Event Triggered Execution

Sub-techniques (17)

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events.[1][2][3]

Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked.[4][5][6]

Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.

ID: T1546

Sub-techniques: T1546.001, T1546.002, T1546.003, T1546.004, T1546.005, T1546.006, T1546.007, T1546.008, T1546.009, T1546.010, T1546.011, T1546.012, T1546.013, T1546.014, T1546.015, T1546.016, T1546.017

ⓘ

Tactics: Privilege Escalation, Persistence

ⓘ

Platforms: IaaS, Linux, Office Suite, SaaS, Windows, macOS

Version: 1.4

Created: 22 January 2020

Last Modified: 15 October 2024

Version Permalink

Procedure Examples

ID	Name	Description
C0035	KV Botnet Activity	KV Botnet Activity involves managing events on victim systems via `libevent` to execute a callback function when any running process contains the following references in their path without also having a reference to `bioset`: busybox, wget, curl, tftp, telnetd, or lua. If the `bioset` string is not found, the related process is terminated.[7]
S1091	Pacu	Pacu can set up S3 bucket notifications to trigger a malicious Lambda function when a CloudFormation template is uploaded to the bucket. It can also create Lambda functions that trigger upon the creation of users, roles, and groups.[8]

Mitigations

ID	Mitigation	Description
M1026	Privileged Account Management	Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.
M1051	Update Software	Perform regular software updates to mitigate exploitation risk.

Detection

ID	Data Source	Data Component	Detects
DS0025	Cloud Service	Cloud Service Modification	Monitor the creation and modification of cloud resources that may be abused for persistence, such as functions and workflows monitoring cloud events.
DS0017	Command	Command Execution	Monitor executed commands and arguments that may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.
DS0022	File	File Creation	Monitor newly constructed files that may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.
		File Metadata	Monitor for contextual data about a file, which may include information such as name, the content (ex: signature, headers, or data/media), user/owner, permissions, etc.
		File Modification	Monitor for changes made to files that may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.
DS0011	Module	Module Load	Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not normally loaded into a process. Look for abnormal process behavior that may be due to a process loading a malicious DLL. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as making network connections for Command and Control, learning details about the environment through Discovery, and conducting Lateral Movement.
DS0009	Process	Process Creation	Tools such as Sysinternals Autoruns can be used to detect changes to execution triggers that could be attempts at persistence. Also look for abnormal process call trees for execution of other commands that could relate to Discovery actions or other techniques.
DS0024	Windows Registry	Windows Registry Key Modification	Monitor for changes made to windows registry keys and/or values that may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.
DS0005	WMI	WMI Creation	Monitor for newly constructed WMI Objects that may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.

References

1. Daniel Grzelak. (2016, July 9). Backdooring an AWS account. Retrieved May 27, 2022.
2. Eric Saraga. (2022, February 2). Using Power Automate for Covert Data Exfiltration in Microsoft 365. Retrieved May 27, 2022.
3. Berk Veral. (2020, March 9). Real-life cybercrime stories from DART, the Microsoft Detection and Response Team. Retrieved May 27, 2022.
4. Ballenthin, W., et al. (2015). Windows Management Instrumentation (WMI) Offense, Defense, and Forensics. Retrieved March 30, 2016.
5. Patrick Wardle. (2015). Malware Persistence on OS X Yosemite. Retrieved July 10, 2017.
6. Claud Xiao, Cong Zheng, Yanhui Jia. (2017, April 6). New IoT/Linux Malware Targets DVRs, Forms Botnet. Retrieved February 19, 2018.
7. Black Lotus Labs. (2023, December 13). Routers Roasting On An Open Firewall: The KV-Botnet Investigation. Retrieved June 10, 2024.
8. Rhino Security Labs. (2019, August 22). Pacu. Retrieved October 17, 2019.