User Execution

Sub-techniques (3)

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of Phishing.

While User Execution frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after Internal Spearphishing.

Adversaries may also deceive users into performing actions such as:

- Enabling Remote Access Software, allowing direct control of the system to the adversary
- Running malicious JavaScript in their browser, allowing adversaries to Steal Web Session Cookies[1][2]
- Downloading and executing malware for User Execution
- Coerceing users to copy, paste, and execute malicious code manually[3][4]

For example, tech support scams can be facilitated through Phishing, vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or Remote Access Software.[5]

ID: T1204

Sub-techniques: T1204.001, T1204.002, T1204.003

Tactic: Execution

Platforms: Containers, IaaS, Linux, Windows, macOS

Contributors: Ale Houspanossian; Fernando Bacchin; Harikrishnan Muthu, Cyble; Menachem Goldstein; Oleg Skulkin, Group-IB; ReliaQuest

Version: 1.7

Created: 18 April 2018

Last Modified: 11 November 2024

Version Permalink

Procedure Examples

ID	Name	Description
G1004	LAPSUS$	LAPSUS$ has recruited target organization employees or contractors who provide credentials and approve an associated MFA prompt, or install remote management software onto a corporate workstation, allowing LAPSUS$ to take control of an authenticated system.[6]
S1130	Raspberry Robin	Raspberry Robin execution can rely on users directly interacting with malicious LNK files.[7]
G1015	Scattered Spider	Scattered Spider has impersonated organization IT and helpdesk staff to instruct victims to execute commercial remote access tools to gain initial access.[8]
C0037	Water Curupira Pikabot Distribution	Water Curupira Pikabot Distribution requires users to interact with malicious attachments in order to start Pikabot installation.[9]

Mitigations

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent executable files from running unless they meet a prevalence, age, or trusted list criteria and to prevent Office applications from creating potentially malicious executable content by blocking malicious code from being written to disk. Note: cloud-delivered protection must be enabled to use certain rules. [10]
M1038	Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
M1031	Network Intrusion Prevention	If a link is being visited by a user, network intrusion prevention systems and systems designed to scan and remove malicious downloads can be used to block activity.
M1021	Restrict Web-Based Content	If a link is being visited by a user, block unknown or unused files in transit by default that should not be downloaded or by policy from suspicious sites as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some download scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious files.
M1017	User Training	Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events.

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor logs from applications to detect user-initiated actions such as opening malicious documents, clicking on phishing links, or executing downloaded malware. Analytic 1 - Logs showing unexpected user actions triggering unusual processes. `sourcetype=application_log EventCode=1000 OR EventCode=1001| search application IN ("winword.exe", "excel.exe", "chrome.exe", "firefox.exe", "adobe.exe", "zip.exe")| stats count by application event_description| where event_description IN ("opened document", "clicked link", "executed file")`
DS0017	Command	Command Execution	Detect commands triggered by users, especially related to decompression tools (e.g., zip files) that may unpack malicious payloads. This includes compression applications, such as those for zip files, that can be used to Deobfuscate/Decode Files or Information in payloads. Analytic 1 - Command lines showing decompression or decoding actions. `sourcetype=WinEventLog:Powershell EventCode=4104| search process_name IN ("powershell.exe", "cmd.exe", "zip.exe", "winrar.exe")| stats count by process_name command_line user| where command_line LIKE "%unzip%" OR command_line LIKE "%decode%"`
DS0032	Container	Container Creation	Monitor for newly constructed containers that may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Analytic 1 - Containers communicating with unexpected external services. `sourcetype=container_creation OR sourcetype=container_start| stats count by container_name event_description user| where container_name NOT IN ("") AND event_description IN ("created", "started")`
		Container Start	Monitor for the activation or invocation of a container (ex: docker start or docker restart)
DS0022	File	File Creation	Anti-virus can potentially detect malicious documents and files that are downloaded and executed on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the file is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning powershell.exe).
DS0007	Image	Image Creation	Monitor for newly constructed image that may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel.
DS0030	Instance	Instance Creation	Monitor for newly constructed instances that may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel.
		Instance Start	Monitor for the activation or invocation of an instance (ex: instance.start within GCP Audit Logs)
DS0029	Network Traffic	Network Connection Creation	Monitor network traffic patterns associated with web-based user actions, such as clicking on phishing links or executing malware that tries to establish C2 communication. Analytic 1 - Web-based network connections to suspicious destinations. `sourcetype=sysmon EventCode=3| search process_name IN ("winword.exe", "chrome.exe", "firefox.exe") | stats count by src_ip dest_ip dest_port process_name| where dest_ip NOT IN ("")`

ID	Data Source	Data Component	Detects
		Network Traffic Content	Monitor and analyze traffic patterns and packet inspection associated with web-based network connections that are sent to malicious or suspicious detinations (e.g. destinations attributed to phishing campaigns). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments (e.g. monitor anomalies in use of files that do not normally initiate network connections or unusual connections initiated by regsvr32.exe, rundll.exe, .SCF, HTA, MSI, DLLs, or msiexec.exe).
DS0009	Process	Process Creation	Identify processes spawned by user actions, especially from Office documents, PDFs, or web browsers that could lead to malicious execution. Analytic 1 - Processes created from user interaction with files. `((sourcetype=WinEventLog:Security EventCode=4688) OR (sourcetype=Sysmon EventCode=1))| search parent_process IN ("winword.exe", "excel.exe", "chrome.exe", "firefox.exe")| stats count by parent_process process_name command_line user| where process_name NOT IN ("chrome.exe", "firefox.exe", "winword.exe", "excel.exe")`

References

1. Tiago Pereira. (2023, November 2). Attackers use JavaScript URLs, API forms and more to scam users in popular online game “Roblox”. Retrieved January 2, 2024.
2. Brian Krebs. (2023, May 30). Discord Admins Hacked by Malicious Bookmarks. Retrieved January 2, 2024.
3. Reliaquest. (2024, May 31). New Execution Technique in ClearFake Campaign. Retrieved August 2, 2024.
4. Tommy Madjar, Dusty Miller, Selena Larson. (2024, June 17). From Clipboard to Compromise: A PowerShell Self-Pwn. Retrieved August 2, 2024.
5. Selena Larson, Sam Scholten, Timothy Kromphardt. (2021, November 4). Caught Beneath the Landline: A 411 on Telephone Oriented Attack Delivery. Retrieved January 5, 2022.
6. MSTIC, DART, M365 Defender. (2022, March 24). DEV-0537 Criminal Actor Targeting Organizations for Data Exfiltration and Destruction. Retrieved May 17, 2022.
7. Microsoft Threat Intelligence. (2022, October 27). Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity. Retrieved May 17, 2024.
8. CISA. (2023, November 16). Cybersecurity Advisory: Scattered Spider (AA23-320A). Retrieved March 18, 2024.
9. Shinji Robert Arasawa, Joshua Aquino, Charles Steven Derion, Juhn Emmanuel Atanque, Francisrey Joshua Castillo, John Carlo Marquez, Henry Salcedo, John Rainier Navato, Arianne Dela Cruz, Raymart Yambot & Ian Kenefick. (2024, January 9). Black Basta-Affiliated Water Curupira’s Pikabot Spam Campaign. Retrieved July 17, 2024.
10. Microsoft. (2021, July 2). Use attack surface reduction rules to prevent malware infection. Retrieved June 24, 2021.