Analýza prebaleného Telegramu a Signalu pomocou pozorovacích a bezpečnostných nástrojov

Vedúci: doc. RNDr. Daniel Olejár, PhD.

Konzultant: Mgr. Peter Košinár – ESET

Ing. Bc. Jakub Škoda

Čo skúmame?

Repackaging attacks – príklad

09:36 4G

Google Play

Signal Plus messenger

Brad Shannon

INSTALL

Signal Plus is a modified instantaneous communication App of the original Signal

READ MORE

Ratings and reviews

16:10 77%

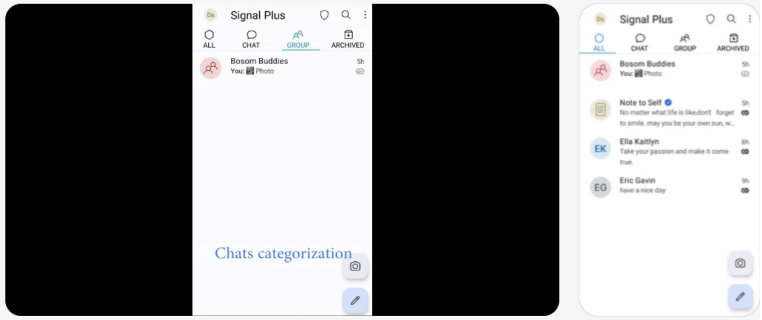
Signal Plus Messenger

Brad Shannon

Rated 12+

#Social media

5.0



What's new

Bug fixes.

Description

Signal Plus is a modified instantaneous communication App of the original Signal with additional features that

Repackaging attacks – príklad

- útok prebiehal od júla 2022 do mája 2023
- malvér verzia Signalu - Signal Plus Messenger
- dostupná na Google Play a Samsung Galaxy Store
- vie extrahovať číslo PIN, ktoré ochraňuje Signal účet
- zneužíva funkciu `Pripojené zariadenia`, ktorá prepája hlavnú aplikáciu Signal (Android a iOS) so Signal Desktop a Signal iPad

Repackaging attacks – charakteristika

- zoberieme legitímnu aplikáciu a dodáme do nej kód navyše
- často ju prezentujeme ako vylepšenú aplikáciu

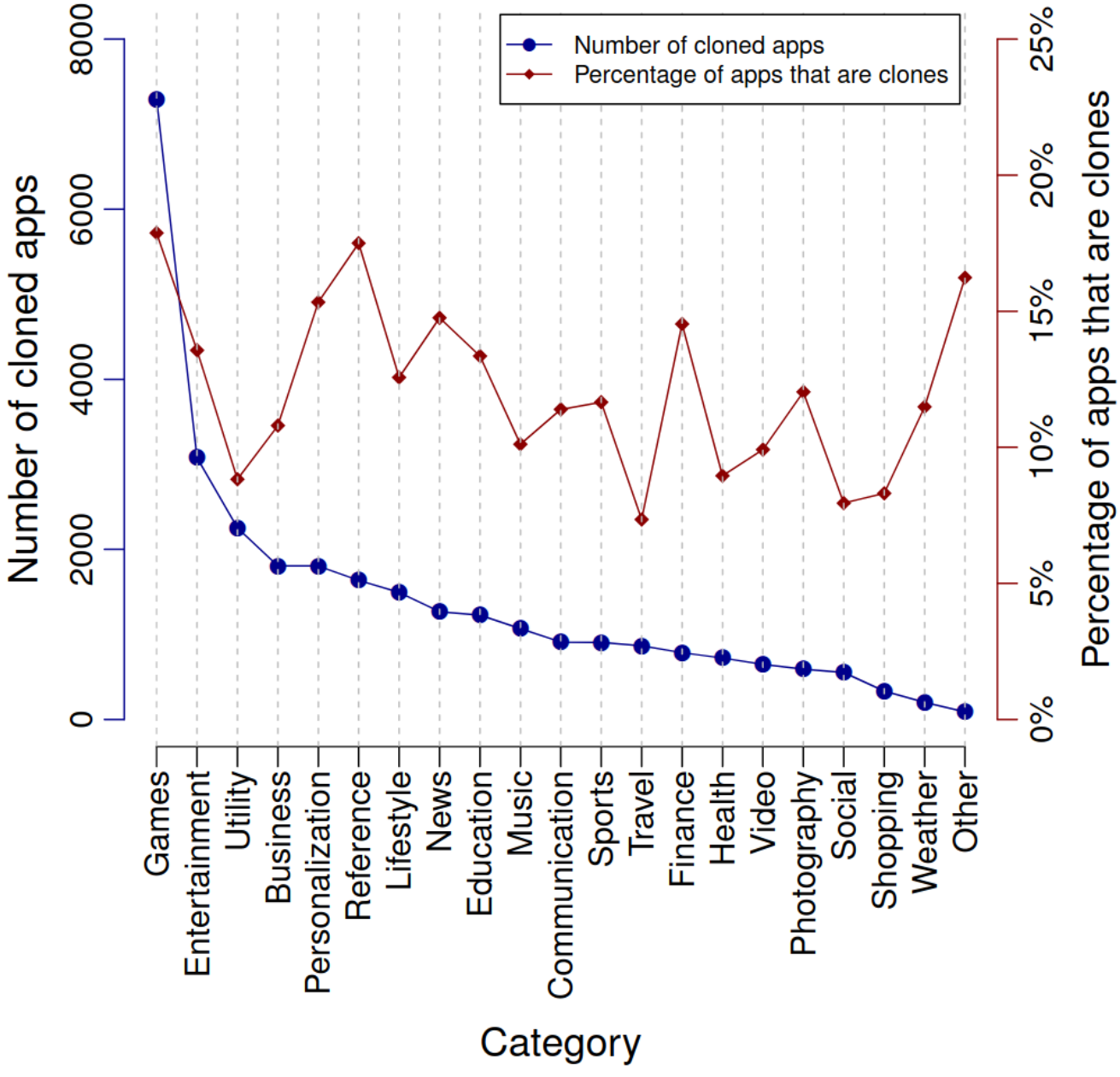
občas upravená verzia nemusí byť hneď malvér

- “iba” adware nie malvér
  - pokles príjmov z reklamy o 14 % pre vlastníka aplikácie (Gibler et al. 2013)

Čo nie je repackaging attack

- neoficiálne modifikácie
- forky open-source aplikácií
- white-label aplikácie

Repackaging attacks – incidencia



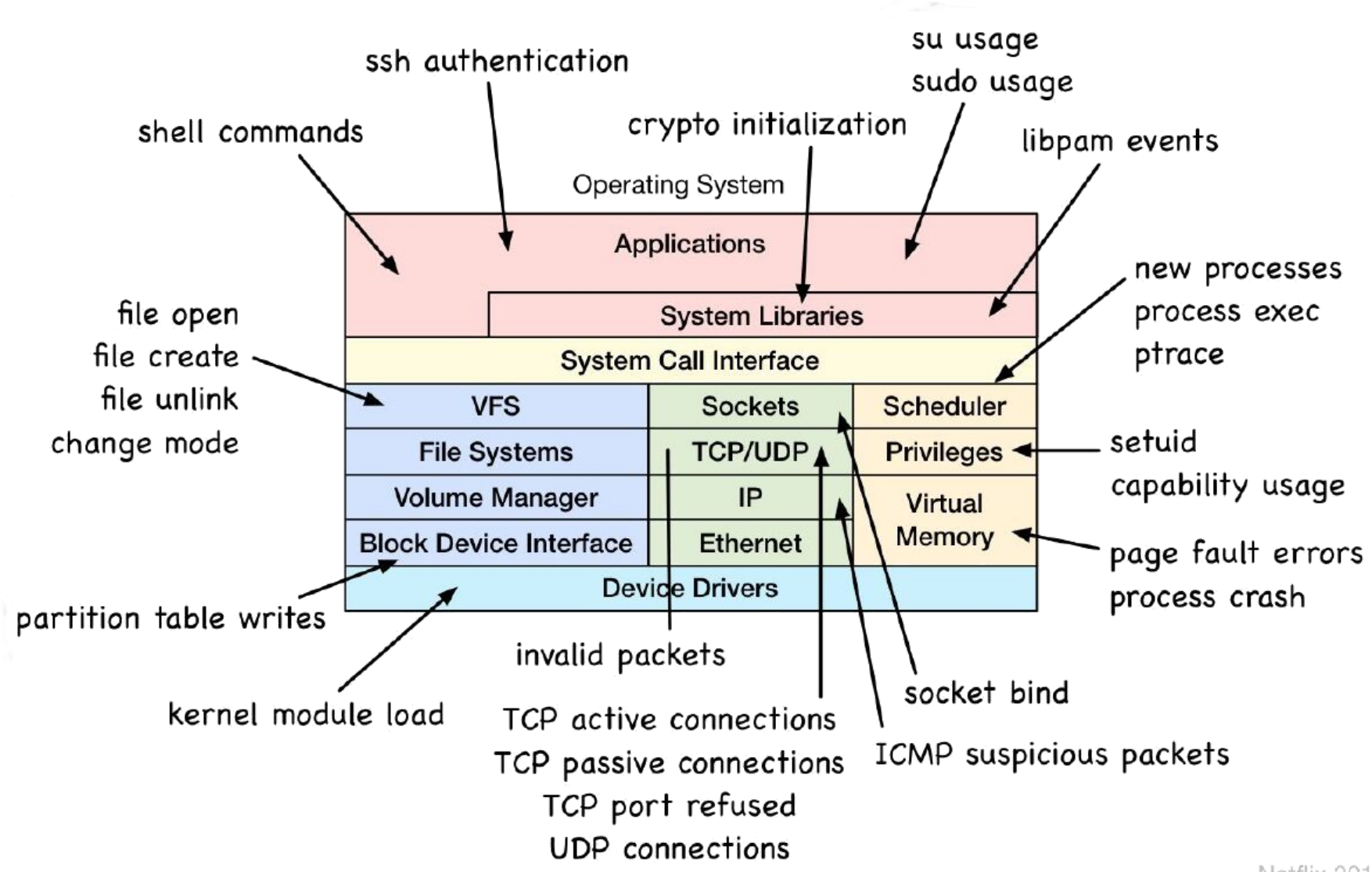
(Gibler et al. 2013)

Repackaging attacks – incidencia

- veľmi populárne v období vzniku Androidu
- (Zhou and Jiang 2012) – 1 083 malvéru z 1 260 (86 %) aplikácií v obchodoch s aplikáciami bol práve repackaging attack
- (Gibler et al. 2013) – 44 268 (16,7 %) z 265 359 aplikácií zadarmo boli klonované aplikácie

Ako to skúmame?

Linux tracing – nástroje



(Gregg 2017)

Metódy skúmania

reverzné inžinierstvo

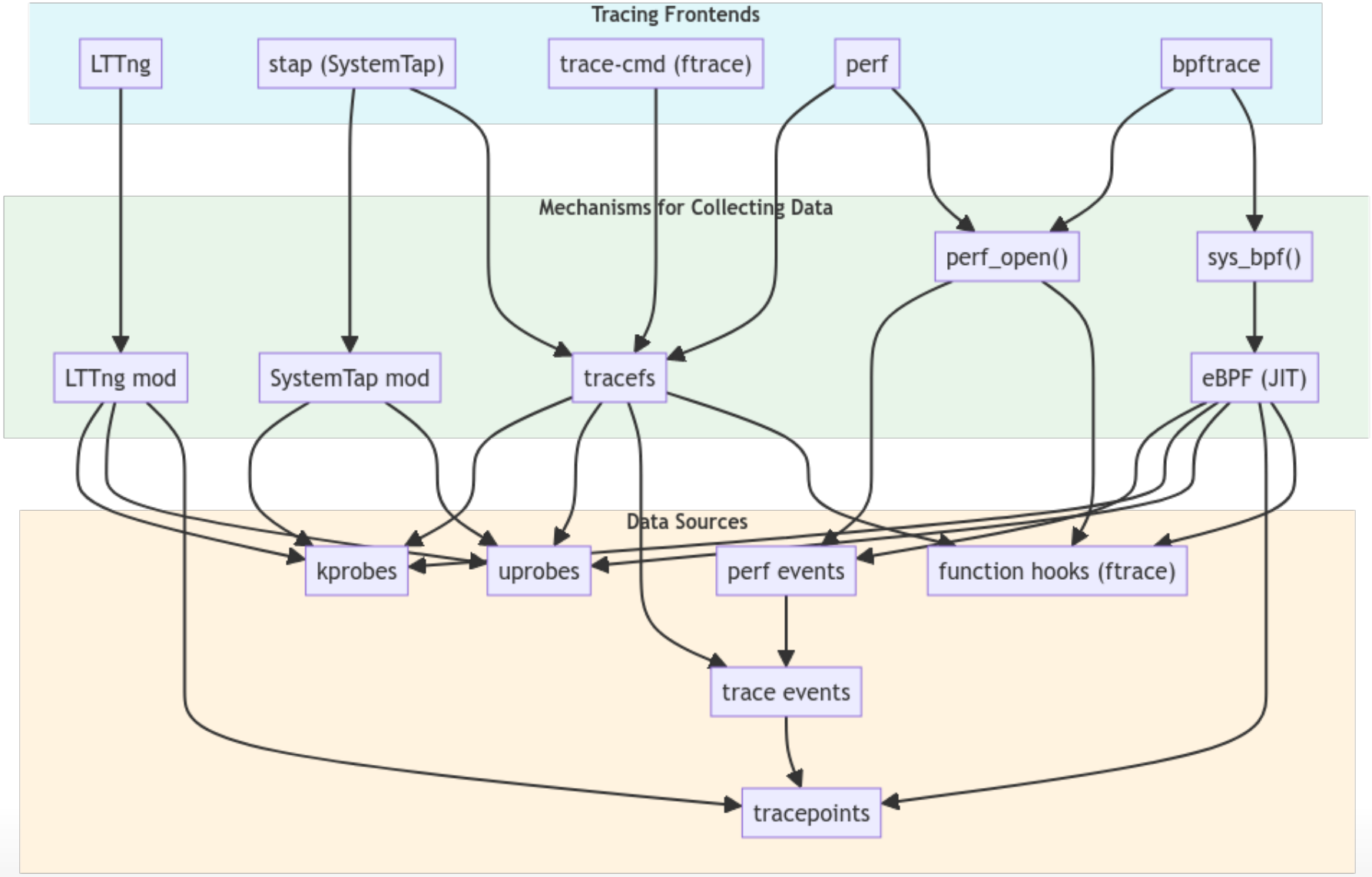
- získaj kód pre originálnu a modifikovanú aplikáciu
- porovnaj a nájdi podozrivý kód

pozorovanie

- pozoruj obe aplikácie
- zisti, akú operáciu navyše spraví modifikovaná aplikácia

Čo presne používame?

Linux tracing – nástroje



vlastné spracovanie

eBPF

- použili sme eBPF pomocou BCC toolkit
- BCC vykonáva väčšinu tracingu na úrovni kernelu
- umožňuje rýchle vyhľadávanie
- pomocou BCC sme napísali vlastný program, ktorý zachytáva naraz všetko, čo potrebujeme

plná verzia na <https://github.com/IacobusKopiirefuto/anbako-BCC

eBPF

pozreli sme sa na systémové volania

- TCP aktívne spojenia pomocou `connect()`
- otvorené súbory pomocou `open()`
- nové procesy pomocou `exec()`

Je signal-cli legitímna aplikácia?

signal-desktop a signal-cli

signal-desktop

- oficiálna verzia pre Linux od developerov Signalu
- grafické rozhranie založené na Electron frameworku

signal-cli

- neoficiálny projekt
- umožňuje ovládanie Signalu cez príkazový riadok
- vhodný ako základ pre ďalšie projekty
  - jednoduché ncurses GUI
  - automatizované posielanie správ (napríklad odosielanie logov)

connect

Pripájanie sa k doménam nesúvisiacich so službou môže naznačovať nekalé posielanie alebo získavanie dát.

Z informácií zo SignalComunity a zdrojového kódu sme vopred vedeli, na aké domény sa má Signal pripájať.

signal-desktop aj signal-cli sa podľa našej analýzy pripájali len na očakávané domény.

Jediný rozdiel bol v tom, že signal-cli používa IPv4 a signal-desktop IPv6.

connect: signal-desktop

PID	COMM	DADDR	DPORT	QUERY
13646	signal-deskt	2600:9000:a61f:527c:	443	chat.signal.org
		d5eb:a431:5239:3232		
13646	signal-deskt	2606:4700:4400::ac40:966c	443	cdn2.signal.org
13646	signal-deskt	2606:4700:4400::ac40:966c	443	cdn2.signal.org
13646	signal-deskt	2606:4700:4400::ac40:966c	443	cdn2.signal.org
13646	signal-deskt	2a00:1450:4014:80e::2013	443	storage.signal.org
13646	signal-deskt	2600:9000:a61f:527c:	443	chat.signal.org
		d5eb:a431:5239:3232		
13646	signal-deskt	2600:9000:2611:9200:	443	cdn.signal.org
		1d:4f32:50c0:93a1		

connect (receiving message): signal-cli

PID	COMM	DADDR	DPORT	QUERY
11084	signal-cli	13.248.212.111	443	chat.signal.org
11084	.signal.org/	13.248.212.111	443	chat.signal.org
11084	.signal.org/	13.248.212.111	443	chat.signal.org
11084	tokio-runtim	2603:1030:7::1	443	cdsi.signal.org
11084	signal-cli	104.18.37.148	443	cdn2.signal.org
11084	pool-6-threa	3.161.119.11	443	cdn.signal.org
11084	pool-6-threa	142.251.36.147	443	storage.signal.org

connect (sending message): signal-cli

PID	COMM	DADDR	DPORT	QUERY
11084	signal-cli	13.248.212.111	443	chat.signal.org
11084	.signal.org/	13.248.212.111	443	chat.signal.org
11084	.signal.org/	13.248.212.111	443	chat.signal.org
11084	tokio-runtim	2603:1030:7::1	443	cdsi.signal.org
11084	signal-cli	104.18.37.148	443	cdn2.signal.org
11084	pool-6-threa	3.161.119.11	443	cdn.signal.org
11084	pool-6-threa	142.251.36.147	443	storage.signal.org

open

Ak program pristupuje k súborom, ktoré by sme neočakávali, môže sa jednať o nekalé získavanie a upravovanie dát alebo enumeráciu.

Nakoľko signal-cli nevyužíva komplexné GUI, jeho legitímnosť sa dala veľmi ľahko overiť.

Pristupoval k rovnakým súborom ako signal-desktop, ale bolo ich výrazne menej.

open: signal-desktop aj signal-cli

- `/etc/passwd`,
- `/dev/urandom`
- `/etc/ld.so.cach`
- `/etc/nsswitch.conf`
- `/etc/resolv.conf`
- `/sys/devices/system/cpu/possible`
- `/proc/stat`
- `/proc/self/maps`
- `/proc/self/fd`
- `/run/systemd/machines/chat.signal.org`.

open: signal-desktop

vlastné (konfiguračné) súbory:

- `/usr/lib/signal-desktop/`
- `~/.config/Signal`

súbory potrebné pre Electron GUI, fonty a ikonky:

- `/usr/share/fonts`, `~/.local/share/fonts/`, `~/.fontconfig`, `/.cache/fontconfig/`
- `~/.icons/`, `~/.local/share/icons`
- `/dev/shm/.org.chromium.Chromium.*`, `/tmp/.org.chromium.Chromium.*`

open: signal-cli

vlastný priečinok

`~/.local/share/signal-cli`

používateľské knižnice

- `/usr/lib/`

exec

Ak by program spúšťal neočakávané príkazy, mohlo by to znamenať, že vykonáva aj inú činnosť než by mal.

signal-desktop spúšťa rôzne procesy súvisiace s Electronom s dlhým zoznamom flagov.

signal-cli bolo znova menej komplexné, pomocou shellu iba zistilo nastavenie terminálu a operačný systém.

exec: signal-desktop

PID	COMM	PPID	RET	ARGS
13546	signal-desktop	13541	0	“/usr/bin/signal-desktop”
13549	signal-desktop	13546	0	“/usr/lib/signal-desktop/signal-desktop” “–type=zygote” “–no-zygote-sandbox”
13550	signal-desktop	13546	0	“/usr/lib/signal-desktop/signal-desktop” “–type=zygote”
13566	xdg-settings	13546	0	“/usr/bin/xdg-settings” “set” “default-url-scheme-handler” “sgnl” “signal.desktop”
13582	xdg-settings	13546	0	“/usr/bin/xdg-settings” “set” “default-url-scheme-handler” “signalcaptcha” “signal.desktop”
13616, 13646, 13679	exe	13546	0	(see next slides)

exec: signal-desktop

PID	COMM	PPID	RET	ARGS
13616	exe	13546	0	“/proc/self/exe” “–type=utility” “–utility-sub-type=network.mojom.NetworkService” “–lang=en-US” “–service-sandbox-type=none” “–enable-crash-reporter=f7e9ea8d-135d-4de5-a67c-95010fb400d7,no_channel” “–user-data-dir=/home/jackie/.config/Signal” “–shared-files=v8_context_snapshot_data:100” “–enable-features=kWebSQLAccess” “–variations-seed-version”

exec: signal-desktop

PID	COMM	PPID	RET	ARGS
13646	exe	13546	0	“/proc/self/exe” “–type=renderer” “–enable-crash-reporter=f7e9ea8d-135d-4de5-a67c-95010fb400d7,no_channel” “–user-data-dir=/home/jackie/.config/Signal” “–app-path=/usr/lib/signal-desktop/resources/app.asar” “–no-sandbox” “–no-zygote” “–enable-blink-features=CSSPseudoDir,CSSLogical” “–first-renderer-process” “–disable-gpu-compositing” “–lang=en-US” “–num-raster-threads=2” “–enable-main-frame-before-activation” “–renderer-client-id=4” “–time-ticks-at-unix-epoch=-1715236720975010” “–launch-time-ticks=25421136890” “–shared-files=v8_context_snapshot_data:100” “–enable-features=kWebSQLAccess” “”

exec: signal-desktop

PID	COMM	PPID	RET	ARGS
13679	exe	13546	0	“/proc/self/exe” “–type=utility” “–utility-sub-type=audio.mojom.AudioService” “–lang=en-US” “–service-sandbox-type=none” “–enable-crash-reporter=f7e9ea8d-135d-4de5-a67c-95010fb400d7,no_channel” “–user-data-dir=/home/jackie/.config/Signal” “–shared-files=v8_context_snapshot_data:100” “–enable-features=kWebSQLAccess” “–variations-seed-version”

exec: signal-cli

PCOMM	PID	PPID	RET	ARGS
signal-cli	11234	10307	0	“./signal-cli -u +421909104930 send -m "Hello, how are you?" +421909543173”
sh	11237	11234	0	“/usr/bin/sh -c stty -a < /dev/tty”
stty	11239	11237	0	“/usr/bin/stty -a”
sh	11240	11234	0	“/usr/bin/sh -c stty -a < /dev/tty”
stty	11241	11240	0	“/usr/bin/stty -a”
uname	11242	11234	0	“/usr/bin/uname -o”

Záver

Výsledok

Vytvorili sme aplikáciu využívajúcu eBPF, ktorá po spustení už sama vygenerovala potrebné logy zachytávajúce:

- TCP aktívne spojenia pomocou `connect()`
- otvorené súbory pomocou `open()`
- nové procesy pomocou `exec()`

Pomocou týchto logov sme porovnali oficiálnu signal-desktop aplikáciu s neoficiálnou signal-cli a zistili sme, že sa jedná o legitímnu aplikáciu poskytujúcu alternatívnu možnosť interakcie so Signalom.

Vyjadrenie k otázke oponenta

Aká bola vaša motivácia písať prácu v angličtine?

- nedostatok slovenskej terminológie v oblasti
- práca v tom istom jazyku ako zdroje informácií zamedzuje skresľovaniu významov pri preklade
- dve záverečné práce som písal v angličtine, nemal som na to negatívne ohlasy

Ďakujem za pozornosť.

Zdroje a literatúra

Gibler, Clint, Ryan Stevens, Jonathan Crussell, Hao Chen, Hui Zang, and Heesook Choi. 2013. “AdRob: Examining the Landscape and Impact of Android Application Plagiarism.” In *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services*, 431–44. MobiSys ’13. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2462456.2464461.

Gregg, Brendan. 2017. “ B Sides S F 2017: Security Monitoring with e B P F.” https://www.brendangregg.com/Slides/BSidesSF2017_BPF_security_monitoring.

Štefanko, Lukáš. 2023. “ Bad Bazaar Espionage Tool Targets Android Users via Trojanized Signal and Telegram Apps.” https://www.welivesecurity.com/en/eset-research/badbazaar-espionage-tool-targets-android-users-trojanized-signal-telegram-apps/.

Zhou, Yajin, and Xuxian Jiang. 2012. “Dissecting Android Malware: Characterization and Evolution.” In *2012 IEEE Symposium on Security and Privacy*, 95–109. https://doi.org/10.1109/SP.2012.16.