**MAPPING A CYBER ATTACK USING MITRE ATT&CK FRAMEWORK**

**Objective: To Use the MITRE ATT&CK framework to map out the tactics used in a recent cyber-attack.**

**Task: Identify and describe the relevant tactics, techniques, and procedures (TTPs).**

**Cybercriminals Use Excel Exploit to Spread Fileless Remcos RAT Malware.**

<https://thehackernews.com/2024/11/new-ymir-ransomware-exploits-memory-for.html>

|  |  |  |
| --- | --- | --- |
| **Tactics** | **Techniques** | **Procedures** |
| **Reconnaissance** | Phishing for information | Attackers use purchase order-themed lures to convince recipients to open a Microsoft Excel attachment |
| **Resource Development** | Develop Capability | Use of legitimate services like DocuSign (Abuse of legitimate services and tools) to deceive users into signing documents |
| **Initial Access** | Phishing | Phishing email contains an Excel attachment exploiting CVE-2017-0199 (RCE) to initiate malware download |
| **Execution** | -User execution  - Fileless execution | Exploiting remote code execution vulnerability (CVE-2017-0199). Malicious Excel document downloads and executes HTA file using mshta.exe to deploy payload.  Malicious HTA file is wrapped in obfuscated JavaScript, VBScript, and PowerShell, and runs directly in memory (fileless Remcos RAT) |
| **Persistence** | Compromised host software | Remcos RAT runs in memory without saving a file, potentially allowing for continued access |
| **Privilege Escalation** | Process injection | Malicious code uses process hollowing to inject Remcos RAT into the process memory |
| **Defense Evasion** | Obfuscation of files | Use of in-memory execution (fileless Remcos RAT), obfuscation through PowerShell, JavaScript, and VBScript.  - ZIP file concatenation to evade detection by different archive tools (7-Zip, WinRAR, Windows Explorer) |
| **Credential Access** | Exploitation for credential access | Use of Remcos RAT to remotely control the compromised system and harvest information. |
| **Discovery** | System information discovery and data collection | Remcos RAT enumerates system metadata, processes, and gathers clipboard content, and other sensitive information |
| **Lateral Movement** | Remote services | Remcos RAT has capabilities for network operations and could facilitate lateral movement in a network |
| **Collection** | Input capture | Remcos RAT collects files, enumerates processes, and gathers clipboard data |
| **Command and Control** | Remote access software | Remcos RAT communicates with a C2 server to receive commands and exfiltrate data |
| **Exfiltration** | File exfiltration over webservice | Exfiltration of collected files and data to the remote C2 server |
| **Impact** | -Data manipulation  -Financial Theft | Remcos RAT can alter system functionality, disable keyboard/mouse input, and even record the screen or enable the camera/microphone.  The use of genuine DocuSign accounts and templates to impersonate reputable companies, catching users and security tools off guard |

*Table showing the use of Mitre Frame work to analyze a recent cyber-attack.*