APT41

Overview

APT41 is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, APT41 has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. APT41 overlaps at least partially with public reporting on groups including BARIUM and Winnti Group.[1][2]

Tactics

APT41 steals sensitive information primarily by attacking the aviation industry's supply chain, particularly third-party IT service providers, targeting airlines in multiple countries. Tactics include exploiting supply chain attacks (T1195.002), persistent access (T1078), credential theft (T1003), lateral movement (T1071.004), and data exfiltration (T1041).

Techniques

APT41's technical techniques include exploiting known vulnerabilities and zero-day vulnerabilities (T1203), infecting target systems via spear phishing emails (T1566.001), and using tools such as Cobalt Strike for subsequent exploitation (T1059.001). Additionally, they utilize DNS tunneling (T1071.004) and SSL encryption (T1071.001) to hide C&C communications and use tools such as Mimikatz to obtain credentials (T1003.001).

1. **Techniques Used:** Access Token Manipulation, Account Discovery: Local Account, Account Discovery: Domain Account, Account Manipulation, Active Scanning: Vulnerability Scanning, Active Scanning: Wordlist Scanning, Application Layer Protocol: Web Protocols, Application Layer Protocol: File Transfer Protocols, Application Layer Protocol: DNS, Archive Collected Data: Archive via Utility, Archive Collected Data: Archive via Custom Method, BITS Jobs, 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, Command and Scripting Interpreter: Unix Shell, Command and Scripting Interpreter: JavaScript, Create Account: Local Account, Create or Modify System Process: Windows Service, Credentials from Password Stores: Credentials from Web Browsers, Data Encrypted for Impact, Data from Information Repositories: Code Repositories, Data from Local System, Data Obfuscation: Protocol Impersonation, Data Staged: Local Data Staging, Data Transfer Size Limits, Deobfuscate/Decode Files or Information, Dynamic Resolution: Domain Generation Algorithms, Event Triggered Execution: Accessibility Features, Execution Guardrails: Environmental Keying, Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2

Protocol, Exfiltration Over C2 Channel, Exfiltration Over Web Service, Exploit Public-Facing Application, Exploitation for Client Execution, Exploitation for Privilege Escalation, External Remote Services, Fallback Channels, File and Directory Discovery, Gather Victim Identity Information: Credentials, Gather Victim Identity Information: Employee Names, Hijack Execution Flow: DLL Search Order Hijacking, Hijack Execution Flow: DLL Side-Loading, Hijack Execution Flow: Dynamic Linker Hijacking, Impair Defenses: Indicator Blocking, Indicator Removal: Clear Windows Event Logs, Indicator Removal: Clear Command History, Indicator Removal: File Deletion, Ingress Tool Transfer, Input Capture: Keylogging, Lateral Tool Transfer, Masquerading: Masquerade Task or Service, Masquerading: Match Legitimate Name or Location, Modify Registry, Multi-Stage Channels, Network Service Discovery, Network Share Discovery, Obfuscated Files or Information, Software Packing, Obtain Capabilities: Tool, OS Credential Dumping: LSASS Memory, OS Credential Dumping: Security Account Manager, OS Credential Dumping: NTDS, Permission Groups Discovery, Phishing: Spearphishing Attachment, Pre-OS Boot: Bootkit, Process Injection, Proxy, Query Registry, Remote Services: Remote Desktop Protocol, Remote Services: SMB/Windows Admin Shares, Resource Hijacking, Rootkit, Scheduled Task/Job: Scheduled Task, Search Open Technical Databases: Scan Databases, Server Software Component: Web Shell, Subvert Trust Controls: Code Signing, Supply Chain Compromise: Compromise Software Supply Chain, System Binary Proxy Execution: Compiled HTML File, System Binary Proxy Execution: Rundll32, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Owner/User Discovery, System Services: Service Execution, Use Alternate Authentication Material: Pass the Hash, Valid Accounts, Web Service: Dead Drop Resolver, Windows Management Instrumentation
2. **Software used:** ASPXSpy, BITSAdmin, BLACKCOFFEE, certutil, China Chopper, Cobalt Strike, DEADEYE, Derusbi, dsquery, Empire, ftp, gh0st RAT, ipconfig, KEYPLUG, MESSAGETAP, Mimikatz, Net, netstat, njRAT, Ping, PlugX, PowerSploit, pwdump, ROCKBOOT, ShadowPad, sqlmap, Winnti for Linux, ZxShell

Procedures

APT41 gained access by attacking Air India's IT service provider during Operation ColunmTK and used the Cobalt Strike framework to move laterally. They maintained communication with C&C servers through DNS tunneling techniques and used Mimikatz to steal NTLM hashes and plaintext passwords.APT41 used the “BadPotato” tool to elevate local privileges and install persistent backdoors in the victim network. During the persistence phase, APT41 ensures its continued control by uploading malicious DLL files and disguising them as legitimate services, creating registry entries and scheduled tasks. Additionally, APT41 infiltrated multiple subnets within the network and successfully extracted hundreds of MB of data, suggesting that the attack may have impacted multiple airlines.APT41's attack methodology demonstrates their strong adaptability and persistent cyber espionage capabilities.