

On the Security of Application Installers & Online Software Repositories

Marcus Botacin¹ Giovanni Bertão² Paulo de Geus²
André Grégio¹ Christopher Kruegel³ Giovanni Vigna³

¹Federal University of Paraná – Brazil (UFPR)
{mfbotacin,gregio}@inf.ufpr.br

²University of Campinas – Brazil (UNICAMP)
{bertao,paulo}@lasca.ic.unicamp.br

³University of California at Santa Barbara – USA (UCSB)
{chris,vigna}@ucsb.edu

2020

Agenda

- 1 Introduction
- 2 Repositories
- 3 Installers
- 4 Trojanization
- 5 Conclusion

Agenda

- 1 Introduction
- 2 Repositories
- 3 Installers
- 4 Trojanization
- 5 Conclusion

Software Repositories



Figure: Evaluated Repositories.

Software Repositories

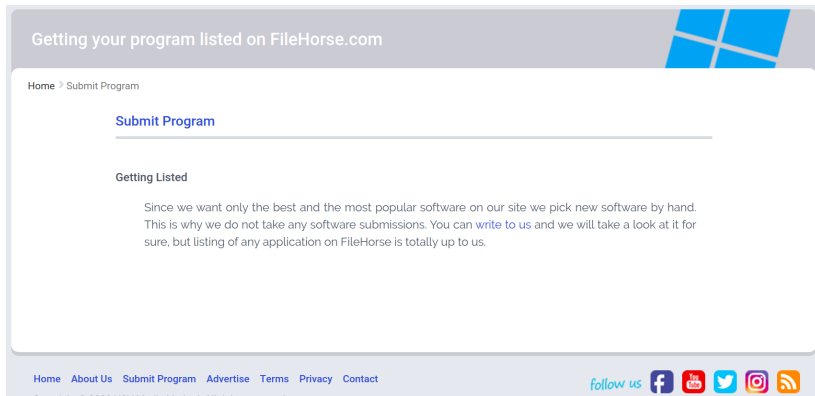


Figure: Software Inclusion.

Software Repositories

- ☐ ★★★ & up
- ☐ ★★ & up
- ☐ ★ & up

USER RATING

- ☐ ★★★★★ & up
- ☐ ★★★★ & up
- ☐ ★★★ & up
- ☐ ★★ & up
- ☐ ★ & up

CATEGORY

- ☐ Browsers
- ☐ Drivers
- ☐ Utilities & Operating Systems
- ☐ Entertainment Software
- more +



Google Chrome

FREE

Make the most of the Web, like quick answers in your address bar, one-click translation, and more.

EDITORS' RATING ★★★★★ USER RATING ★★★★★
PUBLISHER: Google DOWNLOADS: 29,720,260



Google Chrome (64-bit)

FREE

Explore the Web using Google's super-fast browser.

EDITORS' RATING ★★★★★ USER RATING ★★★★★
PUBLISHER: Google DOWNLOADS: 685,161



Google Chrome Canary

FREE

Browse the Web with a version of Chrome that's more cutting-edge than the developer's build.

USER RATING ★★★★★
PUBLISHER: Google DOWNLOADS: 184,936



Google Chrome dev

FREE

Explore the Web in a safe and secure way.

USER RATING ★★★★★
PUBLISHER: Google DOWNLOADS: 141,667



Google Chrome

FREE

Make the most of the Web, like quick answers in your address bar, one-click translation, and more.


EDITORS' RATING ★★★★★ USER RATING ★★★★★
PUBLISHER: Google DOWNLOADS: 920,146

Figure: Multiple Versions.

Software Repositories


Systems

☐ Entertainment Software [more +](#)




Google Chrome
Make the most of the Web, like quick answers in your address bar, one-click translation, and more.
EDITORS' RATING ★★★★★ USER RATING ★★★★★
PUBLISHER: Google DOWNLOADS: 920,228

FREE




Google Chrome Portable
Take Google's Chrome browser with you on a USB stick.
USER RATING ★★★★★
PUBLISHER: PortableApps DOWNLOADS: 1,640,436


FREE




Click&Clean for Chrome
Delete your browsing history, typed URLs, of your online activity.
EDITORS' RATING ★★★★★ USER RATING ★★★★★
PUBLISHER: Mixrosoft DOWNLOADS: 51,134




Google Chrome beta
Explore the Web with the beta channel version of the browser.
EDITORS' RATING ★★★★★ USER RATING ★★★★★
PUBLISHER: Google DOWNLOADS: 965,045



Instagram for Chrome
Browse, like, and comment on all photos of your friends and celebrities.
EDITORS' RATING ★★★★★ USER RATING ★★★★★
PUBLISHER: 64 Pixels DOWNLOADS: 49,930




Google Chrome
Make the most of the Web, like quick answers in your address bar, one-click translation, and more.
EDITORS' RATING ★★★★★ USER RATING ★★★★★
PUBLISHER: Google DOWNLOADS: 920,228



Google Chrome Portable
Take Google's Chrome browser with you on a USB stick.
USER RATING ★★★★★
PUBLISHER: PortableApps DOWNLOADS: 1,640,436

Figure: Repackaging.

Software Repositories



Format Factory

March, 21st 2020 - 100% Safe - Freeware

[Features](#)
[Screenshots](#)
[Change Log](#)
[Old Versions](#)

Latest Version: Format Factory 5.1.0.0 LATEST

Requirements: Windows Vista / Windows 7 / Windows 8 / Windows 10 / Vista64 / Windows 7 64 / Windows 8 64 / Windows 10 64

User Rating: ★★★★★ Click to vote




Author / Product: [Free Time](#) / [Format Factory](#)

Old Versions: [Select Version](#)

Free Download

(76.4 MB) Safe & Secure

Share with Friends

Alternatives

Format Factory is a comprehensive **audio, video** and **image** converter and **riper** that will satisfy your every need, all in one easy to use **GUI** interface that can be used by everyone. **Format Factory** is a **multifunctional media converter**!

Free Download

(76.4 MB) Safe & Secure

Figure: **Security Checks.**

Software Repositories

Table: Repository Summary.

Repository	Uploaded By	Curated By	Sponsored	Ranking	Servers	Security Checks
FileHorse	Users	Site		✓	Internal/External	✓
Cnet	Users	Site		✓	External*	✓
FileHippo	Site	Site		✓	Internal	✓
SourceForge	Users	✗	✗	✗	Internal	✓
Softpedia	Users	Site		✗	Internal/External	✓

Research Questions

Repositories

- How often do they replace binaries?
- How fast do applications climb the rankings?

Installers

- How do installers work?
- Are they vulnerable?

Trojanization

- Are there trojanization evidences?
- Is Trojanization prevalent?

Methodology

Steps & Tools

- 1 Scrapy: Daily crawl installer binaries.
- 2 AutoIT: Automate installers execution on a sandbox.

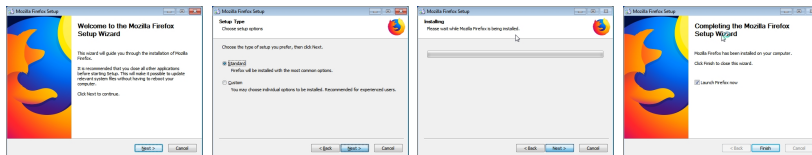


Figure: Automated Installation Example.

Agenda

- 1 Introduction
- 2 Repositories
- 3 Installers
- 4 Trojanization
- 5 Conclusion

Dataset

Table: Dataset overview. The number of unique files differs due to changes in distribution over time.

Repository	Programs (#)	Unique Files (#)
FileHorse	82	314
Cnet	118	295
FileHippo	433	906
SourceForge	99	631
Softpedia	901	897
Total	1,633	2,935

Table: File sharing among repositories. They usually do not share files for the same programs.

Repositories	Sharing Rate (%)
(Cnet, FileHorse)	48.04
(FileHippo, FileHorse)	17.65
(Cnet, FileHippo)	15.69
(FileHippo, Source Forge)	07.84
(Cnet, Softpedia)	04.90
(Cnet, Source Forge)	03.92
(FileHorse, Softpedia)	00.98
(FileHippo, Softpedia)	00.98

Dataset

Table: File types

distribution. Self-contained PE files are the prevalent type of program installers.

Type	Format	Prevalence (%)
Java		0.67
ISO		1.04
Compressed	7-zip 0.37	RAR 0.30
File	XZ 0.37	ZIP 20.47
Formats	bzip2 0.37	gzip 1.34
Windows	DOS 0.45	PE 65.63
Binaries	.Net 0.67	PE+ 0.45
Other		7.87

Table: Binary file's size

distribution. Small binaries are associated to downloaders and large ones to droppers.

Interval (MB)	Frequency	Binaries(%)
[0.000, 0.400)	93	5.42
[0.400, 1.400)	128	7.46
[1.400, 5.000)	242	14.11
[5.000, 70.000)	619	36.08
[70.000, 150.400)	145	8.45
[150.400, 600.400)	105	6.12
[600.400, 888.000)	16	0.93

Evolution

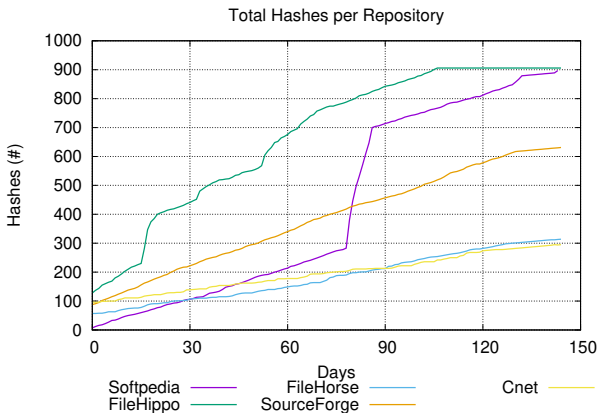


Figure: **Accumulative downloads** for each software repository.

Evolution

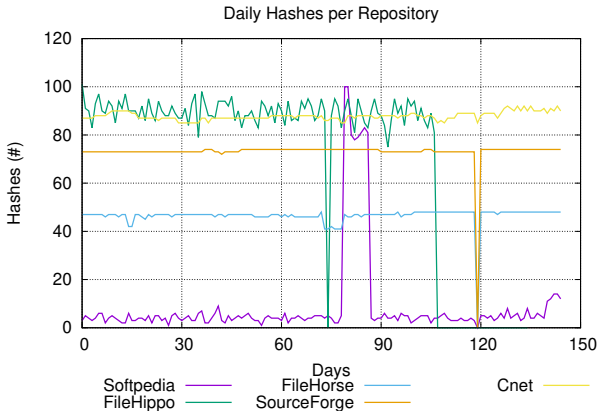


Figure: Daily Downloads. FileHippo's servers were unreachable in the last week.

Evolution Strategy 1: Adding a new repository entry

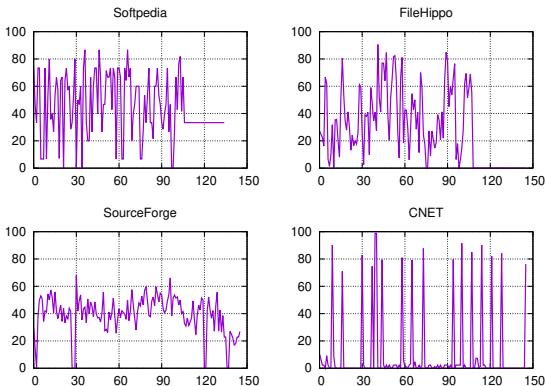


Figure: Ranking position changes of the top-100 downloaded programs in each repository, but FileHorse. Observation days vs. applications (#) whose rank changed.

Evolution Strategy 1: Adding a new repository entry

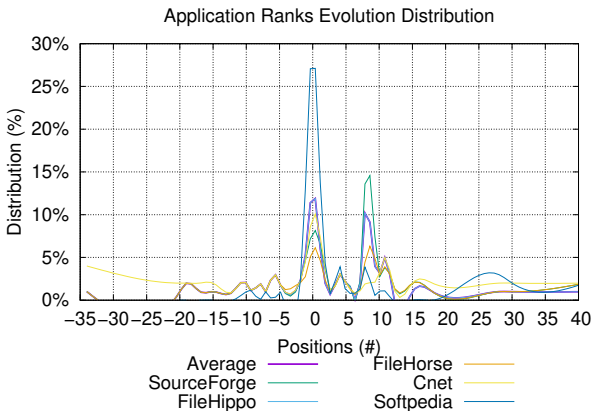


Figure: Distribution of Programs in Ranking Positions. Most programs increase their ranking position (at least once).

Evolution Strategy 2: Replacing an existing binary

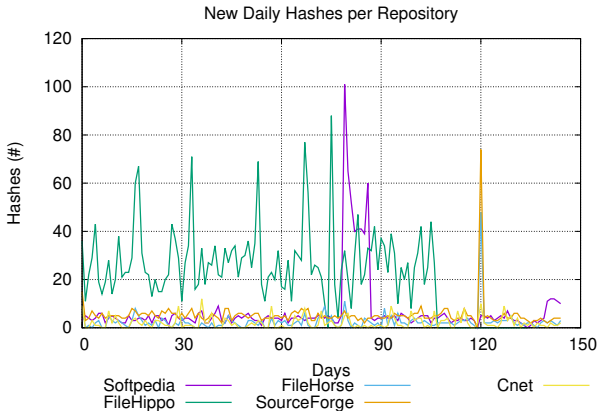


Figure: Download of new (unique) files. FileHippo's repository exhibits periodical peaks of newly added hashes.

Evolution Strategy 2: Replacing an existing binary

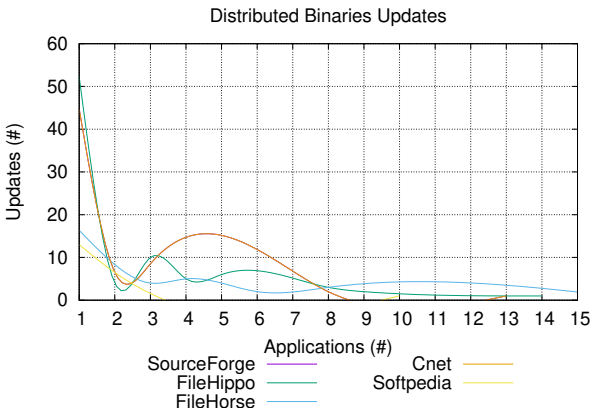


Figure: Distributed Binaries Updates. Most programs were updated few times, whereas some others, every week.

Agenda

- 1 Introduction
- 2 Repositories
- 3 Installers**
- 4 Trojanization
- 5 Conclusion

Installer Types

```
1 C:\installer.exe|Write|C:\Users\Win7\AppData\
   Local\Temp\{907A1104-E812-4b5c-959B-
   E4DAB37A96AB}\vsdrinst64.exe
2 C:\installer.exe|Write|C:\Users\Win7\AppData\
   Local\Temp\{907A1104-E812-4b5c-959B-
   E4DAB37A96AB}\Install.exe
```

Code 1: Dropper Installer. Some Installers drop embedded payloads to disk and launch them as new processes.

```
1 GET 200.143.247.9:80 (et1.zonealarm.com/V1?
2 TW9kdWxlPWluc3RhbgxlcH98U2Vzc2lvdj0wYzNjNDA1OD
   )
```

Code 2: Downloader Installer. Some Installers perform (encoded) network requests to retrieve payloads from Internet.

Downloaders

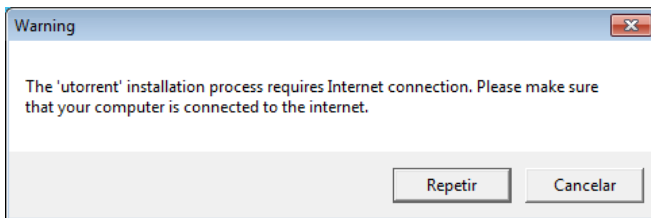


Figure: Internet-Based Installers. Some applications require Internet access for full software installation.

System Changes

Table: Top-5 file extensions most written by installers.

Extension	DLL	EXE	TMP	VPX	SYS
Files (#)	6,949	1,309	1,302	811	790

```
1 C:\Users\Win7\AppData\Local\Temp\BullGuard
  Backup Setup.exe|SetValueKey|HKU\<userid>\
  Software\Microsoft\Windows\CurrentVersion\
  Internet Settings|ProxyEnable|1
```

Code 3: Proxy Definition. Some installers change system-wide proxy settings.

Persistence

```
1 C:\Users\Win7\AppData\Local\Temp\7zS4DEAD364\
  Stub.exe | SetValueKey | HKU\<userid>\Software\
  Microsoft\Windows\CurrentVersion\RunOnce |
  PandaRunOnce |
```

Code 4: Persistence. Some installers set executable paths in the Registry to be executed after a system reboot.

```
1 C:\Users\Win7\AppData\Local\Temp\ajAE1E.exe |
  SetValueKey | HKLM\SOFTWARE\Wow6432Node\AVAST
  Software\Browser | installer_run_count | 1
```

Code 5: Multi-Step Installers. They control how many times they will run.

Network Usage

```
1 GET iavs9x.u.avast.com/iavs9x/  
   avast_free_antivirus_setup_online_x64.exe  
2 GET download.bitdefender.com/windows/bp/all/  
   avfree_64b.exe  
3 GET iavs9x.avg.u.avcdn.net/avg/iavs9x/  
   avg_antivirus_free_setup_x64.exe  
4 GET dm.kaspersky-labs.com/en/KAV/19.0.0.1088/  
   startup.exe  
5 GET download.bullguard.com/  
   BullGuard190AV_x64_190411.exe
```

Code 6: Unencrypted Download by Installers. The use of HTTP-only connections may make users vulnerable.

Network Attacks

Bad Practice

- <https://www.youtube.com/watch?v=dRI0J9TGqy4>

Good Practice

- <https://www.youtube.com/watch?v=vGrLbFlyXb0>

Installation Tracking

```
1 GET /v1/offer/campaignFilter/?bundleId=UT006&
   campaignId=5b6352b3ce72513ae0a6beef
2 GET sos.adaware.com|/v1/offer/campaignFilter/?
   bundleId=UT006&campaignId=5
   b6352b3ce72513ae0a6beef
3 GET flow.lavasoft.com|/v1/event-stat?ProductID
   =IS&Type=StubBundleStart
```

Code 7: Installation Tracking. Some installers sent back tracking information to notify providers about the installation.

Uninstallers

```
1 C:\Users\Win7\AppData\Local\Temp\{907A1104-  
   E812-4b5c-959B-E4DAB37A96AB}\Install.exe |  
   Create|C:\Users\Win7\AppData\Local\Temp  
   \{907A1104-E812-4b5c-959B-E4DAB37A96AB}\  
   Uninst.exe
```

Code 8: Uninstaller Definition. Some Installers set
uninstallers for the applications.

```
1 C:\Users\Win7\AppData\Local\Temp\{907A1104-  
   E812-4b5c-959B-E4DAB37A96AB}\Install.exe |  
   Create|C:\Users\Win7\AppData\Local\Temp  
   \{907A1104-E812-4b5c-959B-E4DAB37A96AB}\  
   Uninst.exe
```

Code 9: Uninstaller Definition. Some Installers set
uninstallers for the applications.

Installers Evolution

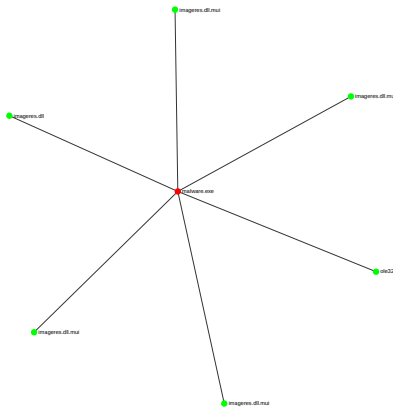


Figure: First CCleaner Installer. File access rates are very homogeneous.

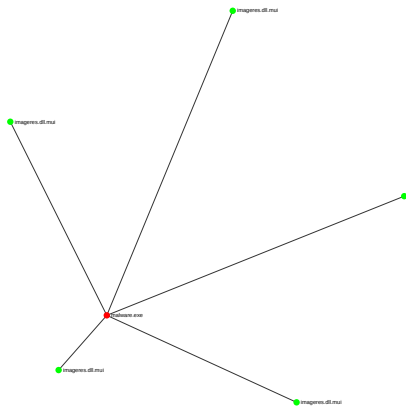


Figure: Second CCleaner Installer. Some files are more accessed than others.

Third-Party Components

```
1 C:\installer\3rdPartyApp\GoogleToolBar\  
   GoogleToolbarInstaller_zh-TW.exe
```

Code 10: Google Toolbar. It is embedded as third-party extensions of the main application.

```
1 HKCU\Software\Microsoft\Internet Explorer\  
   LinksBar\ItemCache\ToolBar\Add
```

Code 11: IE Settings Modification. New bookmarks, cookies, and configurations set in the browser.

```
1 C:\Users\Win7\AppData\Local\Temp\is-3ACQL.tmp\  
   Advertising_english.exe
```

Code 12: Adware. The advertisement software is dropped from a file created by the main installer.

Targeting & Fingerprintg

```
1 C:\Setup.exe | SetValueKey | HKCU\<userid>\  
   Software\Microsoft\SQMClient\UserId | {  
   C2CFE0D4-A3A2-4458-A73F-F16F10E4C0D7}  
2 C:\Setup.exe | SetValueKey | HKCU\<userid>\  
   Software\Microsoft\SQMClient\UserId | {  
   EA0CB74D-DB5D-40EE-A402-47A97F23904E}  
3 C:\Setup.exe | SetValueKey | HKCU\<userid>\  
   Software\Microsoft\SQMClient\UserId | {  
   E81A6607-9EB3-49BA-B354-FA42817594BA}
```

Code 13: Tracking IDs of installers of distinct repositories.

Each installer presents a distinct tracking ID according the repository from which they were downloaded.

Agenda

- 1 Introduction
- 2 Repositories
- 3 Installers
- 4 Trojanization**
- 5 Conclusion

Popularity

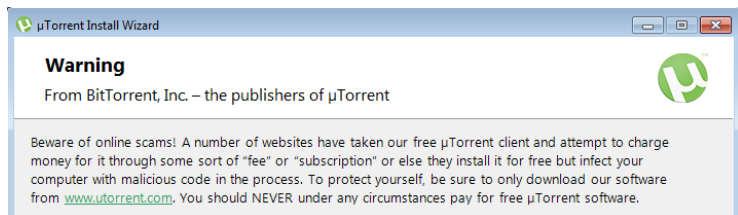


Figure: Security Warning. Trojanization has become popular to the point of some installers warning users about this possibility.

AV Scans

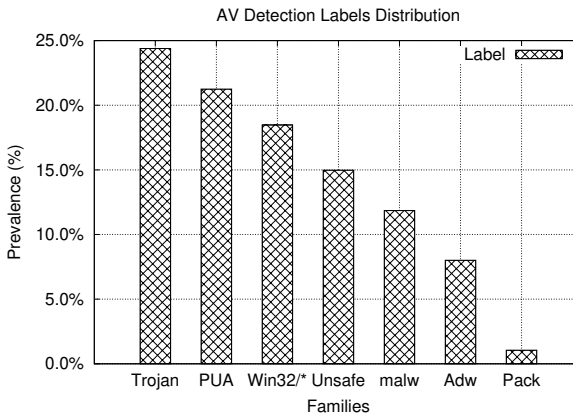


Figure: AV Labels Distribution. Many samples were considered either as malicious or as Trojanized.

AV Scans

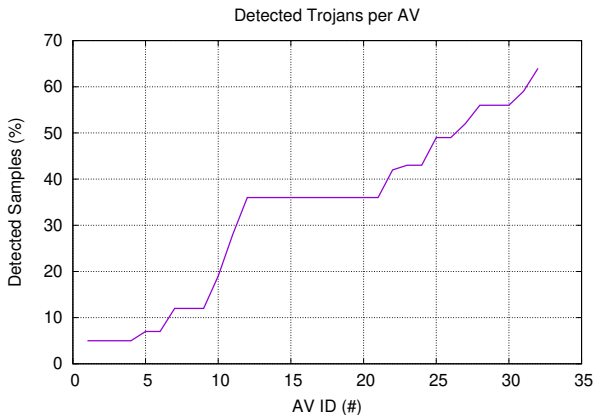


Figure: Trojanized Apps Detection per AV. Distinct AVs present very distinct criteria and thus detection rates.

Repositories

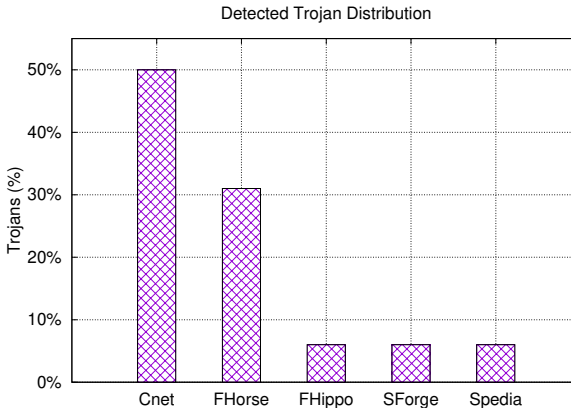


Figure: Trojanized Apps Detection per Repository. Distinct repositories present very distinct rates.

Agenda

- 1 Introduction
- 2 Repositories
- 3 Installers
- 4 Trojanization
- 5 Conclusion**

Implications

For Users

- Always prefer downloading from the official source.

For Repositories

- Pay special attention to popular applications.

For Researchers

- Scan binaries before assuming goodware ground-truth.
- Make hashes available to ensure reproducibility.

Thank You

Contact

- **E-mail:** mfbotacin@inf.ufpr.br
- **Twitter:** @MarcusBotacin

Source Code

- **Github:** [https://github.com/marcusbotacin/
Application.Installers.Overview](https://github.com/marcusbotacin/Application.Installers.Overview)