Deceiving Developers: Abusing Legitimate GitHub Repositories to Deliver Malware

Theo Webb

2026/1/23

Contributors: Shungo Kumasaka & Yasuyuki Kobayashi

TLP:CLEAR

Theo Webb

GMO Cybersecurity by Ierae, Inc

SOC Innovation Division

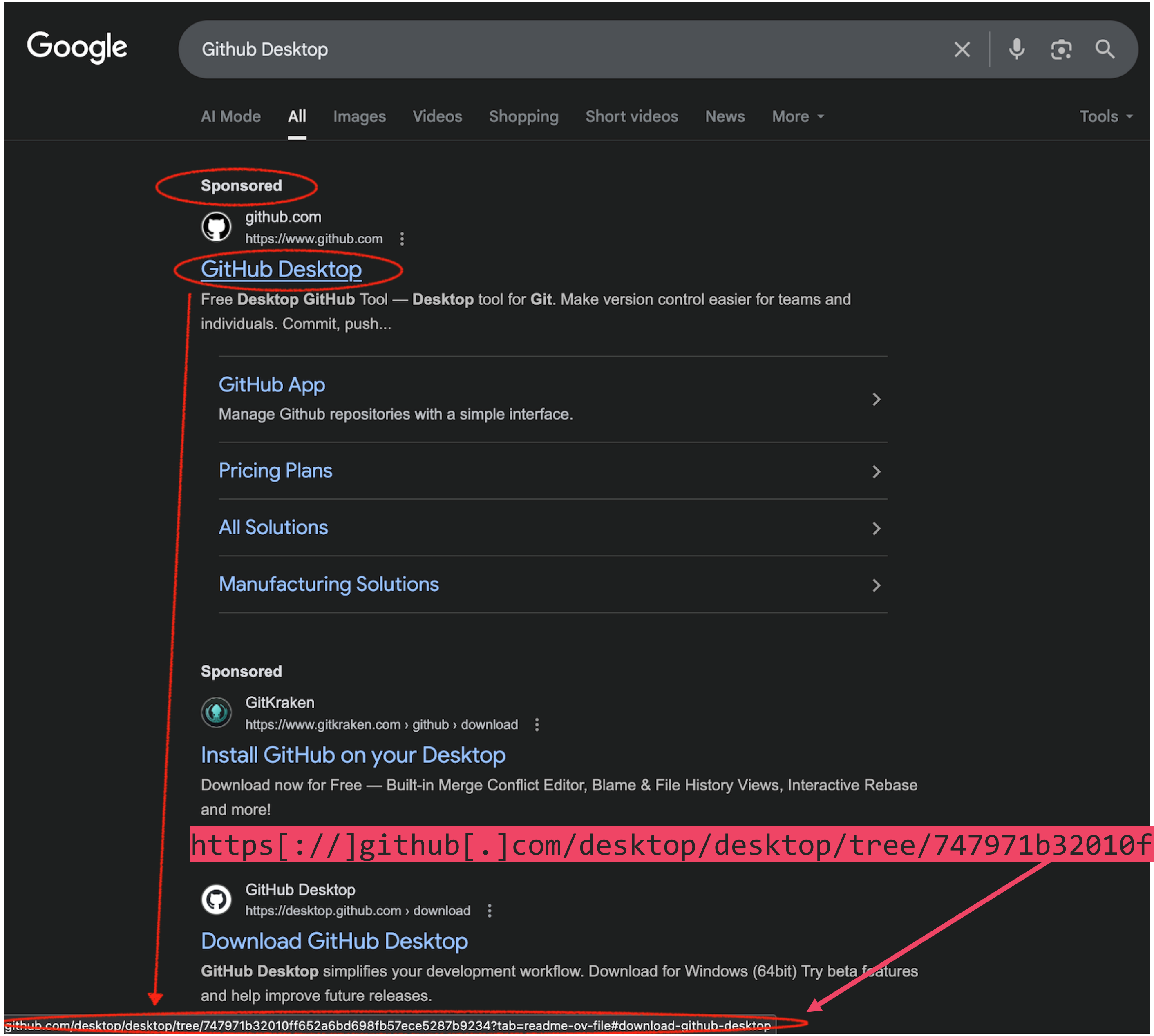
Security Engineer ・Malware Researcher

Overview

- Delivery technique: malvertising + GitHub repo squatting
- Why it works: non-official commits in official repos
- Reproducibility: GitLab + package managers
- How to avoid this attack
- Infection chain overview

Key Takeaways

- Campaign most active between September and October 2025
- EU/EEA-focused malvertising was observed, but infections also occurred in Japan
- Targets users searching for developer tools
- Uses a multi-stage loader (Windows) that deploys HijackLoader; macOS victims receive AMOS stealer



Sponsored

github.com
https://www.github.com

GitHub Desktop

Free **Desktop GitHub** Tool — **Desktop** tool for **Git**. Make version control easier for teams and individuals. Commit, push...

GitHub App
Manage Github repositories with a simple interface.

Pricing Plans

All Solutions

Manufacturing Solutions

Sponsored

GitKraken
https://www.gitkraken.com › github › download

Install GitHub on your Desktop

Download now for Free — Built-in Merge Conflict Editor, Blame & File History Views, Interactive Rebase and more!

GitHub Desktop
https://desktop.github.com › download

Download GitHub Desktop

GitHub Desktop simplifies your development workflow. Download for Windows (64bit) Try beta features and help improve future releases.

github.com/desktop/desktop/tree/747971b32010ff652a6bd698fb57ece5287b9234?tab=readme-ov-file#download-github-desktop

Malware Delivery

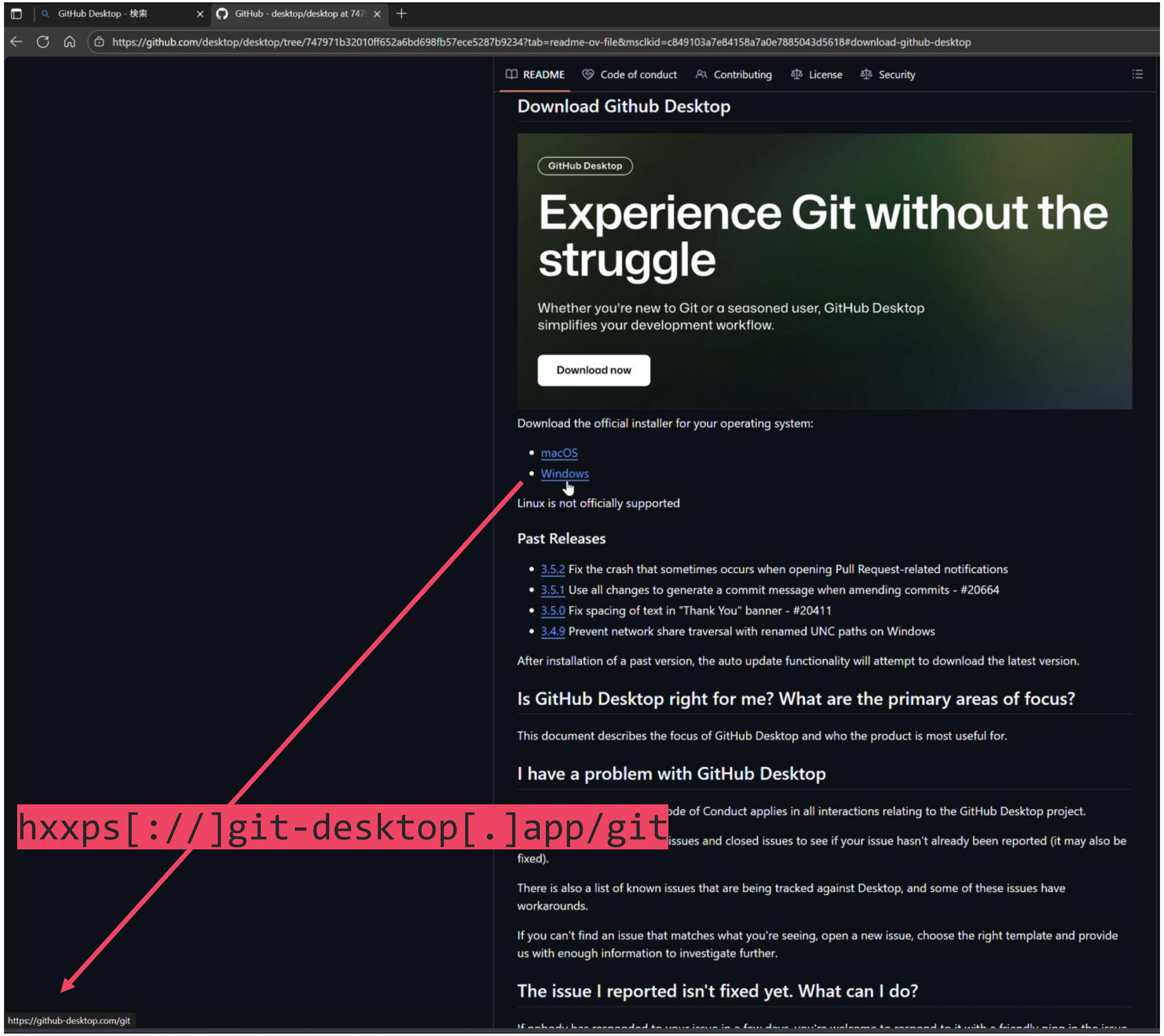
1. Victim searches for "GitHub Desktop" and clicks the sponsored result.

Note: URL, domain, and icon all appear official.

https[://]github[.]com/desktop/desktop/tree/747971b32010ff652a6bd698fb57ece5287b9234?tab=readme-ov-file

Malware Delivery

2. Clicks the download link in the README.



https://github.com/desktop/desktop/tree/747971b32010ff652a6bd698fb57ece5287b9234?tab=readme-ov-file&msclkid=c849103a7e84158a7a0e7885043d5618#download-github-desktop

Download Github Desktop

Experience Git without the struggle

Whether you're new to Git or a seasoned user, GitHub Desktop simplifies your development workflow.

Download the official installer for your operating system:

- macOS
- Windows

Linux is not officially supported

Past Releases

- 3.5.2 Fix the crash that sometimes occurs when opening Pull Request-related notifications
- 3.5.1 Use all changes to generate a commit message when amending commits - #20664
- 3.5.0 Fix spacing of text in "Thank You" banner - #20411
- 3.4.9 Prevent network share traversal with renamed UNC paths on Windows

After installation of a past version, the auto update functionality will attempt to download the latest version.

Is GitHub Desktop right for me? What are the primary areas of focus?

This document describes the focus of GitHub Desktop and who the product is most useful for.

I have a problem with GitHub Desktop

ode of Conduct applies in all interactions relating to the GitHub Desktop project.

issues and closed issues to see if your issue hasn't already been reported (it may also be fixed).

There is also a list of known issues that are being tracked against Desktop, and some of these issues have workarounds.

If you can't find an issue that matches what you're seeing, open a new issue, choose the right template and provide us with enough information to investigate further.

The issue I reported isn't fixed yet. What can I do?

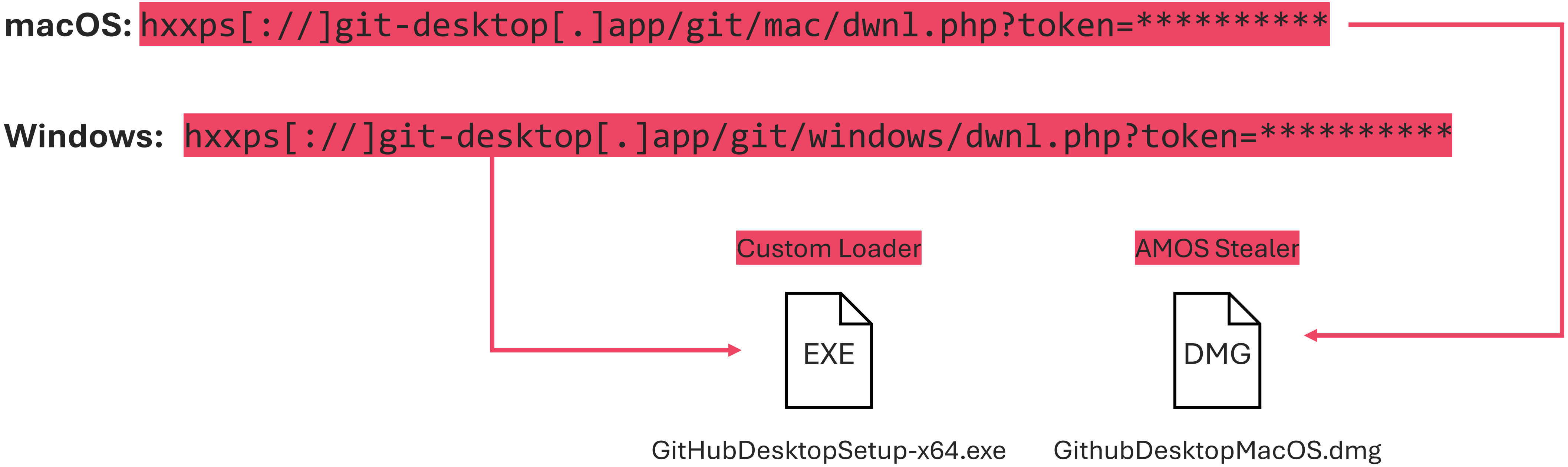
If nobody has responded to your issue in a few days, you're welcome to respond to it with a friendly ping in the issue

https://github-desktop.com/git

hxxps[://]git-desktop[.]app/git

Malware Delivery

3. Victim is redirected to an external host and downloads the malicious installer:



macOS: `hxxps[://]git-desktop[.]app/git/mac/dwnl.php?token=**********`

Windows: `hxxps[://]git-desktop[.]app/git/windows/dwnl.php?token=**********`

Custom Loader

EXE

GitHubDesktopSetup-x64.exe

AMOS Stealer

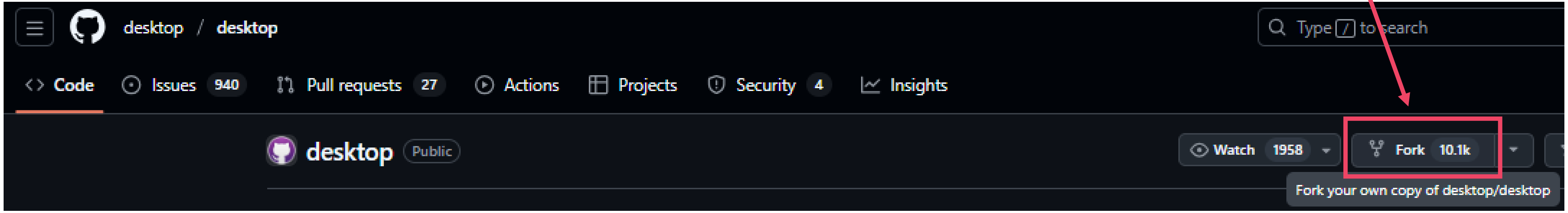
DMG

GithubDesktopMacOS.dmg

Delivery Technique: Malvertising + GitHub Repo Squatting

Step 1. Attacker creates a throwaway GitHub account and forks the official GitHub Desktop repository:

`https://github.com/desktop/desktop`



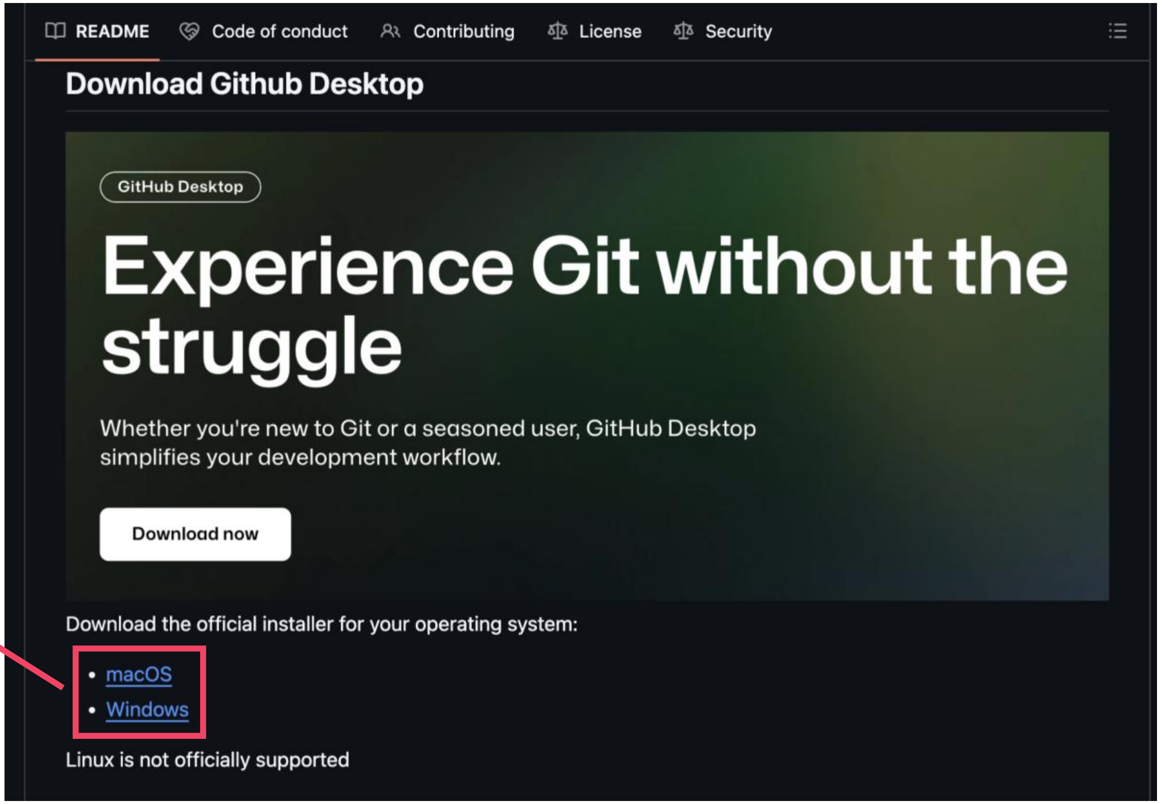
Delivery Technique

Step 2. Attacker edits the download link in the README to point to their domain and commits.

`hxxps[://]git-desktop[.]app/git`

That commit is viewable under the official repository's namespace:

`github.com/desktop/desktop/tree/<commit_hash>`



Download Github Desktop

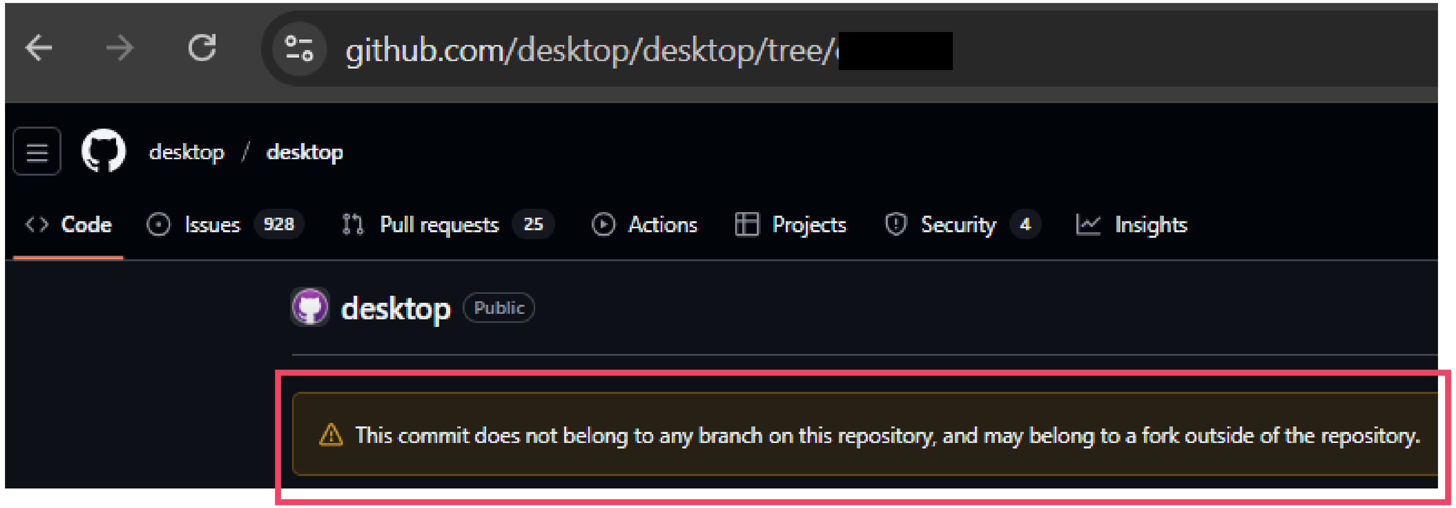
Experience Git without the struggle

Whether you're new to Git or a seasoned user, GitHub Desktop simplifies your development workflow.

Download the official installer for your operating system:

- macOS
- Windows

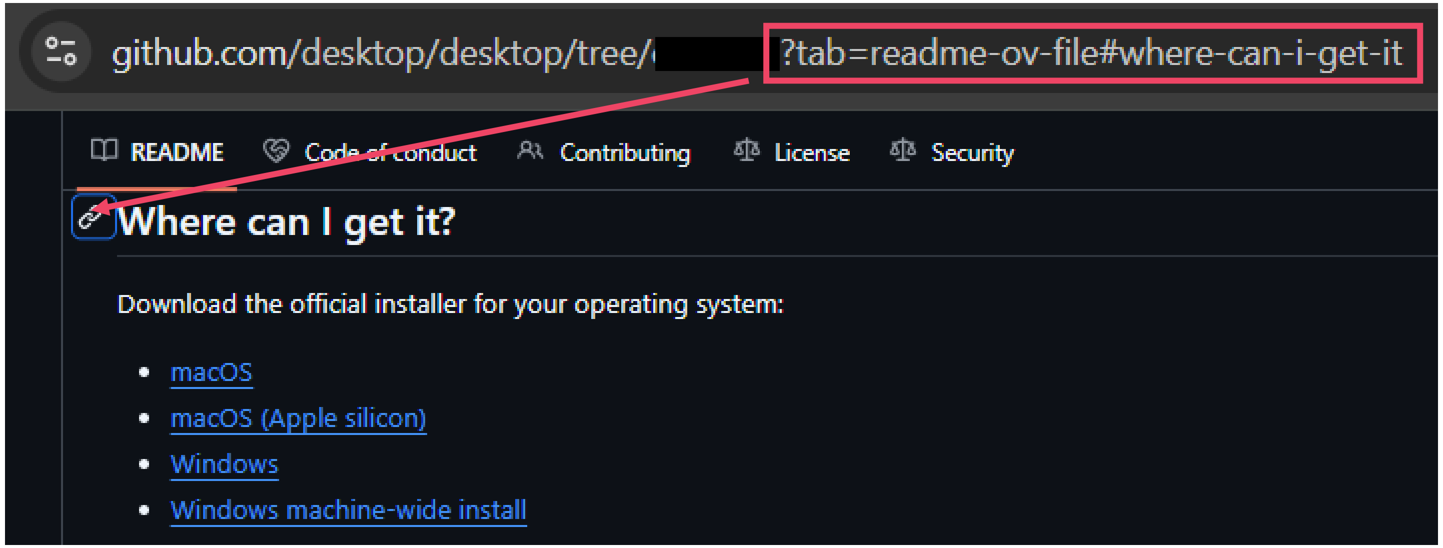
Linux is not officially supported



github.com/desktop/desktop/tree/[redacted]

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

Anchor skips GitHub’s warning message.

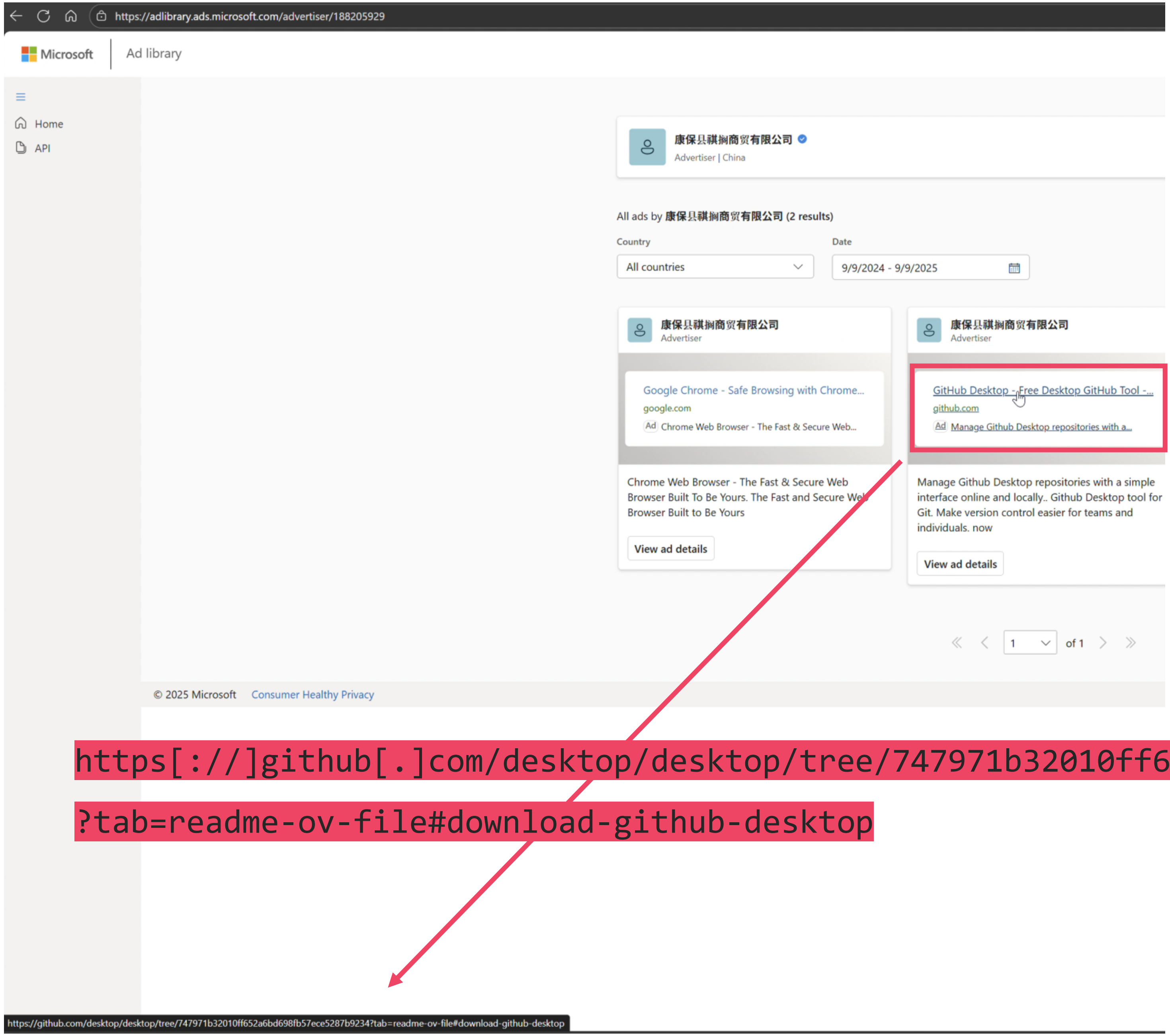


github.com/desktop/desktop/tree/[redacted]?tab=readme-ov-file#where-can-i-get-it

Where can I get it?

Download the official installer for your operating system:

- macOS
- macOS (Apple silicon)
- Windows
- Windows machine-wide install



https://adlibrary.ads.microsoft.com/advertiser/188205929

康保县祺搁商贸有限公司
Advertiser | China

All ads by 康保县祺搁商贸有限公司 (2 results)

Country: All countries

Date: 9/9/2024 - 9/9/2025

康保县祺搁商贸有限公司
Advertiser

Google Chrome - Safe Browsing with Chrome...
google.com
Ad Chrome Web Browser - The Fast & Secure Web...

Chrome Web Browser - The Fast & Secure Web Browser Built To Be Yours. The Fast and Secure Web Browser Built to Be Yours

康保县祺搁商贸有限公司
Advertiser

GitHub Desktop - Free Desktop GitHub Tool -...
github.com
Ad Manage Github Desktop repositories with a...

Manage Github Desktop repositories with a simple interface online and locally.. Github Desktop tool for Git. Make version control easier for teams and individuals. now

© 2025 Microsoft Consumer Healthy Privacy

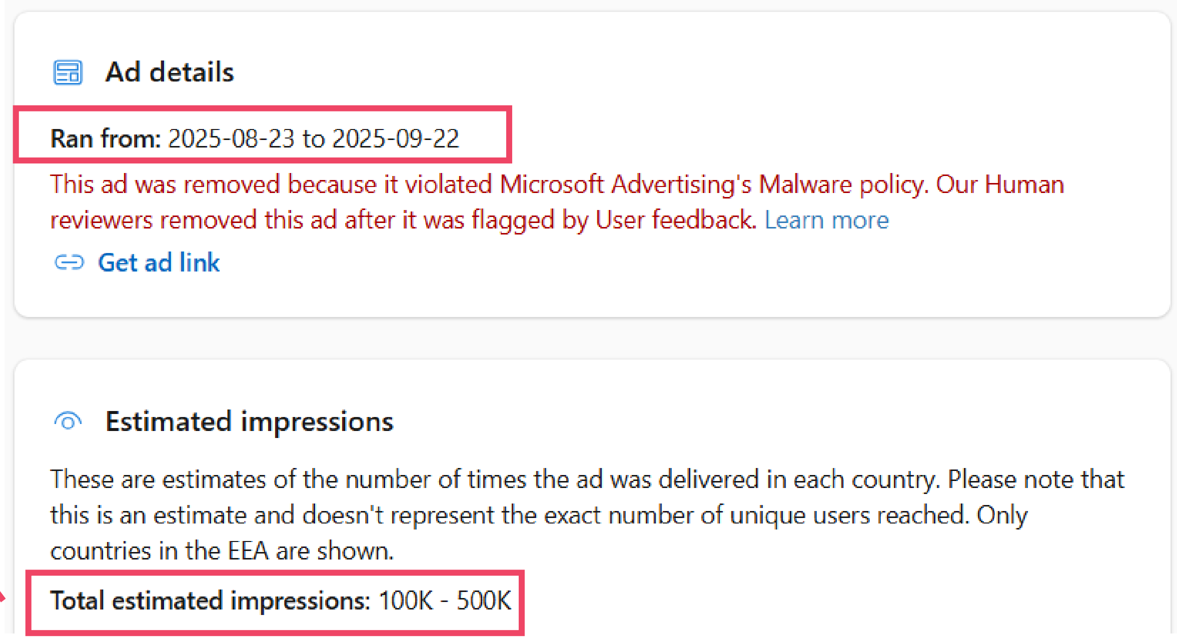
https://github.com/desktop/desktop/tree/747971b32010ff652a6bd698fb57ece5287b9234?tab=readme-ov-file#download-github-desktop

Step 3. Attacker uses sponsored ads for "GitHub Desktop" to promote their commit.

https[://]github[.]com/desktop/desktop/tree/747971b32010ff652a6bd698fb57ece5287b9234?tab=readme-ov-file#download-github-desktop

Outcome

- **Bing Ads (estimated) impressions:** That one ad, pointing to a malicious commit, received an estimated **100K - 500k** impressions.
- **Six** malicious commits were identified.
- Malicious commits were also promoted via Google Ads.



Ad details

Ran from: 2025-08-23 to 2025-09-22

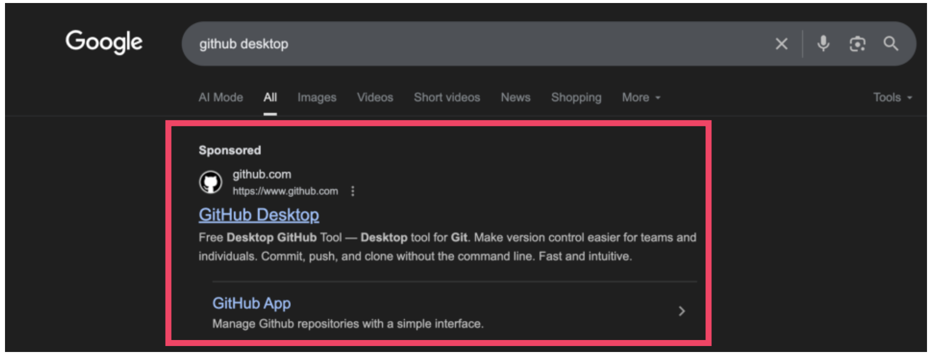
This ad was removed because it violated Microsoft Advertising's Malware policy. Our Human reviewers removed this ad after it was flagged by User feedback. Learn more

Get ad link

Estimated impressions

These are estimates of the number of times the ad was delivered in each country. Please note that this is an estimate and doesn't represent the exact number of unique users reached. Only countries in the EEA are shown.

Total estimated impressions: 100K - 500K



Sponsored

github.com
https://www.github.com

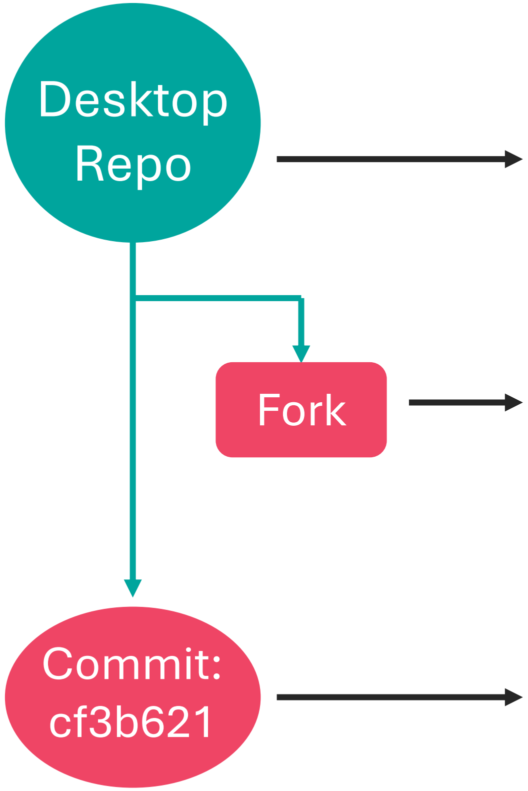
GitHub Desktop

Free **Desktop GitHub** Tool — **Desktop** tool for **Git**. Make version control easier for teams and individuals. Commit, push, and clone without the command line. Fast and intuitive.

GitHub App

Manage Github repositories with a simple interface.

Why It Works:
Non-Official Commits in Official Repos



GitHub stores repositories, forks, and commits in a “repository network”.

Upstream repo `github.com/desktop/desktop`

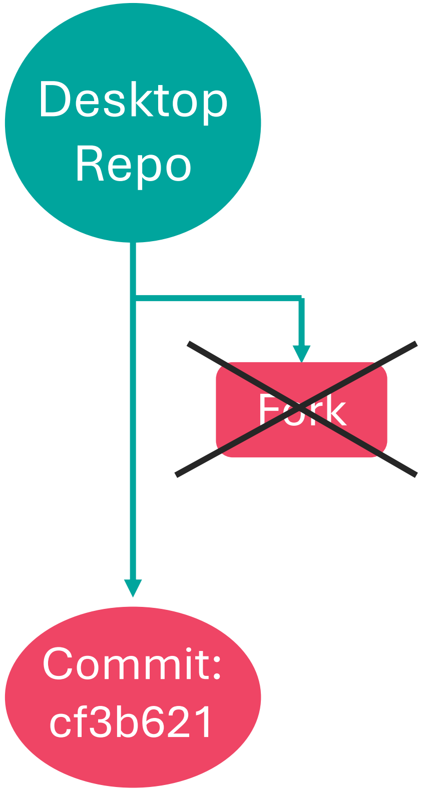
Fork commit `github.com/<username>/desktop/commit/<commit_hash>`

A commit hash created in a fork is addressable from the upstream:

`github.com/desktop/desktop/tree/<commit_hash>`

`github.com/desktop/desktop/tree/cf3b621` (Short SHA-1)

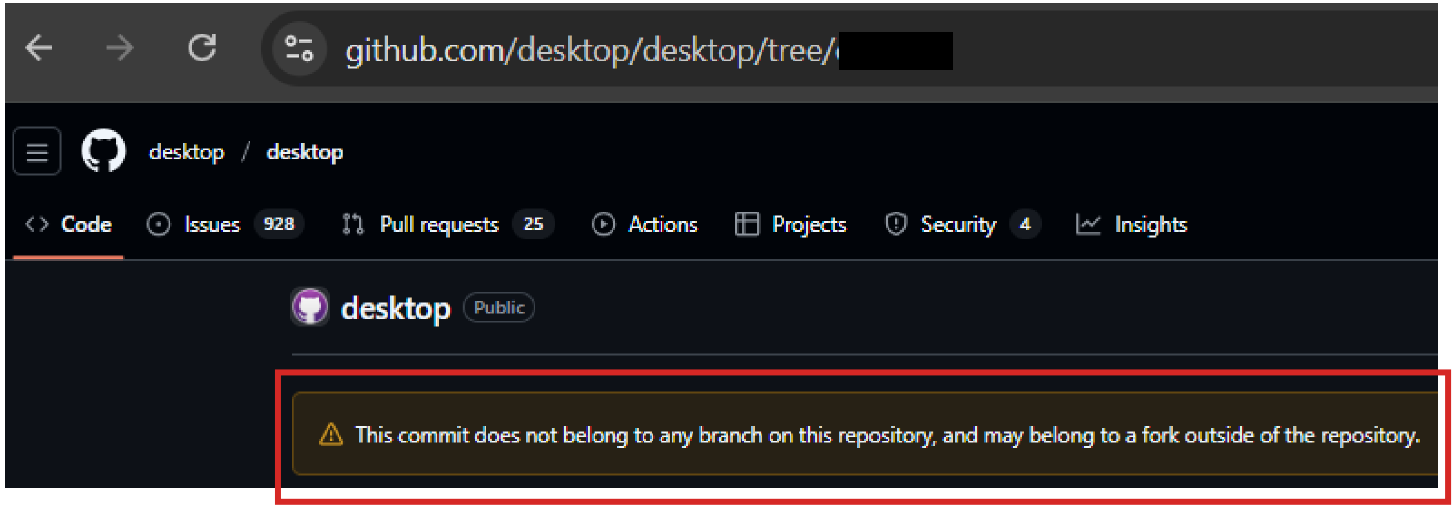
Why It Works:
Non-Official Commits in Official Repos



Deleted Fork/Account ≠ Deleted Commit

- If you delete the fork (or the account that created it), the commit hash can still be accessed from the upstream. It exists forever.
- This is a property of the repository network, and GitHub documents it explicitly.
- This makes it much harder to track and clean up malicious commits.

GitHub’s Mitigations



github.com/desktop/desktop/tree/[redacted]

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

.. bypassed with an anchor in the README:

```
github.com/desktop/desktop/tree/<commit_hash>?tab=readme-ov-file#where-can-i-get-it
```

GitHub’s Response

- GitHub removed the malicious commits.
- On September 9, 2025, GitHub stated that their security team is aware of this issue and is taking measures to mitigate it.
- As of December 29th, 2025, it can still be reproduced.

Reproducibility: GitLab

Upstream repo `gitlab.com/<namespace>/<project>/`

Fork commit `gitlab.com/<attacker-namespace>/<project>/-/tree/cf3b621`

Try to access the same commit from the upstream repository:

```
https://gitlab.com/<namespace>/<project>/-/tree/cf3b621
```

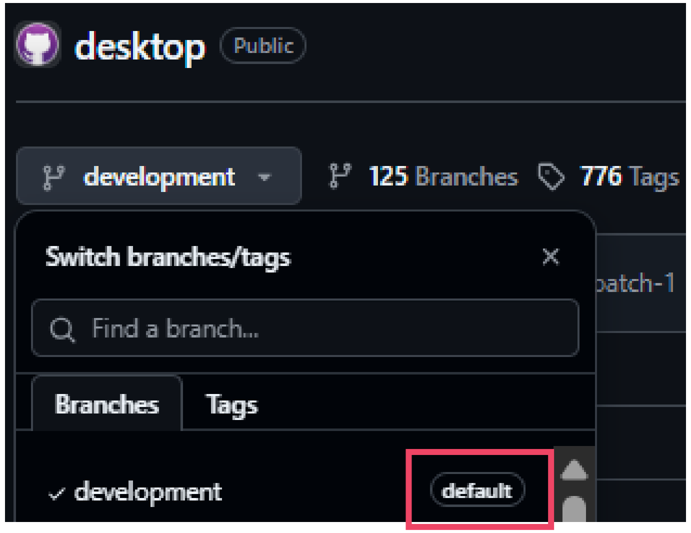
You will receive: `404: Page not found`

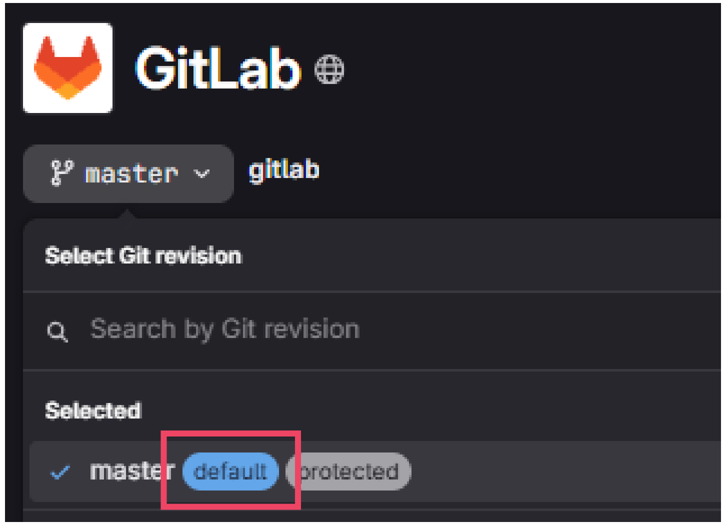
In-person only

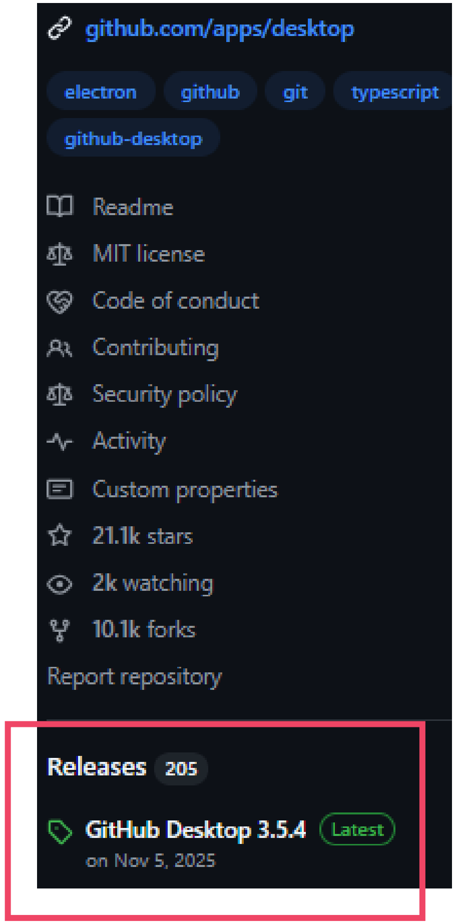
In-person only

How to Avoid This Kind of Attack

Confirm you are on the official **default** branch:





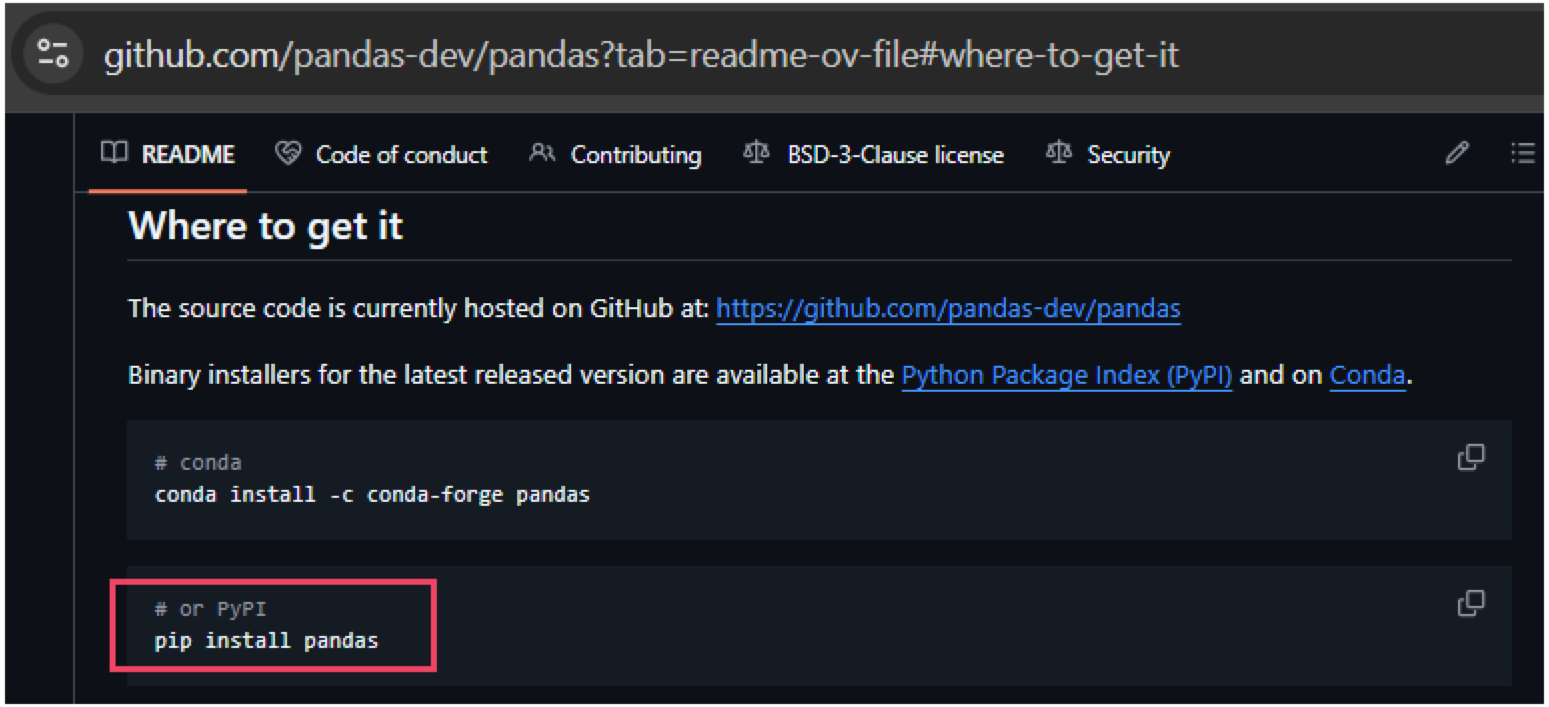


Alternatively, download installers from the repository’s **Releases** page.

Reproducibility: Package Managers

READMEs often use **pip** for software installation. For example:

```
pip install pandas
```



github.com/pandas-dev/pandas?tab=readme-ov-file#where-to-get-it
README
Code of conduct
Contributing
BSD-3-Clause license
Security

Where to get it

The source code is currently hosted on GitHub at: https://github.com/pandas-dev/pandas

Binary installers for the latest released version are available at the Python Package Index (PyPI) and on Conda.

```
# conda
conda install -c conda-forge pandas
```

```
# or PyPI
pip install pandas
```

In-person only

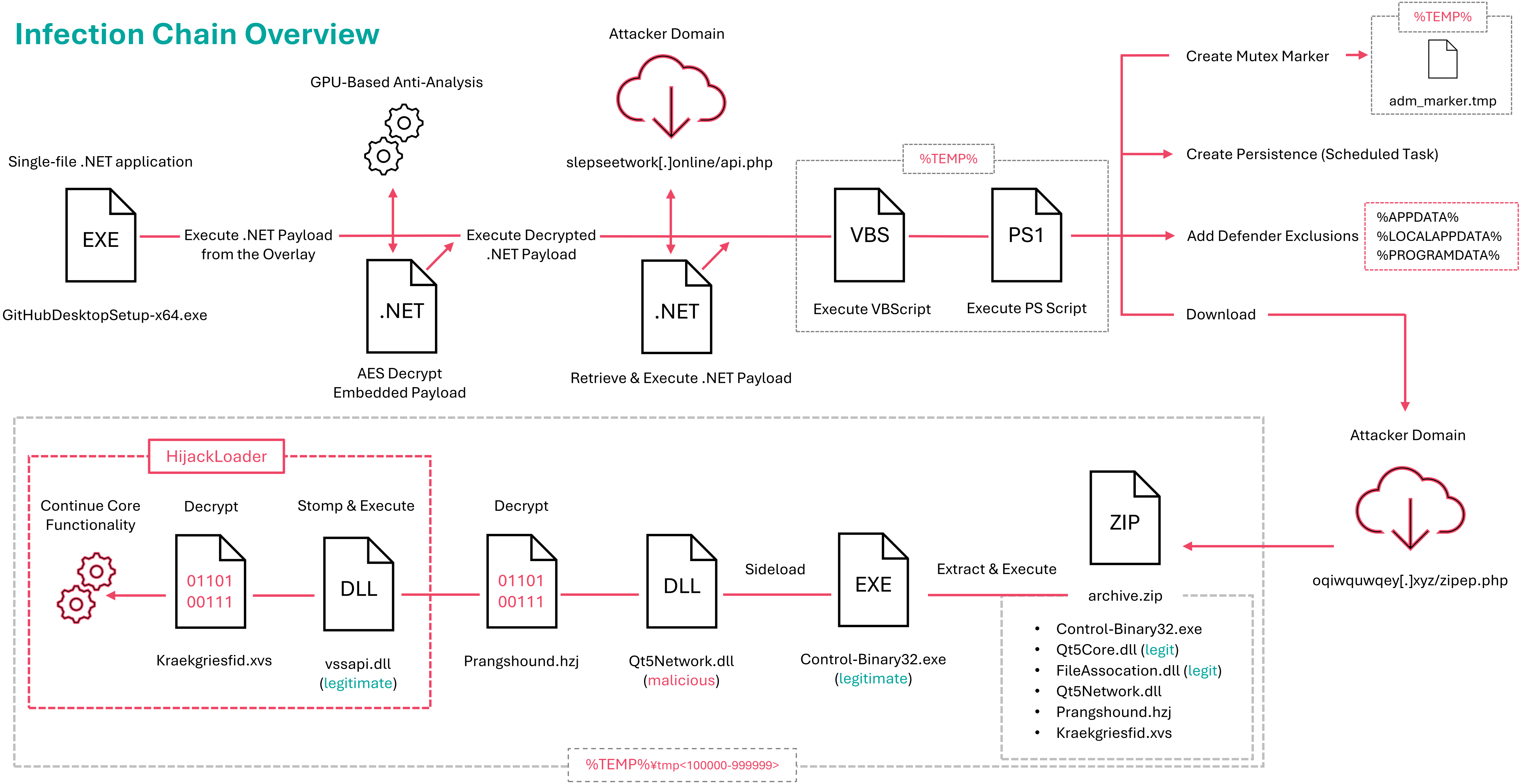
Reproducibility: git clone

- `git clone` cannot be manipulated in the same way as pip. For example:

```
git clone github.com/<owner>/<repository> && cd <repository> && git
checkout <attacker_commit> && pip install -e
```

- This fails at `git checkout` because the cloned local repository **does not** contain a reference to `<attacker_commit>`.
- That commit only exists in the attacker’s fork, not in the upstream repository.

Infection Chain Overview



Conclusion

GitHub and GitLab repositories can be abused to host malicious installers within official repository networks.

Mitigation

Download installers from official Releases pages (or vendor download pages) and exercise caution when interacting with sponsored search ads.

Thank You

Scan the QR code for our full malware analysis

Detection Opportunities

YARA Rule

```
rule MAL_Loader_WIN_1
{
    meta:
        description = "Generic rule to detect the single-file malicious installer"
        author = "GMO Cybersecurity by Ierae, Inc"

    strings:
        // .NET single-file bundle marker (sfbm)
        // 4 bytes (non-zero), 4 bytes (any), 32-byte fixed tail
        $sfbm = { ?? ?? ?? ?? ?? ?? ?? ?? 8B 12 02 B9 6A 61 20 38 72 7B 93 02 14 D7 A0 32 13
F5 B9 E6 EF AE 33 18 EE 3B 2D CE 24 B3 6A AE }

        $a1 = "No OpenCL platforms found" ascii wide
        $a2 = "No OpenCL GPU devices found" ascii wide
        $a3 = "Failed to create context" ascii wide
        $a4 = "Failed to create command queue" ascii wide
        $a5 = "Failed to create program" ascii wide
        $a6 = "Failed to build program" ascii wide
        $a7 = "Failed to create kernel" ascii wide
        $a8 = "generate_key" ascii wide

    condition:
        uint16(0) == 0x5a4d and
        (#sfbm > 0 and
         for any i in (1..#sfbm):
            ( uint8(@sfbm[i]) > 0 and
              uint8(@sfbm[i]+1) > 0 and
              uint8(@sfbm[i]+2) > 0 and
              uint8(@sfbm[i]+3) > 0 )) and
        (all of ($a*))
}
```

Detection Opportunities

IOCs: Malicious Commits

SHA-1 commit hashes
3b3e14cec9f2c7f9567bb1a50ece12d4eb337305
629f3ab77b0c6840618029d39869d078f8a5a694
636f5d478fa774635da5b25ecb842822ab444009
747971b32010ff652a6bd698fb57ece5287b9234
a48188b0d5bdc3e8728cb37619cc51f7392b086f
e24d78ebb3c7302cc6aa8e2231f847a53e1345f2

Detection Opportunities

URLs Hosting Malicious Installers

hxxps[://]git-desktop[.]app/git
hxxps[://]gitpage[.]app/
hxxps[://]git-desktop[.]it[.]com/git

Malicious Installers

SHA-256
ad07ffab86a42b4befaf7858318480a556a2e7c272604c3f1dcae0782339482e
e252bb114f5c2793fc6900d49d3c302fc9298f36447bbf242a00c10887c36d71

Detection Opportunities

Decrypted .NET Payload

SHA-256
e5c01a6f3d85c469e16857d92d9f0a1b01d14b0f0dad7df94b1afa6dc1ff4490
731f03daacb38f70bf2178f2ab100b68fc189c9c8da19cc2be24d31d35e799b1

Next-stage .NET Payload URLs

hxxps[://]slepseetwork[.]online/api[.]php (observed at 45.59.124[.]94:443)
hxxps[://]poiwerpolymersinc[.]online/api[.]php

Detection Opportunities

PowerShell Stager Variants

SHA-256	Next Stage Payload (HijackLoader) URL
8cd7d9ccea98ad6a3dfb4767e574349c9fd5678150c629661574ddd45e40cd37	hxxps[://]oqiwquwqey[.]xyz/zipep[.]php
6f9a1286f950da68e81bfe3e6c7655df00558df4d50289bf84df79c7d5073a2e	hxxps[://]sleeposeirer[.]online/zip[.]php
75deee7af25dc4f772661f17be4938c1980a703a785dc32274bf1647f8133cec	hxxps[://]21ow[.]icu/arasa[.]php
2299b795169494d3717140bf34ea4574b6a9d7d8aecf77fd9ca932925373a23f	hxxps[://]kololjrdtgted[.]click/zip[.]php
95974060b0dfc45401d15ef9d07392b338fb7af2e3f623eb85b0ef5d1f5759d5	hxxps[://]lofiufueyer[.]blog/aps[.]php
a46170be7cca7d8bcecf3da4caf035ec24f758eba45936ed802c1a03beab1c0a	hxxps[://]polwique[.]blog/fils[.]php
dbe1ec81fe1cb7f0249f47ed83be1b80ac99b2ae726a19b2083cb6fb585515d9	hxxps[://]21gweweqax[.]online/api[.]php
f3a914a46795021afd35b6c54a3c64ffedf33fbc3398dea84e6f71dc2d3ae198	hxxps[://]appsiauer[.]online/api[.]php

Detection Opportunities

HijackLoader IOCs

Filename	SHA-256	Description
Control-Binary32.exe (32-bit)	79384ef76740962757d617bc056bf8a45b2ef8f1e1587632b36830e2fc6ab21a	Legitimate executable
Qt5Network.dll (32-bit)	719a726d54161a1a95cf69f3001b74fe15661b83d995b89bcca5ecc8e792e2eb	Hijacked DLL that loads Prangshound.hzj
FileAssocation.dll (32-bit)	95d51ee9c58f789213cedac7e82c7ba064364d9e5c8ca76ad27a5e53537f9fdf	Legitimate dependency DLL
Qt5Core.dll (32-bit)	b967ade09a9338320e0db4e5da11a2ac396950f0eed689b28bd31686b7baf018	Legitimate dependency DLL
Prangshound.hzj	58f897d4369a4c667b2f40a6703c7ae42912a10186d81c6eaa7809513da86a51	Encrypted staging data (module to stomp, plaintext decryption key, and configuration)
Kraekgriesfid.xvs	be503f616edacac10689b63ba39c4b5d791fcf365bc80a0c8bc27c2c3d3cb2a4	Encrypted HijackLoader modules/config and the encrypted final payload

References

- Truffle Security: *Anyone can Access Deleted and Private Repository Data on GitHub*
- GitHub Docs: *About permissions and visibility of forks*
- GitHub Docs: *Understanding connections between repositories*
- GitHub Docs: *What happens to forks when a repository is deleted or changes visibility?*
- Git Docs: Short SHA-1
- Git Docs: git-clone
- Pip Docs: *VCS Support*

TLP:CLEAR

Related Publications

- GMO Cybersecurity by Ierae: *GitHub Desktop を模したマルウェアダウンロードの誘導に関する注意喚起*
- Palo Alto Networks – Unit 42: *GitHub Actions Supply Chain Attack*
- Palo Alto Networks: *Tracking Down Malicious Communication with Advanced XDR Detection Tactics*
- Arctic Wolf: *GPUGate Malware: Malicious GitHub Desktop Implants Use Hardware-Specific Decryption, Abuse Google Ads to Target Western Europe*
- Vladyslav Bahlai: *HijackLoader/GhostPulse/IDAT Loader Comprehensive Analysis*
- Ryan Weil from Trellix: *A Comprehensive Analysis of HijackLoader and Its Infection Chain*

TLP:CLEAR