S

Silver Sparrow Malware on Mac: Facts, Detection, and Removal

Silver Sparrow was a 2021 macOS downloader found on Intel and M1 Macs. Learn the confirmed facts, how to interpret a present-day detection, and what to check.

PUBLISHER
Gridinsoft Support

UPDATED
Aug 28, 2026

READ TIME
4 min

Silver Sparrow is the name researchers gave to a macOS downloader discovered in February 2021. Two installer variants were observed: one targeting Intel Macs and another containing code compiled for Apple's then-new M1 architecture. The malware used JavaScript inside signed `.pkg` installers, created LaunchAgent persistence, and contacted cloud-hosted infrastructure.

The most important historical fact is often missed: researchers did not observe Silver Sparrow deliver its intended final payload during the original investigation. That does not make the installer harmless—it could run code and fetch additional content—but claims that it definitely stole passwords, recorded cameras, or performed some other specific final action are not supported by the original evidence.

How Silver Sparrow worked

- Victims encountered installer packages with names such as `update.pkg` or `updater.pkg`.
- Installer JavaScript executed during the installation workflow, potentially before the user expected the visible installation to finish.
- The installer placed scripts and a LaunchAgent property-list file in the user's Library to run periodically.
- The agent contacted infrastructure hosted on public cloud services and checked for more instructions.
- A self-removal mechanism was also observed, although researchers did not see it activated.

Red Canary documented the original technical findings and Malwarebytes reported detections across many countries. Apple revoked the developer certificates used to sign the packages, limiting further installation of those known samples.

What a Silver Sparrow detection means today

A present-day alert may identify an old installer in Downloads, a backup, an archived disk image, or a remaining LaunchAgent artifact. It does not by itself prove that the 2021 infrastructure is active or that the Mac currently has a live connection. Read the detection path, timestamp, quarantine status, and process activity.

It may also be a generic or heuristic detection that a vendor maps to the Silver Sparrow family. Confirm the exact security product, detection name, hash, and file path before relying on old indicator lists. Cloud-hosting domains and common filenames are not safe to block or delete broadly because legitimate software may use them.

What to do if Silver Sparrow is detected

1. **Update macOS and security definitions.** Built-in protections such as Gatekeeper and XProtect improve through system security updates.
2. **Quarantine with a current security scanner.** Scan the complete Mac, not only the detected package, to find persistence or an unrelated secondary payload.

3. **Inspect the detection location.** If it is an unopened old installer, remove it and empty Trash after quarantine. If it is an active process or LaunchAgent, disconnect from networks while investigating.

4. **Review persistence.** Check Login Items, browser extensions, configuration profiles, and user LaunchAgents for unfamiliar entries created at the same time. Do not delete random files from `/System` or `/Library`; ask an administrator or security professional when ownership is unclear.

5. **Review the source.** Remove the application or installer that introduced the artifact and any unexpected software installed with it.

When to reset passwords or reinstall macOS

Reset credentials from a clean device if investigation finds an additional payload, an unknown installer actually ran, browser or credential data may have been accessed, or suspicious account sessions appear. Revoke active sessions and check email, Apple Account, password-manager, financial, and work accounts.

Erase and reinstall macOS when administrator-level unauthorized software ran, security controls were altered, unknown payloads remain, or you cannot establish what happened. Restore personal documents from a backup made before the incident and reinstall applications from trusted sources rather than restoring questionable executables or packages.

How to reduce Mac malware risk

- Install applications from the App Store or the publisher's official site.
- Do not bypass Gatekeeper for an unexpected update, crack, or “required” media plugin.
- Read installer prompts and verify the developer before entering an administrator password.
- Keep macOS, browsers, and applications updated and retain versioned backups.
- Review Login Items, profiles, and browser extensions after installing unfamiliar software.

Silver Sparrow FAQ

Was Silver Sparrow the first M1 malware?

It was among the earliest widely reported malware families with a native M1 build, but “first” depends on definitions and discovery dates.

Does a 2026 alert mean the campaign returned?

No. A detection can be a dormant or archived artifact. Active process, network, and persistence evidence is needed before making that conclusion.

Can I remove it manually?

A current scanner is safer because paths and related payloads can vary. Manual cleanup should be based on verified artifacts, not copied filename lists.

See the original analyses from Red Canary and Malwarebytes for the confirmed 2021 findings.