Chimera

Overview

Chimera is a suspected China-based threat group that has been active since at least 2018 targeting the semiconductor industry in Taiwan as well as data from the airline industry.[1][2]

Tactics

The Chimera APT's main goal is to steal intellectual property from Taiwan's semiconductor industry, and the main tactics it employs include remote access by virtue of legitimate accounts (T1078) and maintaining persistence through timed tasks (T1053.005). In addition, the organization evades detection by replacing legitimate applications with malware.

Techniques

Chimera primarily uses operating system credential dumps (T1003.003), scheduled task execution (T1053.005), command and script interpreters (T1059.001, T1059.003), and lateral movement with legitimate accounts (T1078). In addition, Chimera uses DLL hijacking (T1574.002) and disguising legitimate software names and locations (T1036.005) to hide its activities.

1. **Techniques Used:** Account Discovery: Local Account, Account Discovery: Domain Account, Application Layer Protocol: Web Protocols, Application Layer Protocol: DNS, Archive Collected Data: Archive via Utility, Automated Collection, Browser Information Discovery, Brute Force: Password Spraying, Brute Force: Credential Stuffing, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Windows Command Shell, Data from Information Repositories: Sharepoint, Data from Network Shared Drive, Data Staged: Local Data Staging, Data Staged: Remote Data Staging, Domain Trust Discovery, Email Collection: Local Email Collection, Email Collection: Remote Email Collection, Exfiltration Over C2 Channel, Exfiltration Over Web Service: Exfiltration to Cloud Storage, External Remote Services, File and Directory Discovery, Gather Victim Identity Information: Credentials, Hijack Execution Flow: DLL Side-Loading, Indicator Removal: Clear Windows Event Logs, Indicator Removal: File Deletion, Indicator Removal: Timestomp, Ingress Tool Transfer, Lateral Tool Transfer, Masquerading: Match Legitimate Name or Location, Modify Authentication Process: Domain Controller Authentication, Multi-Factor Authentication Interception, Native API, Network Service Discovery, Network Share Discovery, Obfuscated Files or Information: Command Obfuscation, Obtain Capabilities: Tool, OS Credential Dumping: NTDS, Password Policy Discovery, Permission Groups Discovery: Local Groups, Process Discovery, Protocol Tunneling, Query Registry, Remote Services: Remote Desktop Protocol, Remote Services: SMB/Windows Admin Shares, Remote Services: Windows Remote Management, Remote System

Discovery, Scheduled Task/Job: Scheduled Task, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Owner/User Discovery, System Service Discovery, System Services: Service Execution, System Time Discovery, Use Alternate Authentication Material: Pass the Hash, Valid Accounts, Domain Accounts, Windows Management Instrumentation

2. **Software used:** BloodHound, Cobalt Strike, esentutl, Mimikatz, Net, PsExec

Procedures

During the attack, Chimera APT maintains its persistence on infected systems by using legitimate accounts (T1078) for remote access and timed tasks (T1053.005). Its malware often masquerades as legitimate updaters such as GoogleUpdate.exe or Java Updater (T1036.005) in order to evade detection.Chimera performs data archiving through RAR tools (T1560.001) and uses filenames like RecordedTV.ms to disguise data exfiltration. Additionally, Chimera uses Cobalt Strike as a remote access Trojan (T1071.001) and persistence by hijacking the execution process (T1574.002).