exploits.