

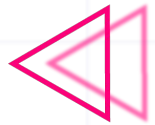
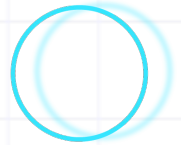
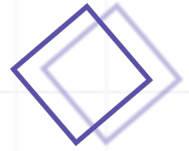


Quarantine nights

Exploring File Quarantine handling in macOS Apps / @Metnëw 🐱

Quarantine Nights

- What is macOS **File Quarantine**? 🤔
- **Payloadable** macOS-recognized files ✂️
- Quarantine in **messengers** 💬
- Quarantine in **cloud file storages** 📁
- Summary 💀



Who am I?

- AppSec@Grammarly
- twitter.com/vladimir_metnew
- Hackerone.com/Metnew, Grammarly(#1), MacPaw(#1), Brave(#1)...
- Focus: code analysis, *macOS*, browser environments.

5.52

Signal

91st

Percentile

27.07

Impact

97th

Percentile

2458

Reputation



Rank



What is File Quarantine?

Why is there so much hype around Gatekeeper?



localhost:5000



[File with malicious payload](#)

macOS File Quarantine

- **Quarantine** prevents downloaded content from being launched without the user's explicit confirmation.
- **Gatekeeper** enforces code signing and verifies downloaded applications before allowing them to run.
- **Gatekeeper** relies on the **com.apple.quarantine** extended file attribute that Quarantine attaches to downloaded files.
- Windows clone: **MOTW** (Mark-Of-The-Web).
- Default for files written by **App Sandboxed apps**

macOS File Quarantine: references

- File Quarantine is explained in-depth in “[*OS Internals III](#)” by *Jonathan Levin*.
- Check *@patrickwardle*'s research on [GateKeeper bypasses](#).
- WWDC2019 [“Advances in macOS Security”](#).
- [“Grokking Gatekeeper in Catalina”](#) by *@howardnoakley*.
- Gatekeeper bypass is a [MITRE ATT&CK technique](#).

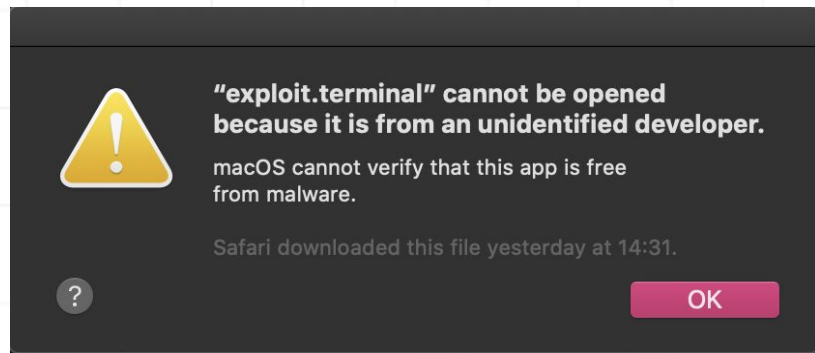
Quarantine (file downloading)

1. The app downloads a file from a **remote** resource.
2. The app can “quarantine” the file directly by adding **com.apple.quarantine** extended attribute via **xattr** util or **<sys/xattr.h>**.
3. It can also “quarantine” files indirectly by delegating the quarantine process to OS, which requires setting the **LSFileQuarantineEnabled** property to **<false/>** in *Info.plist*.

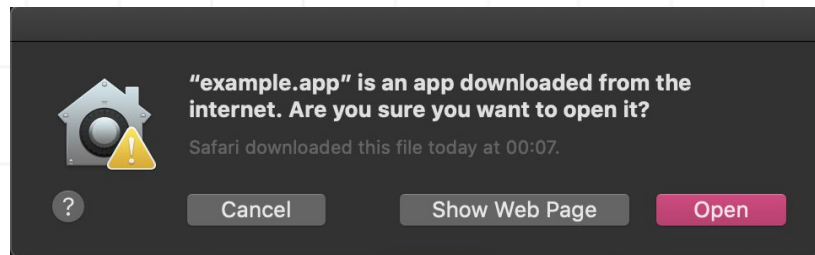
```
o xattr ./example.app  
com.apple.quarantine
```


Quarantine (file launching)

1. OS checks **com.apple.quarantine** attribute once the file is launched via **LaunchServices**.
2. **If enabled**, Gatekeeper runs codesign check, notarization check and malware scan.
3. Depending on the user's Gatekeeper settings, macOS might prevent the file from launching.
4. **[Gatekeeper:3rd-party]** If the app is signed with a 3rd-party developer certificate and the user allows it to open, the Quarantine dialog pops up.



Gatekeeper alert



Quarantine dialog

Imagine there was no Quarantine 🤔

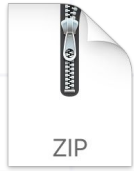
- Any downloaded file could be launched in a single `open(1)`.
- OS wouldn't enforce codesign requirements for executables.
- There would be no OS protection against malware.
- Websites would be able to execute arbitrary code via Windshift APT's [trick with app URI schemes](#).



Payload all the things!

A short guide to “payloadable” macOS files

Files that can include other files



<code>.zip</code> , <code>.bin</code> , <code>.tar</code> , <code>.tgz</code> , and 17 other archive file types	File archives can include files.
<code>.dmg</code> , <code>.cdr</code> , <code>.dart</code> , <code>.dc42</code> , and 11 other disk image file types	Disk Images can include files.
<code>.pkg</code> and <code>.mpkg</code>	Package installers can include files and <u>can execute code.</u>

You can find a full list of file extensions in Chromium project:

src/chrome/browser/resources/safe_browsing/download_file_types.asciipb

Harmful macOS files

.app	App(bundle) is a directory ; it needs +x file permission to launch.
.webarchive	2000day : This file can cause UXSS in Safari; it can't be signed.
.action, .caction, .workflow, .wflow	Automator actions don't need +x to launch. Automator UI pops up on launch :(
.tool, .command, .dylib	Terminal.app is a default handler; These files need +x permission to launch :(
.terminal (✓)	Terminal.app preferences file; allows running code, XML file (plist); it can't be signed .
.internetconnect, .networkconnect, .configprofile...	Configuration profiles can modify device settings. The user's explicit confirmation is required .

.terminal file

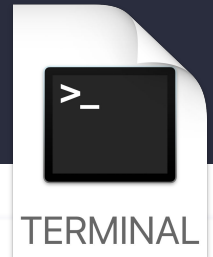
- Terminal.app profile configuration file.
- **.terminal** can't be signed, but signing isn't a concern, if it has already bypassed Quarantine.
- It's a plist. It could be delivered in both binary and XML formats.
- **.terminal** can launch an invisible Terminal.app window.
- Bypasses notarization check.

```
1 bplist00
2 _ RunCommandAsShell_ProfileCurrentVersion]CommandStringNameTtType#a0z0G0
  {_ echo "Hello" && id;Wexploit_Window Settings '?'
   MRWXaw000000 0000000 0000000000000000
```

Binary .terminal

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
  PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5   <key>CommandString</key>
6   <string>echo "Hello" &amp;&amp; id;</string>
7   <key>ProfileCurrentVersion</key>
8   <real>2.0600000000000001</real>
9   <key>RunCommandAsShell</key>
10  <false/>
11  <key>name</key>
12  <string>exploit</string>
13  <key>type</key>
14  <string>Window Settings</string>
15 </dict>
16 </plist>
17
```

XML .terminal





Quarantine in Messengers

Messengers from AppStore = ❤️

Messengers and UX Security

- Unsafe UX: many apps have an “Open” functionality that is implemented via **NSWorkspace.open** with no safety checks.
- Unsafe UX: apps don't have file preview for non-image files. **.terminal** files in binary format can bypass text previews.
- Unsafe UX: apps might download files without the user's consent.
- Filename-spoofing bugs (e.g., CVE-2019-3571 WhatsApp)

metnew

Metnew

All Threads

Channels

c2-server

general

random

x

+ Add a channel

Direct Messages

slackbot

Metnew (you)

+ Invite people

Apps

recon

Slack Developer Tools

#general

☆ | 👤 1 | 🔔 0 | Company-wide announcements and work-based matters

general

You created this channel on December 3rd. This is the very beginning of the # general channel. Purpose: This channel is for workspace-wide communication and announcements. All members are in this channel. ([edit](#))

+ Add an app [Invite others to this channel](#)

Monday, December 3rd



Metnew 5:59 AM

joined #general.



Metnew 5:59 AM

Woohoo!

Today



Metnew 6:33 PM

exploit.terminal

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//
  "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5   <key>CommandString</key>
6   <string>echo "Hello" &id;&id;</string>
7   <key>ProfileCurrentVersion</key>
8   <real>2.0600000000000001</real>
9   <key>RunCommandAsShell</key>
10  <false/>
11  <key>name</key>
12  <string>exploit</string>
13  <key>type</key>
14  <string>Window Settings</string>
15 </dict>
16 </plist>
17

```

Collapse ↑



Message #general



Downloads



exploit.terminal

Hold **Shift** to open the file.

Slack

- **21 Dec 2018** — The vulnerability was reported to Slack on HackerOne.
- **13 June 2019** — Triaged with “High” severity.
- **16 Aug 2019** — The vulnerability was fixed.
- It took Slack **235 days** to fix this vulnerability.





Quarantine
Вы

Батарея почти разряжена
Зарядите свой телефон, чтобы продолжить использование WhatsApp

Поиск или новый чат

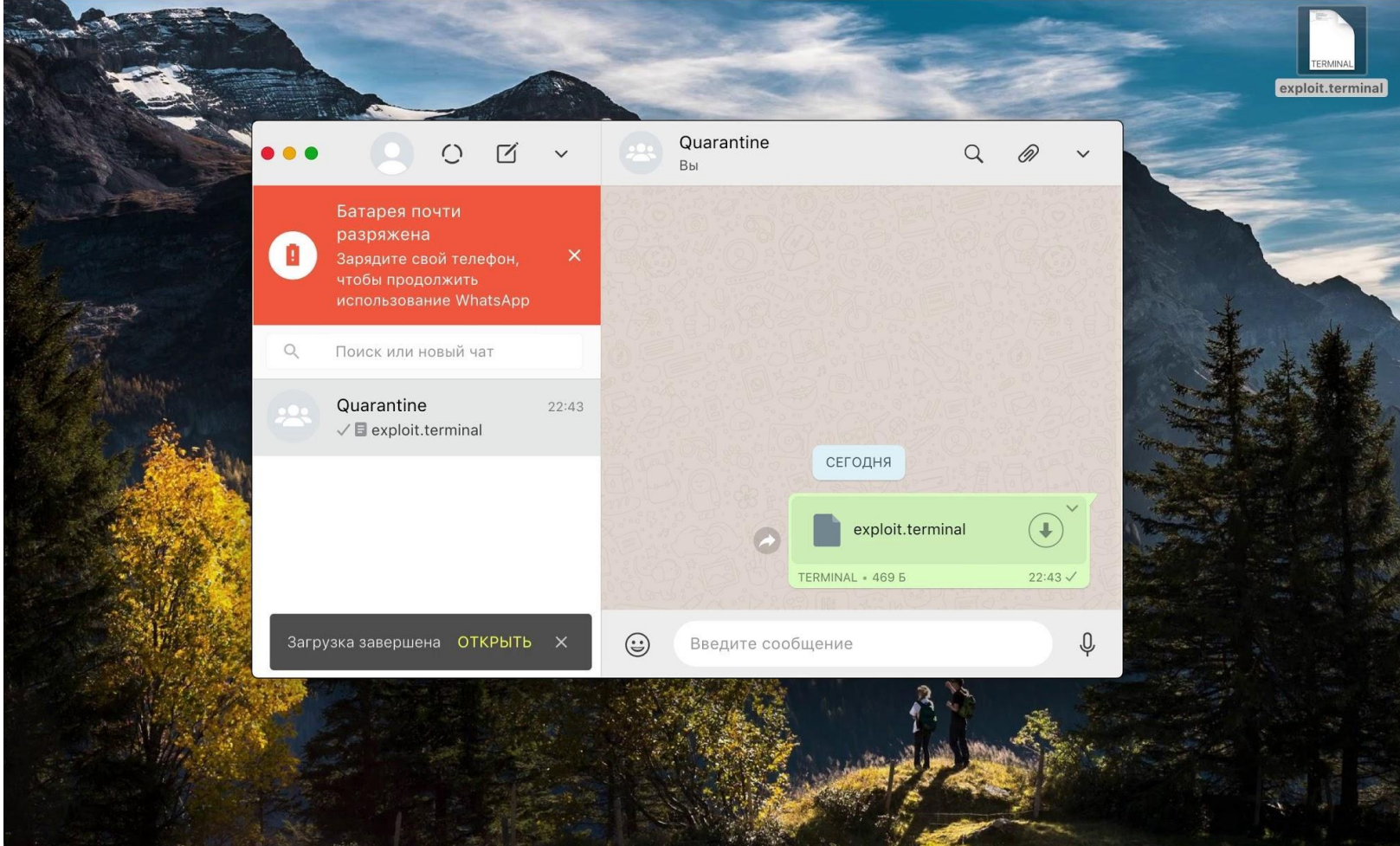
Quarantine 22:43
✓ exploit.terminal

СЕГОДНЯ

exploit.terminal
TERMINAL • 469 Б 22:43 ✓

Загрузка завершена **ОТКРЫТЬ**

Введите сообщение



WhatsApp

- **30 Oct 2018** — The vulnerability was reported to FB.
- **11 Jan 2019** — The WhatsApp Team confirmed that the issue had been resolved.
- The WhatsApp team **doesn't consider** this issue to be a vulnerability but rather a platform-specific behavior.



WhatsApp: File extension spoofing



Nico Waisman
@nicowaisman

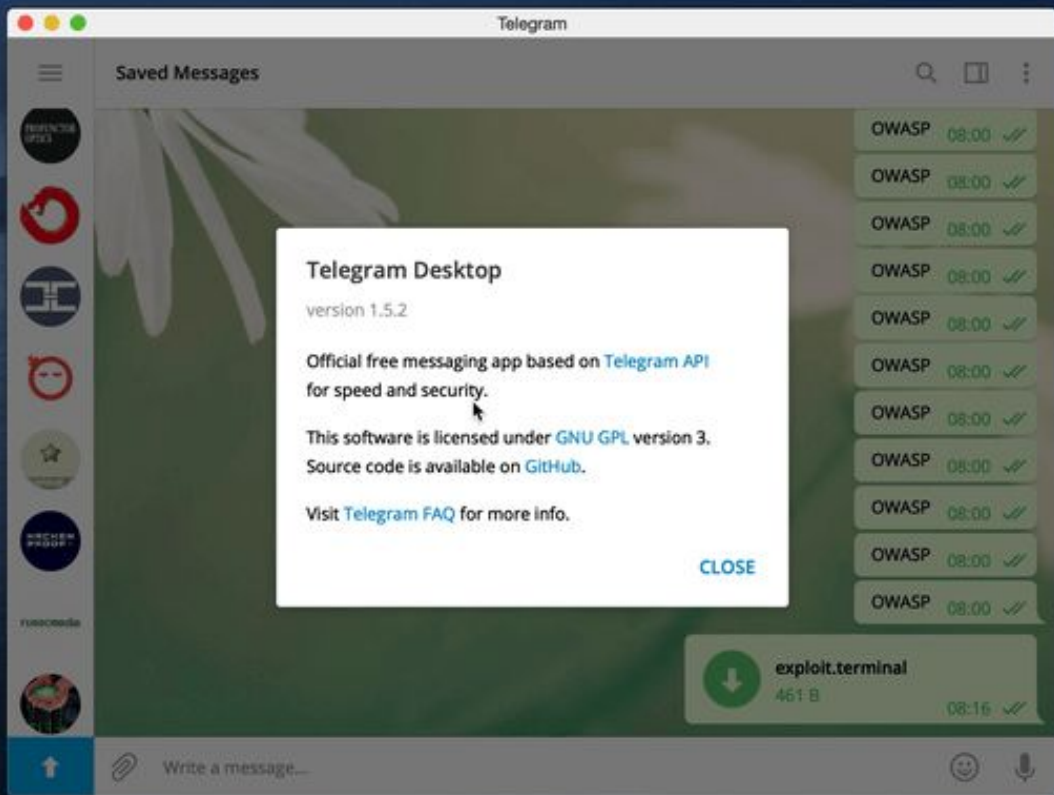


CVE of the day: CVE-2019-3571

An input validation issue affected WhatsApp Desktop versions prior to 0.3.3793 which allows malicious clients to send files to users that would be displayed with a wrong extension.



Imagine the potential impact from combining a filename spoofing bug with the lack of Quarantine.



Telegram

- **18 Dec 2018** — The issue was reported to security@telegram.com.
- **21 Jan 2019** — Telegram (v1.5.8) fixed the issue by requiring a user's consent to open **.terminal** files.
- **29 Jan 2019** — I provided additional file extensions that should be filtered.
- **Later** — Telegram enabled macOS File Quarantine.



Telegram: imagine if I hadn't reported this bug

v1.5.8 includes an “*auto-downloading*”
feature: the app downloads files
without the user's consent, making
the Quarantine issue a **single-click**
code execution.

v 1.5.8



john-preston released this on 21 Jan

- Global permissions for groups. Restrict all members in a
- Unified group settings. Make groups public, set admins v
history in just a few clicks in any group.
- Choose the emoji set you would like to use in Chat Settir
- Choose input and output devices for Telegram Calls in S
- Support for automatically downloading files and music.

Skype interface sidebar containing search, contact list, and navigation icons.

M_ [notification] [profile] [refresh] [more]

Q Search Skype +

Time ▾

- quarantine** 09:50
Metnew ___ has renamed the...
- Skype Translator** 09:50
Alternatively, you can create a ...
- Echo / Sound Test Service**

Skype chat window for "quarantine" with 1 participant and gallery view.

quarantine
1 participant | Gallery

Today

Today

Metnew ___ has made the chat history visible to everyone

Metnew ___ joined this conversation

Metnew ___ has renamed the conversation to "quarantine"

[Invite More People](#)

< [emojis] Type a message here [video] [image] [location] [share] [add]

Terminal window titled "exploit.terminal" with a cursor.

TERMINAL
exploit.terminal

Skype

- **23 Dec 2019** — I sent a report to *security@ mail*, but MS didn't have a *security@* alias 🙄
- **22 Jan 2019** — The bug is reported to *secure@*.
- **24 Jan 2019** — MS confirms the bug.
- **Later** — The bug is silently fixed; no updates from MS, no HoF.



Security [Signal for macOS]: Lack of quarantine meta-attribute for downloaded files leads to GateKeeper bypass #3590

Edit New issue

Open Metnew opened this issue on 12 Sep · 2 comments



Metnew commented on 12 Sep

+ 😊 ...

Bug Description

Report to Brave: <https://hackerone.com/reports/374106>

1. Signal doesn't handle quarantine properly.
2. Downloaded files bypass Quarantine & Gatekeeper checks
3. Downloaded files are executable in 2 clicks
4. `.terminal` file can be used for this purpose (it's executable after downloading from the web).

OS

macOS

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Notifications

Customize

🔊 Unsubscribe

You're receiving notifications because you authored the thread.

1 participant



Metnew commented on 17 Sep

Author + 😊 ...



Metnew commented yesterday

Author + 😊 ...



Metnew changed the title to `leads-to-GateKeeper-byp downloaded files leads t`

kenpowers-signal commented 5 days ago

Collaborator + 😊 ...

Sorry, not quite sure I follow. Are you saying that the same issue that applies to Brave applies to downloaded attachments in Signal?



Anita L. wrote: Jan 30, 2019 10:09 AM
To You

Hello Vladimir,

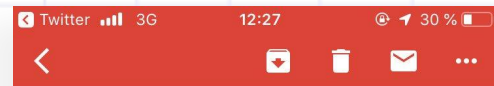
Unfortunately, we do not have a bug bounty program however we will be happy to add 25\$ Viber Out credit to your account.

Please let us know if you would like the credit to be added to Viber account with the number +380 93 333 3333

Awaiting your reply.

Best regards,
Anita L.
Viber support team leader
Quick question? Tweet to [@ViberHelp](#)

You wrote: Jan 29, 2019 03:26 PM
To Viber



Anita L. wrote: Feb 05, 2019 12:26 PM
To You

Hello Vladimir,

We understand your frustration however we believe that our users is a community that share good things and bad things in the favor of improving the app for the benefit of all.

Viber Out credit can be used for placing calls to non-Viber numbers through your Viber app, be it landline or mobile. Please let us know the number to add Viber Out credit for.

Thank you!

Best regards,
Anita L.
Viber support team leader
Quick question? Tweet to [@ViberHelp](#)

Anita L. wrote: Jan 30, 2019 10:09 AM
To You



• Zoho for desktop app for macOS: lack of com.apple.quarantine meta-attribute for downloaded files leads to GateKeeper bypass for mail attachments

Reported to Mail · [redacted] 0 · Jan 26, 2019 4:08:23 PM



Vladimir Metnew (metnew)

2328 -
Reputation Rank

5.50 91st
Signal Percentile

27.69 97th
Impact Percentile

50

#374106

Lack of quarantine meta-attribute for downloaded files leads to GateKeeper bypass

Share:     



Vladimir Metnew (metnew)

2328 -
Reputation Rank

5.50 91st
Signal Percentile

27.69 97th
Impact Percentile

18

#484664

ICQ for macOS: lack of `com.apple.quarantine` meta-attribute on downloaded files leads to GateKeeper/Quarantine bypass for downloaded executables

Share:     



Vladimir Metnew (metnew)

2328 -
Reputation Rank

5.50 91st
Signal Percentile

27.69 97th
Impact Percentile

#702608

[redacted] for macOS: lack of `com.apple.quarantine` meta-attribute on downloaded files leads to GateKeeper/Quarantine bypass



Professor (insomniac)

2034

Reputation

-

Rank

0.34

Signal

60th

Percentile

14.82

Impact

80th

Percentile

#696756

User-assisted RCE [redacted] client: downloaded executables lack "com.apple.quarantine" meta-attribute [macOS]



Sergey Kashatov (iframe)

2246

Reputation

-

Rank

2.45

Signal

74th

Percentile

13.47

Impact

78th

Percentile

#691446

[redacted] Выполнение произвольных файлов из за небезопасной загрузки файлов на компьютер приводит к RCE через оболочку Java.



Just Stay Shhhhh (h33t)

3205

Reputation

-

Rank

3.99

Signal

82nd

Percentile

19.27

Impact

90th

Percentile



0

#708426

Gatekeeper Bypass due to lack of `com.apple.quarantine`



alexbirsan filed a duplicate (#703077) and was invited to participate in this report.

Oct 10th (about 1 month ago)

Summary

- At least **15 affected apps**: Telegram, WhatsApp, Slack, Skype, Signal, Wickr ...
- Extremely powerful bug for **red teaming!**
- Security teams treat secure file handling as a user's responsibility. **Is this the right approach?**
- It seems that many people are **unaware** of File Quarantine.
- Apps might need to improve their **UX security**.
- I haven't seen a single non-AppStore app with enabled Quarantine during **Q4 2018/Q1 2019**.



Quarantine in Cloud File Storage Apps

Is it possible to exploit file quarantine in such apps, too?

Quarantine in cloud file storage apps

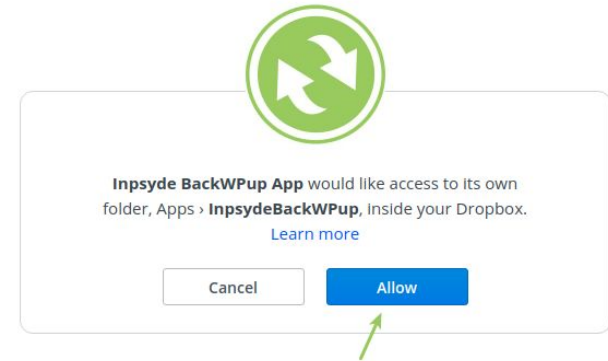
- Affected cloud file storage apps: Keybase, Dropbox, Google Drive, OneDrive ...
- As of Q4 2018, the only app with enabled Quarantine was Yandex.Disk 🤪
- Only Keybase fixed the issue!
- Quarantine is not easy to exploit here, but there is a way 🤪
- “Product-friendly” fix: attach quarantine file attribute to dangerous files like `.terminal` and `.webarchive`.

Attack scenario: Sync'n'Launch

1. To leverage file quarantine, we need to **deliver a file** to the user's device.
2. Let's leverage the **sync functionality** of syncing apps!
3. However, we still need to somehow **launch** the delivered file 🤔
4. In short, we're looking for a way to execute "**\$ open /path/to/synced/file.terminal**" on the user's device.

Attack scenario: Sync stage

- ✓ - Sync files to the user's device without the user's consent (**legitimate** Keybase feature)
- ✗ - Sync files by sharing a folder (Dropbox, OneDrive, Google Drive). Requires too much interaction from the targeted user.
- ❄️ - Leverage applications' web APIs and OAuth access!



Attack scenario: Sync via “App Folder”



1. Both [Dropbox](#) and [Google Drive](#) have “**App Folder**” integrations.
2. Many apps require this permission: cloud file converters, file previewers, graphic and video editors ...

Attackers can trick the user into authorizing a new “App Folder” integration or leverage existing vulnerable integrations to deliver a malicious payload to the user’s device.

[Redacted] wants to access your Google Account



[Redacted]

This will allow [Redacted] to:



Add itself to Google Drive



View and manage Google Drive files and folders that you have opened or created with this app



Make sure you trust [Redacted]

You may be sharing sensitive info with this site or app. Learn about how [Redacted] will handle your data by reviewing its [terms of service](#) and [privacy policies](#). You can always see or remove access in your [Google Account](#).



[Learn about the risks](#)

Cancel

Allow

Attack scenario: Launch stage

- If files have *+x permission* after the sync -> use **Windtail** trick.
- Launch of **.url** file equals “**\$ open <URL>**”.
- A **.url** file isn't tracked by Quarantine; it's a shortcut file.
- **.url** file's file-opening behavior was fixed in **macOS Catalina***.

 - Ask the user to run your payload in Finder 

 - Find an ***OS feature** 

```
File: x.url
1  [{000214A0-0000-0000-C000-000000000046}]
2  Prop3=19,2
3  [InternetShortcut]
4  URL=file:///Keybase/private/metnew,max/exploit.terminal
5  IDList=
```

Attack scenario: Sync'n'Launch

1. Sync a malicious **.terminal** file to the user's device
(*"App Folder"*, folder sharing, application's features).
2. Send a shortcut file (**.url**) that points to the **.terminal** file that has been synced to the user's device.
3. **.terminal** executes when the victim opens the **.url** file.

Keybase (sync + .url vector*)

1. Attackers can sync a **.terminal** file with the targeted user via KBFS without the user's consent.
2. Due to the design of KBFS, the file will have a predictable absolute path on the user's device.
3. The user opens a **.url** file that points to the synced **.terminal** file.
4. **.terminal** launches!



Keybase

Report: <https://hackerone.com/reports/430463>

Oct 29 2018 — The vulnerability was reported to Keybase.

Oct 30 2018 — Quarantine was enabled in Keybase chat app.

2 Nov 2018 — The vulnerability was patched in KBFS.

6 Feb 2019 — The Keybase Team remediated the issue.

16 Sep 2019 — The report was [disclosed on HackerOne](#).



Microsoft OneDrive 🙄

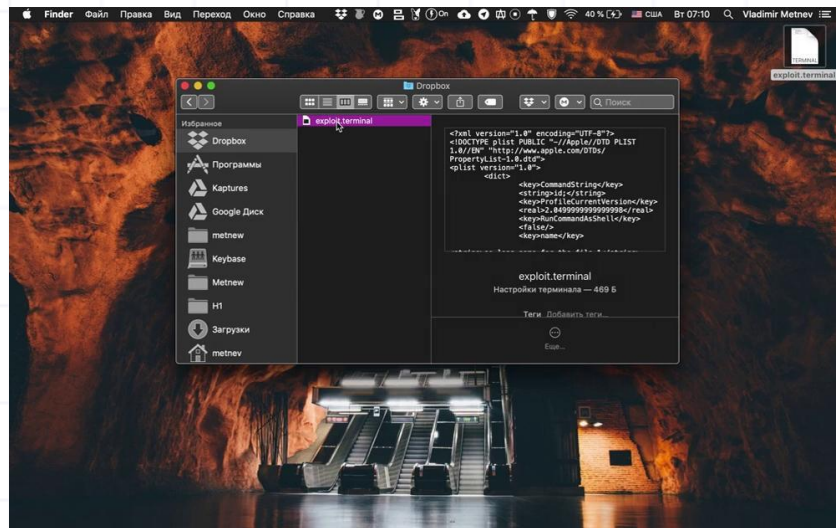
“We asked for (and received) an exception from Apple's head of macOS security to set an entitlement [on OneDrive app distributed through AppStore] that does not cause the quarantine bit to be set. Apple's position is generally that sync apps do not need to have MOTW/quarantine set on synced content.”

(c) MSRC

Dear OneDrive Team, only you are responsible for security issues in your app, not Apple's head of macOS security. (c) Author of this slide

Dropbox

- Dropbox seem to be aware of the Quarantine issue. The Dropbox Team has said that they're not going to track this as a vulnerability, unless the exploitation doesn't require any user interaction
- Dropbox has the capacity to implement a fix of any granularity, but they haven't done so.
- You can find the exported version of the report [here](#).
- It's likely that the Dropbox Team didn't think about a sync vector via "App Folder" integration.



.fileloc is the new .url!

- Apple fixed `.url` file handling in Catalina.
- `.fileloc` file still allows to open local executables!
- **Opinion:** Neither `.url` nor `.fileloc` have any value unless the attacker can plant a malicious payload that has already bypassed the Quarantine mechanism.



File: `calc.fileloc`

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>URL</key>
    <string>file:///System/Applications/Calculator.app</string>
  </dict>
</plist>
```

CVE-2009-2811: **.fileloc** aka “10years-day”

Current Description

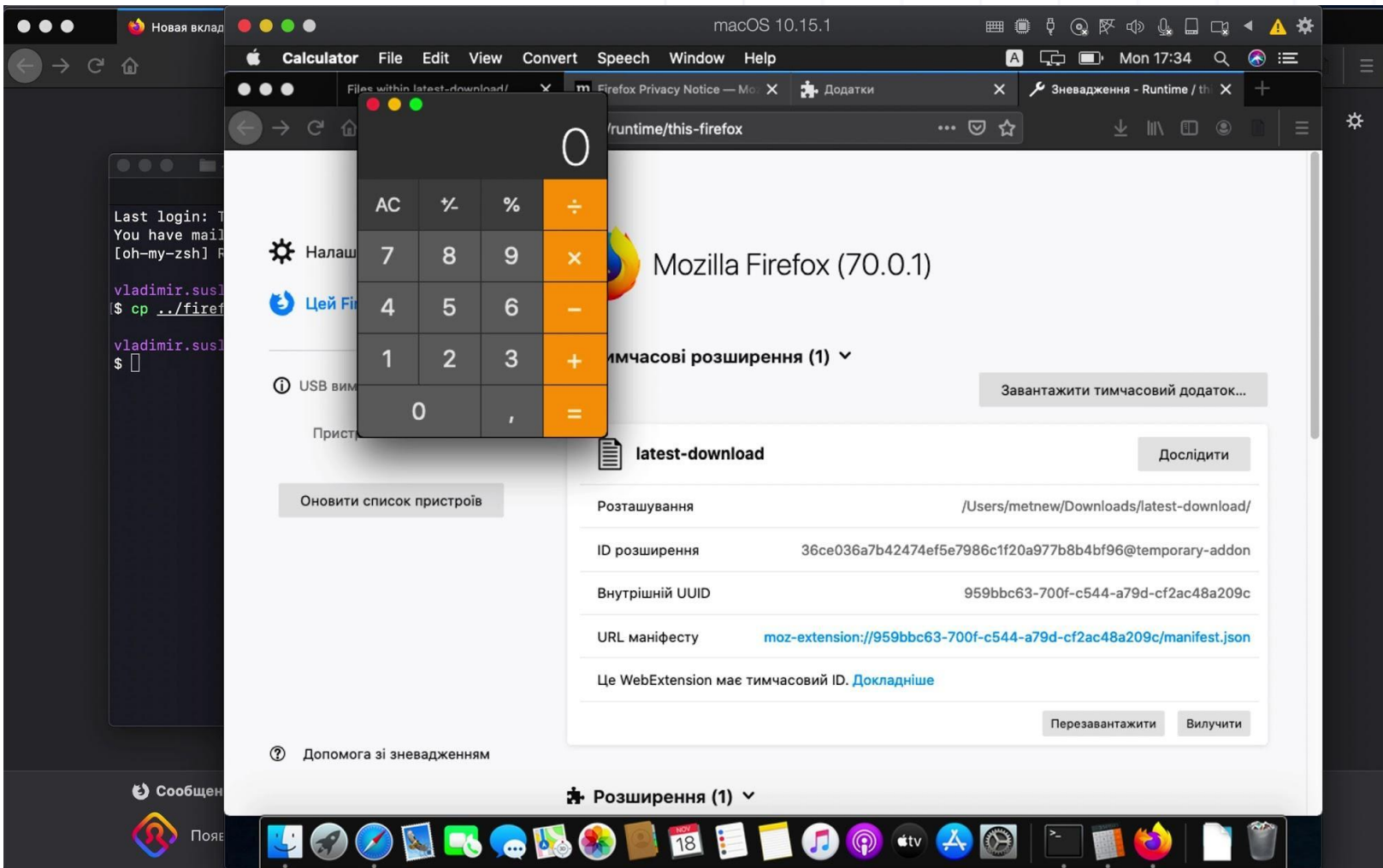
Incomplete blacklist vulnerability in Launch Services in Apple Mac OS X 10.5.8 allows user-assisted remote attackers to execute arbitrary code via a **.fileloc** file, which does not trigger a "potentially unsafe" warning message in the Quarantine feature.

Source: MITRE

- It has been known that **.fileloc** is dangerous for macOS devices without enabled GateKeeper.
- How did OneDrive receive the “exception” from Apple?

File: **calc.fileloc**

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>URL</key>
    <string>file:///System/Applications/Calculator.app</string>
  </dict>
</plist>
```



macOS 10.15.1

Calculator File Edit View Convert Speech Window Help

Files within latest-download/ Firefox Privacy Notice — Мо. X Додатки

runtime/this-firefox

Mozilla Firefox (70.0.1)

Тимчасові розширення (1) ▾

Завантажити тимчасовий додаток...

latest-download

Дослідити

Розташування	/Users/metnew/Downloads/latest-download/
ID розширення	36ce036a7b42474ef5e7986c1f20a977b8b4bf96@temporary-addon
Внутрішній UUID	959bbc63-700f-c544-a79d-cf2ac48a209c
URL маніфесту	moz-extension://959bbc63-700f-c544-a79d-cf2ac48a209c/manifest.json
Ця WebExtension має тимчасовий ID. Докладніше	

Перезавантажити

Вилучити

Допомога зі зневадженням

Розширення (1) ▾

Personal opinion

- MOTW bypass on Windows is considered as a severe bug. Why the same bug on macOS is considered as a violation of best practices and not as a vulnerability?
- It's absurd, how well-known apps can be affected to such a simple issue.
- 🍏 must educate developers on secure file handling and UX security.
- Developers must be responsible for secure file handling in their apps and educate users about security.
- Nice UX -> more users -> more revenue. Security > UX.

Outcomes

- Popular macOS apps now enforce File Quarantine (15+ apps). Except of mentioned syncing apps.
- The technique has become popular among bug hunters.
- The research describes attack vectors that can be effectively abused by unsophisticated attackers.
- The research revealed *unknown* macOS “features”: **.url** and **.fileloc** files.

And now I have a bunch of screencasts demonstrating how a single click on a file icon leads to code execution 🤪🐱

Open questions

- Who should be responsible for secure file handling?
- Is there a way to fix file quarantine issues?
- Is it an unique case in the Apple ecosystem?
- Is it normal to make “exceptions” for some companies?
- Do developers need to educate users?

Postmortem

- Postponing the disclosure was a bad idea.
- I'm glad to see that bug hunters and researchers report File Quarantine issues to other products.
- I wish the unpatched apps will implement additional security measures (e.g., direct quarantining).
- Try to search for misconfigurations when hunting *OS apps. Nobody reads Apple's guides. (SMJobBless is a good example)

Thank you!

twitter.com/vladimir_metnew 🙄