# Boot or Logon Initialization Scripts

## Sub-techniques (5)

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence.[1][2] Initialization scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server. These scripts can vary based on operating system and whether applied locally or remotely.

Adversaries may use these scripts to maintain persistence on a single system. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

An adversary may also be able to escalate their privileges since some boot or logon initialization scripts run with higher privileges.

ID: T1037

Sub-techniques: T1037.001, T1037.002, T1037.003, T1037.004, T1037.005

Tactics: Persistence, Privilege Escalation

Platforms: Linux, Network, Windows, macOS

Version: 2.3

Created: 31 May 2017

Last Modified: 16 April 2024

Version Permalink

## Procedure Examples

| ID | Name | Description |
|---|---|---|
| G0016 | APT29 | APT29 has hijacked legitimate application-specific startup scripts to enable malware to execute on system startup.[1] |
| G0096 | APT41 | APT41 used a hidden shell script in `/etc/rc.d/init.d` to leverage the `ADORE.XSEC` backdoor and `Adore-NG` rootkit.[3] |
| G0106 | Rocke | Rocke has installed an "init.d" startup script to maintain persistence.[2] |
| S1078 | RotaJakiro | Depending on the Linux distribution and when executing with root permissions, RotaJakiro may install persistence using a `.conf` file in the `/etc/init/` folder.[4] |

## Mitigations

| ID | Mitigation | Description |
|---|---|---|
| M1022 | Restrict File and Directory Permissions | Restrict write access to logon scripts to specific administrators. |
| M1024 | Restrict Registry Permissions | Ensure proper permissions are set for Registry hives to prevent users from modifying keys for logon scripts that may lead to persistence. |

# Detection

| ID | Data Source | Data Component | Detects |
|---|---|---|---|
| DS0026 | Active Directory | Active Directory Object Modification | Monitor for changes made in the Active Directory that may use scripts automatically executed at boot or logon initialization to establish persistence. |
| DS0017 | Command | Command Execution | Monitor executed commands and arguments that may consist of logon scripts for unusual access by abnormal users or at abnormal times. |
| DS0022 | File | File Creation | Monitor for newly constructed files that may use scripts automatically executed at boot or logon initialization to establish persistence. |
| | | File Modification | Monitor for changes made to files that are modified by unusual accounts outside of normal administration duties. |
| DS0009 | Process | Process Creation | Monitor for newly executed processes that may use scripts automatically executed at boot or logon initialization to establish persistence. Adversaries may schedule software to run whenever a user logs into the system; this is done to establish persistence and sometimes for lateral movement. This trigger is established through the registry key `HKEY_CURRENT_USER\Environment\UserInitMprLogonScript`. This signature looks edits to existing keys or creation of new keys in that path. Users purposefully adding benign scripts to this path will result in false positives; that case is rare, however. There are other ways of running a script at startup or login that are not covered in this signature. Note that this signature overlaps with the Windows Sysinternals Autoruns tool, which would also show changes to this registry path.<br><br>Analytic 1 - Boot or Logon Initialization Scripts<br><br>`(source="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode="1") OR (source="WinEventLog:Security" EventCode="4688") AND CommandLine="regadd\EnvironmentUserInitMprLogonScript"` |
| DS0024 | Windows Registry | Windows Registry Key Creation | Monitor for newly constructed windows registry keys that may use scripts automatically executed at boot or logon initialization to establish persistence. |

# References


1. Mandiant. (2022, May 2). UNC3524: Eye Spy on Your Email. Retrieved August 17, 2023.
2. Anomali Labs. (2019, March 15). Rocke Evolves Its Arsenal With a New Malware Family Written in Golang. Retrieved April 24, 2019.
3. Mandiant. (n.d.). APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION. Retrieved June 11, 2024.
4. Alex Turing, Hui Wang. (2021, April 28). RotaJakiro: A long live secret backdoor with 0 VT detection. Retrieved June 14, 2023.