BRONZE BUTLER

Overview

BRONZE BUTLER is a cyber espionage group with likely Chinese origins that has been active since at least 2008. The group primarily targets Japanese organizations, particularly those in government, biotechnology, electronics manufacturing, and industrial chemistry.[1][2][3]

Tactics

REDBALDKNIGHT (also known as BRONZE BUTLER) intrudes into targeted organizations, particularly corporations and government agencies located in Japan, through spear phishing (T1566), exploitation of known software vulnerabilities (T1203), and watering hole attacks (T1071.001). The main goal is to steal intellectual property and sensitive data, often spying for extended periods of time on areas such as critical infrastructure, heavy industry and manufacturing.

Techniques

The organization uses custom malware such as Daserf and xxmm to perform remote control (T1219), including downloading, uploading files, taking screenshots, and recording keystrokes. Additionally, Daserf uses steganography (T1027.003) to embed malicious code into image files to circumvent traditional security protections. The malware communicates with its C&C server via encrypted communication (T1573.001).

1. **Techniques Used:** Abuse Elevation Control Mechanism: Bypass User Account Control, Account Discovery: Domain Account, Application Layer Protocol: Web Protocols, Archive Collected Data: Archive via Utility, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Windows Command Shell, Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: Python, Data Encoding: Standard Encoding, Data from Local System, Data from Network Shared Drive, Deobfuscate/Decode Files or Information, Drive-by Compromise, Encrypted Channel: Symmetric Cryptography, Exploitation for Client Execution, File and Directory Discovery, Hijack Execution Flow: DLL Side-Loading, Impair Defenses: Disable or Modify Tools, Indicator Removal: File Deletion, Ingress Tool Transfer, Masquerading, Right-to-Left Override, Match Legitimate Name or Location, Obfuscated Files or Information: Binary Padding, Obfuscated Files or Information: Steganography, Obtain Capabilities: Tool, OS Credential Dumping: LSASS Memory, Phishing: Spearphishing Attachment, Remote System Discovery, Scheduled Task/Job: At, Scheduled Task/Job: Scheduled Task, Screen Capture, Software Discovery, System Service Discovery, System Time Discovery, Taint Shared Content, Use Alternate Authentication

Material: Pass the Ticket, User Execution: Malicious File, Web Service: Dead Drop Resolver

2. **Software used:** ABK, at, Avenger, BBK, build_downer, cmd, Daserf, down_new, gsecdump, Mimikatz, Net, schtasks, ShadowPad, Windows Credential Editor

Procedures

REDBALDKNIGHT first sends documents with exploits to the target via spear phishing emails, and once opened, Daserf or other malware is installed.Daserf connects to the compromised website and downloads image files embedded with malicious code, using steganography to hide its C&C communications. Its malware can use a variety of encryption algorithms (e.g., RC4 and Base64) to circumvent detection, as well as remote control features such as executing commands, file transfers, taking screenshots, and recording keystrokes. In addition, REDBALDKNIGHT deletes traces, maintains persistent access, and periodically accesses infected systems for data theft.