Sign in

redcanaryco / **atomic-red-team** Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 4 Actions Wiki Security Insights

atomic-red-team / atomics / T1553.001 / **T1553.001.md**

Atomic Red Team doc generat... Generated docs from job=generate-docs branch=master [ci ... b1f3c96 · last year

56 lines (26 loc) · 3.47 KB

Preview Code Blame Raw

T1553.001 - Subvert Trust Controls: Gatekeeper Bypass

Description from ATT&CK

> Adversaries may modify file attributes and subvert Gatekeeper functionality to evade user prompts and execute untrusted programs. Gatekeeper is a set of technologies that act as layer of Apple's security model to ensure only trusted applications are executed on a host. Gatekeeper was built on top of File Quarantine in Snow Leopard (10.6, 2009) and has grown to include Code Signing, security policy compliance, Notarization, and more. Gatekeeper also treats applications running for the first time differently than reopened applications.(Citation: TheEclecticLightCompany Quarantine and the flag)(Citation: TheEclecticLightCompany apple notarization)
> Based on an opt-in system, when files are downloaded an extended attribute (xattr) called `com.apple.quarantine` (also known as a quarantine flag) can be set on the file by the application performing the download. Launch Services opens the application in a suspended state. For first run applications with the quarantine flag set, Gatekeeper executes the following functions:

> 1. Checks extended attribute – Gatekeeper checks for the quarantine flag, then provides an alert prompt to the user to allow or deny execution.(Citation: OceanLotus for OS X)(Citation: 20 macOS Common Tools and Techniques)
>
> 2. Checks System Policies - Gatekeeper checks the system security policy, allowing execution of apps downloaded from either just the App Store or the App Store and identified developers.
>
> 3. Code Signing – Gatekeeper checks for a valid code signature from an Apple Developer ID.
>
> 4. Notarization - Using the `api.apple-cloudkit.com` API, Gatekeeper reaches out to Apple servers to verify or pull down the notarization ticket and ensure the ticket is not revoked. Users can override notarization, which will result in a prompt of executing an “unauthorized app” and the security policy will be modified.
>
> Adversaries can subvert one or multiple security controls within Gatekeeper checks through logic errors (e.g. Exploitation for Defense Evasion), unchecked file types, and external libraries. For example, prior to macOS 13 Ventura, code signing and notarization checks were only conducted on first launch, allowing adversaries to write malicious executables to previously opened applications in order to bypass Gatekeeper security checks.(Citation: theevilbit gatekeeper bypass 2021)(Citation: Application Bundle Manipulation Brandon Dalton)
>
> Applications and files loaded onto the system from a USB flash drive, optical disk, external hard drive, from a drive shared over the local network, or using the curl command may not set the quarantine flag. Additionally, it is possible to avoid setting the quarantine flag using Drive-by Compromise.

Atomic Tests

- Atomic Test #1 - Gatekeeper Bypass

Atomic Test #1 - Gatekeeper Bypass

Gatekeeper Bypass via command line

Supported Platforms: macOS

auto_generated_guid: fb3d46c6-9480-4803-8d7d-ce676e1f1a9b

Inputs:

Name	Description	Type	Default Value
app_path	Path to app to be used	path	myapp.app

Attack Commands: Run with `sh`! Elevation Required (e.g. root or admin)

```
sudo xattr -d com.apple.quarantine #{app_path}
```