On the Security of Application Installers & Online Software Repositories

Marcus Botacin[1] Giovanni Bertão[2] Paulo de Geus[2] André Grégio[1]
Christopher Kruegel[3] Giovanni Vigna[3]

[1]Federal University of Paraná – Brazil (UFPR)
{mfbotacin,gregio}@inf.ufpr.br
[2]University of Campinas – Brazil (UNICAMP)
{bertao,paulo}@lasca.ic.unicamp.br
[3]University of California at Santa Barbara – USA (UCSB)
{chris,vigna}@ucsb.edu

2020

Agenda

Agenda

Apps Stores

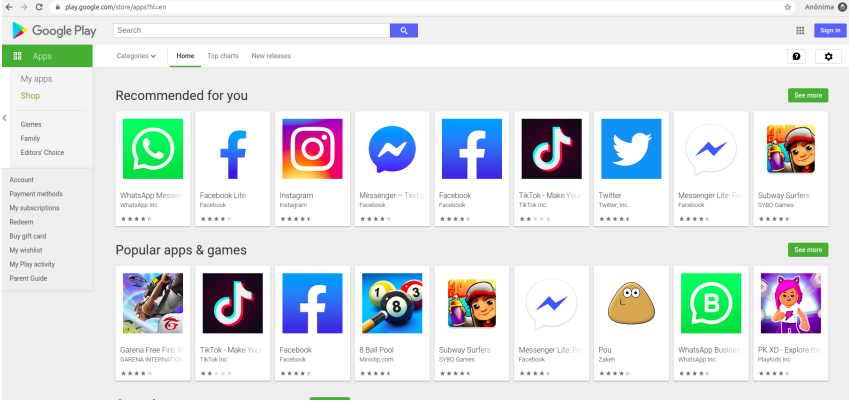

Figure: **Android's App Store.**

Desktop Software Repositories

Figure: **Evaluated Repositories.**

Software Repositories

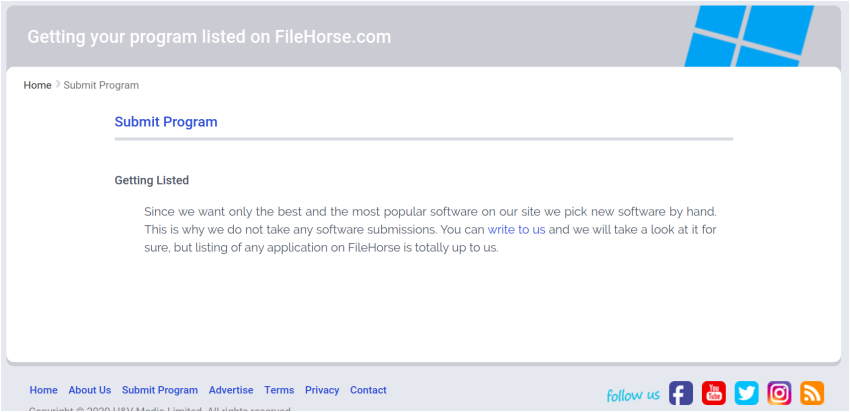

Figure: **Software Inclusion.**

Software Repositories

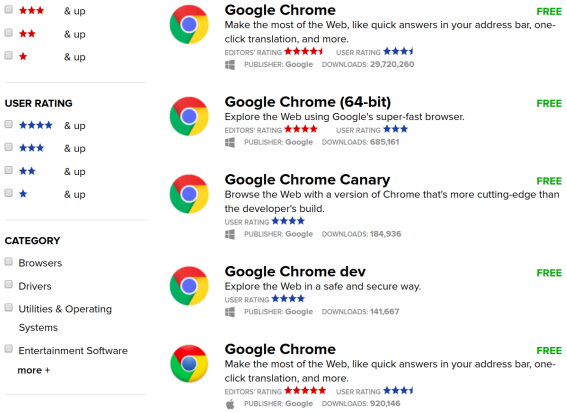

Figure: **Multiple Versions.**

Software Repositories

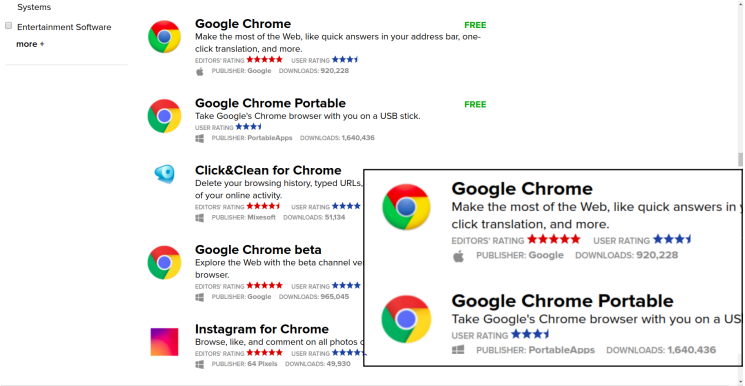

Figure: **Repackaging.**

Software Repositories

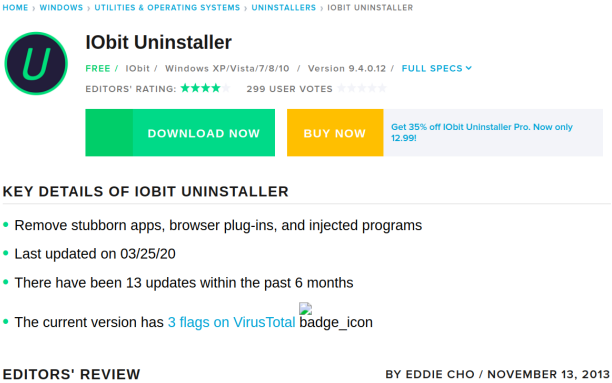

Figure: **Binary Replacement.**

Software Repositories

Figure: **Security Checks.**

Software Repositories

Table: **Repository Summary.**

Repository	Uploaded By	Reviewed 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

- Is there evidence of Trojanization?
- Is Trojanization prevalent?

Methodology

Steps & Tools

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

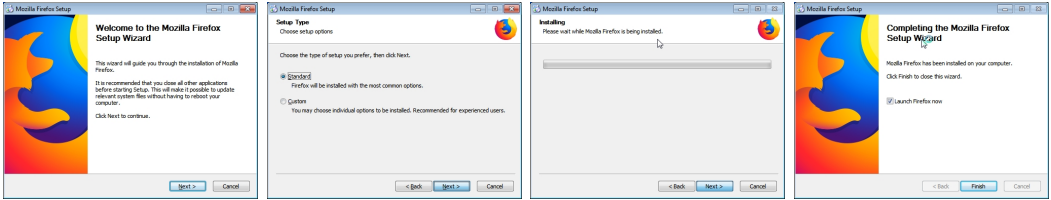

Figure: **Automated Installation Example.**

Agenda

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 File Formats	7-zip 0.37	RAR 0.30
	XZ 0.37	ZIP 20.47
	bzip2 0.37	gzip 1.34
Windows Binaries	DOS 0.45	PE 65.63
	.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

Installers Collection

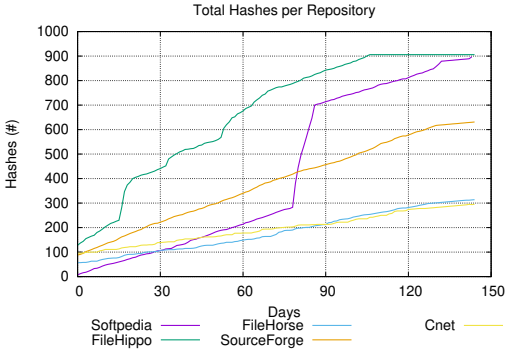

Figure: **Accumulative downloads** for each software repository.

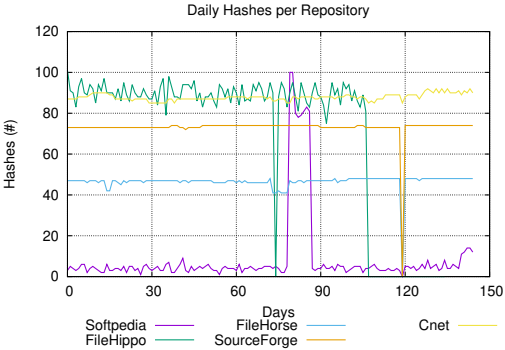

Figure: **Daily Downloads.** FileHippo's servers were unreachable in the last week.

Evolution Strategy 1: Adding a new repository entry[1]

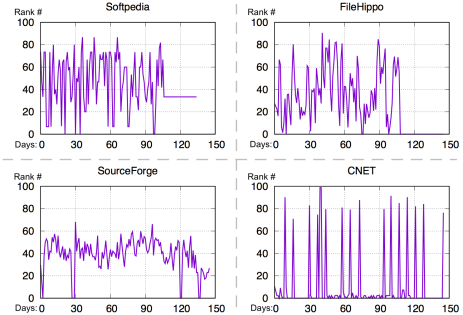

Figure: **Ranking position changes** of the top-100 downloaded programs.

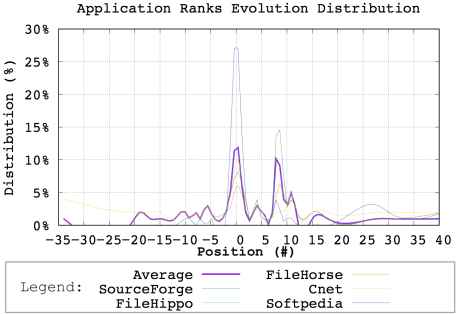

Figure: **Distribution of Programs in Ranking Positions.**

[1] Hypothesized based on the behavior of all installers, not only Trojanized ones.

Evolution Strategy 2: Replacing an existing binary[2]

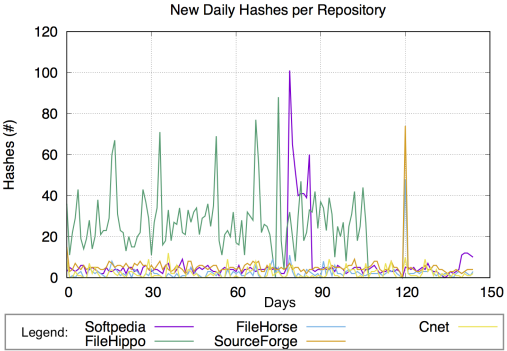

Figure: **Download of new (unique) files.**

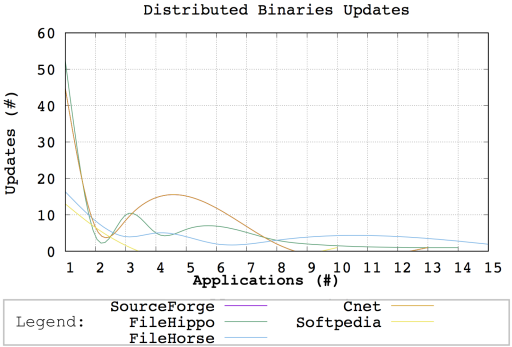

Figure: **Distributed Binaries Updates.**

[2] Hypothesized based on the behavior of all installers, not only Trojanized ones.

Agenda

Installer Types

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

```
GET 200.143.247.9:80 (et1.zonealarm.com/V1?
TW9kdWxlPWluc3RhbGxlch98U2Vzc2lvbj0wYzNjNDA1OD)
```

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

Downloaders

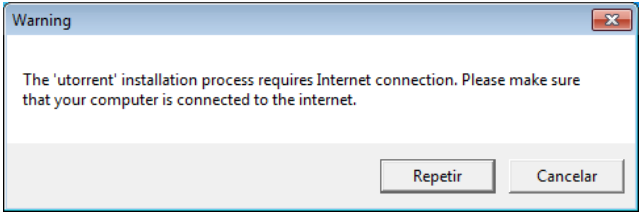

Figure: **Internet-Based Installers.** Some applications require Internet access for full software installation.

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

```
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

```
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.

```
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

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

```
GET /v1/offer/campaignFilter/?bundleId=UT006&campaignId=5b6352b3ce72513ae0a6beef
GET sos.adaware.com|/v1/offer/campaignFilter/?bundleId=UT006&campaignId=5b6352b3ce72513ae0a6beef
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

```
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.

```
C:\Program Files (x86)\GUM5D5C.tmp\fmanUpdate.exe|SetValueKey
    ||HKU\<userid>\Software\fman\Update|UninstallCmdLine|"C:\
    Users\Win7\AppData\Local\fman\Update\fmanUpdate.exe" /
    uninstall
```

Code 9: **Parameter-Based Uninstallers.** They define command line parameters for software removal.

Third-Party Components

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

Code 10: **Google Toolbar** embedded as third-party extension of the main app.

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

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

```
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 & Fingerprinting

```
C:\Setup.exe|SetValueKey|HKCU\<userid>\Software\Microsoft\
    SQMClient|UserId|{C2CFE0D4-A3A2-4458-A73F-F16F10E4C0D7}
C:\Setup.exe|SetValueKey|HKCU\<userid>\Software\Microsoft\
    SQMClient|UserId|{EA0CB74D-DB5D-40EE-A402-47A97F23904E}
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

Popularity

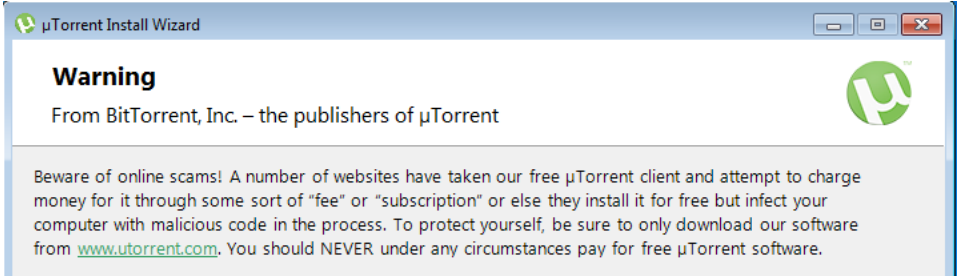

Figure: **Security Warning.** Trojanization has become popular to the point of some installers warning users about this possibility.

AV Scans

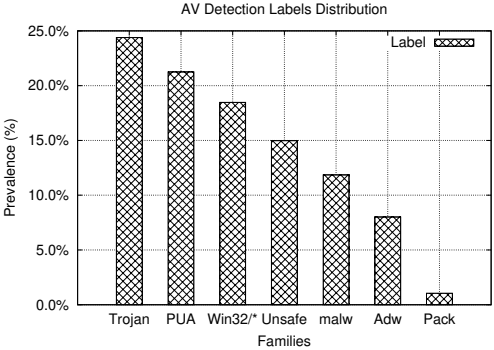

Figure: **AV Labels Distribution.** Many samples were considered either as malicious or as Trojanized.

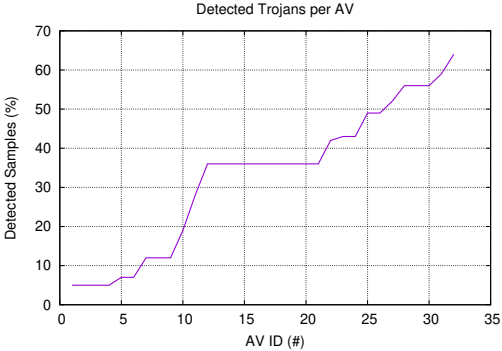

Figure: **Trojanized Apps Detection per AV.** Distinct AVs present very distinct criteria and thus detection rates.

Repositories

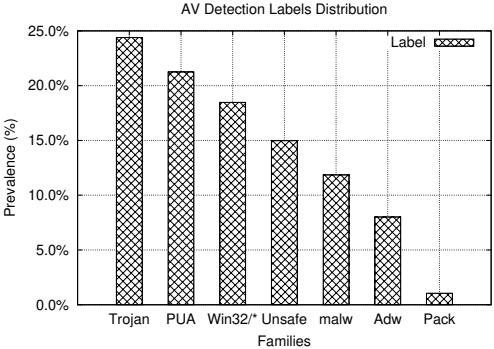

Figure: **AV Labels Distribution.** Many samples were considered either as malicious or as Trojanized.

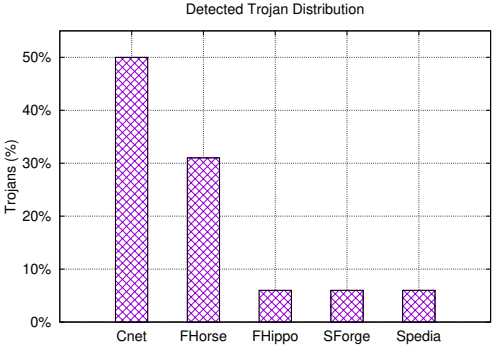

Figure: **Trojanized Apps Detection per Repository.** Distinct repositories present very distinct rates.

Agenda

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.

A Possible Future

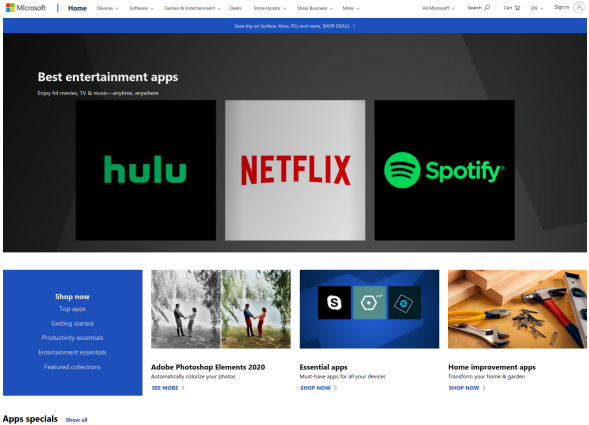

Figure: **Microsoft's App Store.**

Thank You!

Contact

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

Source Code

- **Github:**
  `https://github.com/marcusbotacin/Application.Installers.Overview`

Multiple Apps Versions

```
apocalypse@demise:find . -name "*Skype*"
./a1e345498c89f31d6576333228 4b4aa3/bin/Skype.exe
./208d150aef1cca9956f763878153bde7/bin/Skype.exe
./7d1e3fc65e117485e16326dc3c7387da/bin/Skype.exe
./6b30b75c6008a7beb12af23928698862/bin/Skype.exe
./dce4e3f1310e0e2a7fdcd0a5b11ca01a/bin/Skype.exe
./2a0c34eec72b233c4f89b5347f381297/bin/Skype.exe
./c255d16ad06aa1d1563b6670e767945c/bin/Skype.exe
./8cbbdf4c6e2be9b16039b03f36318be3/bin/Skype.exe
./45ed9696f86419239b3fc3647356ad88/bin/Skype.exe
./2e42376b834735e2cd48de5b4467707b/bin/Skype.exe
./dd18a745a900a6ef24fde30ca3f06877/bin/Skype.exe
./5c0afbd59656cb48b01bd9da668ff657/bin/Skype.exe
./66ea1ca7d3f3bc4bce8d517f746c27f2/bin/Skype.exe
./4deba6929be3eb8ecbc76647821ae96d/bin/Skype.exe
./927aa920c9d61b3e047b3a315c916ded/bin/Skype.exe
./3b7f6ab75ece6d88b6523e967b7a294f/bin/Skype.exe
```

Figure: Multiple Skype Versions.

```
apocalypse@demise:find . -name "*Chrome*"
./0a794408e82e0fedfba7e34cd3d50c93/bin/Google_Chrome.exe
./3a619481c57511014e36154c0c39120d/bin/Google_Chrome.exe
./cda51365130b7eed14fa6d8cf3e6c0bd/bin/Google_Chrome.exe
./5cee85a622fd3f100f534408e637599e/bin/Google_Chrome.exe
./1e5a43d283e35ae1d0d53eb18505e3cb/bin/Google_Chrome.exe
./9c3ab36d50d438639909a82415e7af1c/bin/Google_Chrome.exe
./18ebdc6aa251b1ba9dba7f9072100417/bin/Google_Chrome.exe
./98b6115d215b2e2bd928ca2e4d6bc59d/bin/Google_Chrome_Canary
./92a45c2781e05a0ff3f500bde3bb5626/bin/Google_Chrome.exe
./4ce907a1a773c8ac53a6117999ce702c/bin/Google_Chrome.exe
./bb5361f74358f83f140b7134a3ed1ec2/bin/Google_Chrome.exe
./69ea19438a35e20abceac0c16cffba25/bin/Google_Chrome.exe
```

Figure: Multiple Chrome Versions.

Installer's Policies

Action

"*We collect some limited information that your device and browser routinely make available whenever you visit a website or interact with any online service.*"

Goal

"*We collect this data to improve the overall quality of the online experience, including product monitoring, product improvement, and targeted advertising.*"

Scope

"*We may also include offers from third parties as part of the installation process for our Software.*"

Integrity Checking (Other Platforms)


```
[
 {
   "caminhoDownload": "https://staticext-bi.safra.com.br/dist/apl-mobile-pf/apl-mobile-pf-3.7.65.zip",
   "hash": "0fb6aa5859a2bbf0077e8c309926b7c50accc4ddd78edb17715cc7cdbb5f4fd0",
   "versaoAtual": "3.7.65",
   "modulo": "apl-mobile-pf",
   "versaoMinima": "3.7.65"
 }
]
```


Figure: Integrity check on a bank's app.

Thank You (Once Again)!

Contact

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

Source Code

- **Github:**
  `https://github.com/marcusbotacin/Application.Installers.Overview`