HACK IN BO®
Winter 2018 Edition

SMARTPHONE USATI: SCATOLE NERE DELLE NOSTRE VITE

Matteo Redaelli

Bologna, 27 Ottobre 2018

AGENDA

HACK IN BO® Winter 2018 Edition

- INTRODUZIONE
- SCENARIO DI RIFERIMENTO
- STATO DELL'ARTE DELLA SECURITY DEI DEVICE MOBILI
- ESEMPI REALI
- CONCLUSIONI
- Q&A

HACK IN BO®
Winter 2018 Edition

INTRODUZIONE

WHO AM I?

HACK IN BO Winter 2018 Edition

MATTEO REDAELLI

@solventred

https://www.forensics-matters.com new

Formazione:
Laurea Magistrale in Informatica presso Università degli Studi di Milano - Bicocca

Lavoro:
Blue Team Security Consultant per **Accenture** Security

Passions:
Appassionato di Digital Forensics, Incident Response e Malware Analysis

Skills:
Developer Ruby e Python

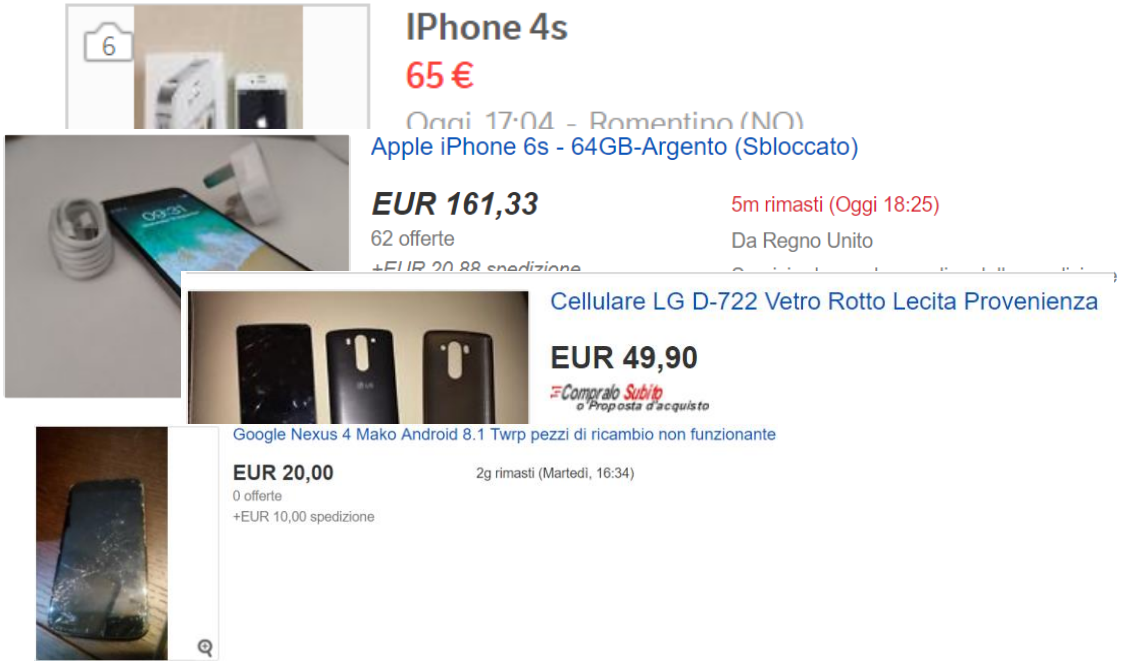
GIAC CERTIFIED FORENSIC ANALYST GCFA

GIAC CERTIFIED INCIDENT HANDLER GCIH

INTRODUZIONE

DI COSA PARLEREMO?

- Chi può essere interessato a recuperare i dati dal nostro telefono?
- A che rischi andiamo in contro?
- Qual è lo stato dell'arte della sicurezza dei dispositivi mobili?
- Come si possono recuperare i dati da un dispositivo mobile?

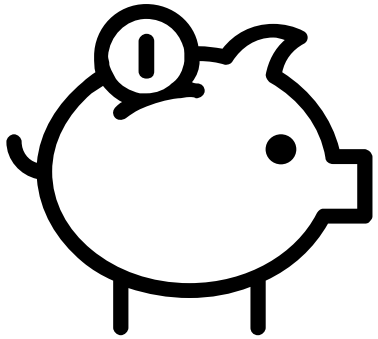


HACK IN BO®
Winter 2018 Edition

SCENARIO DI RIFERIMENTO

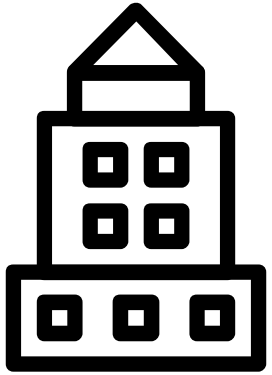
PRINCIPALI SCENARI

CHI POTREBBE ESSERE INTERESSATO AL NOSTRO CELLULARE USATO?



SEMPLICE UTENTE

Finalità: Risparmio
Probabilità di Acquisto: Alta
Rischio: **Basso**



AZIENDA DEL SETTORE

Finalità: n/a
Probabilità di Acquisto: n/a
Rischio: **Basso**

UTENTE CON FINALITÁ MALEVOLE

Finalità: Recupero Dati
Probabilità di Acquisto: Alta
Rischio: **Alto**

PRINCIPALI TIPOLOGIE DI ACQUISIZIONE DEI DATI

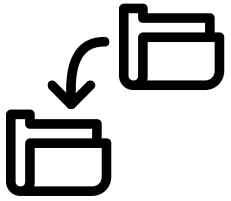
COME SI POSSONO RECUPERARE I DATI?

HACK IN BO® Winter 2018 Edition

ACQUISIZIONE MANUALE

Visualizzazione dati direttamente sul dispositivo

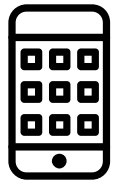
PRO: veloce, economica, non richiede connessione
CONTRO: necessita di un dispositivo totalmente integro e non lockato, tempo di acquisizione proporzionale alla mole di dati memorizzati, rischio di cancellazione accidentale dei dati, recupero dati parziale



ACQUISIZIONE LOGICA

Estrazione della struttura logica del filesystem (file, directory)

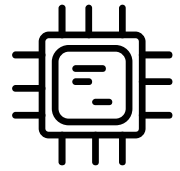
PRO: può essere eseguita tramite software di sincronizzazione e backup
CONTRO: necessita di diverse precondizioni per essere eseguita, non permette di recuperare tutti i file presenti e tutte le zone del filesystem



ACQUISIZIONE FISICA

Copia bit-a-bit della memoria fisica del dispositivo

PRO: permette di estrarre tutti i dati e anche lo spazio non allocato
CONTRO: necessita di diverse precondizioni per essere eseguita, costosa, l'estrazione necessita di essere interpretata



CHIP OFF E MICRO READ, JTAG

Estrazione dei dati direttamente dal chip di memoria

PRO: permette l'acquisizione di device che non sono più utilizzabili
CONTRO: Molto complesso da portare a termine, richiede conoscenze a livello hardware, strumentazione corretta e manualità.

DIFFICOLTÀ

ALCUNE SFIDE DELLA MOBILE FORENSICS

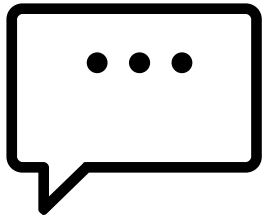
HACK IN BO Winter 2018 Edition

SISTEMI OPERATIVI DIFFERENTI (IOS, ANDROID E VERSIONI…)	NECESSITÀ DI MANTENERE INALTERATO IL DISPOSITIVO A LIVELLO HARDWARE E A LIVELLO DI DATI	SECURITY FEATURES E TECNICHE DI ANTI FORENSICS (DATA WIPING, DATA OBFUSCATION…)
• L'attaccante può scegliere i dispositivi per i quali è confidente di poter **recuperare i dati presenti**. • Sistemi operativi non aggiornati possono avere diverse **vulnerabilità documentate e facilmente sfruttabili**.	• L'attaccante può permettersi di **manomettere il dispositivo** per raggiungere il suo scopo. • L'attaccante può compromettere irrimediabilmente il dispositivo senza alcun problema. • L'attaccante non deve rispettare nessuna **chain of custody** né deve produrre evidenze riproducibili.	• L'attaccante può scegliere ad esempio dispositivi con touch rotto per abbassare «il rischio» di incorrere in questo tipo di problemi. • L'attaccante può fare uso di strumenti che permettono di **evadere le misure di protezione** documentate e facilmente riproducibili

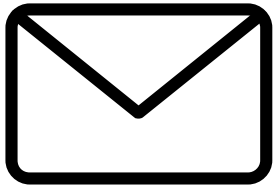
CHE DATI SI POSSONO RECUPERARE DA UN CELLULARE?

HACK IN BO Winter 2018 Edition

RUBRICA



SMS

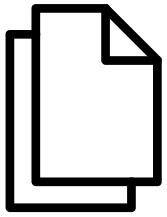


E-MAIL

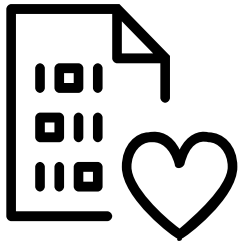
GALLERIA

MAPPE

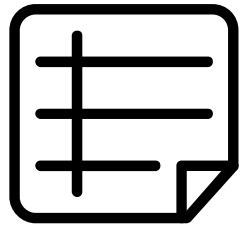
WEB BROWSER HISTORY



DOCUMENTI



DATI DEI SOCIAL NETWORK



NOTE

DATI ELIMINATI

QUANTO VALGONO EFFETTIVAMENTE I DATI RECUPERATI?

DATI BANCARI E FINANZIARI

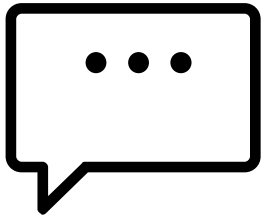
Paypal Login: 247 $
Account Bancario online: 160.15$
Dettagli Debit Card: 67.50$
Dettagli Carta di credito: 50$
(*solo vendita, in più c'è il danno da utilizzo*)

FOTO ID & PASSAPORTO

Foto Passaporto: 62.61$
ID: 29.59$
(*solo vendita, in più c'è il danno da utilizzo*)

FOTO PRIVATE

Ricatti ed estorsioni
Valore: $$$



SMS, CONTATTI, CHAT…

Estorsioni e ricatti, attacchi di phishing, contraffazioni…

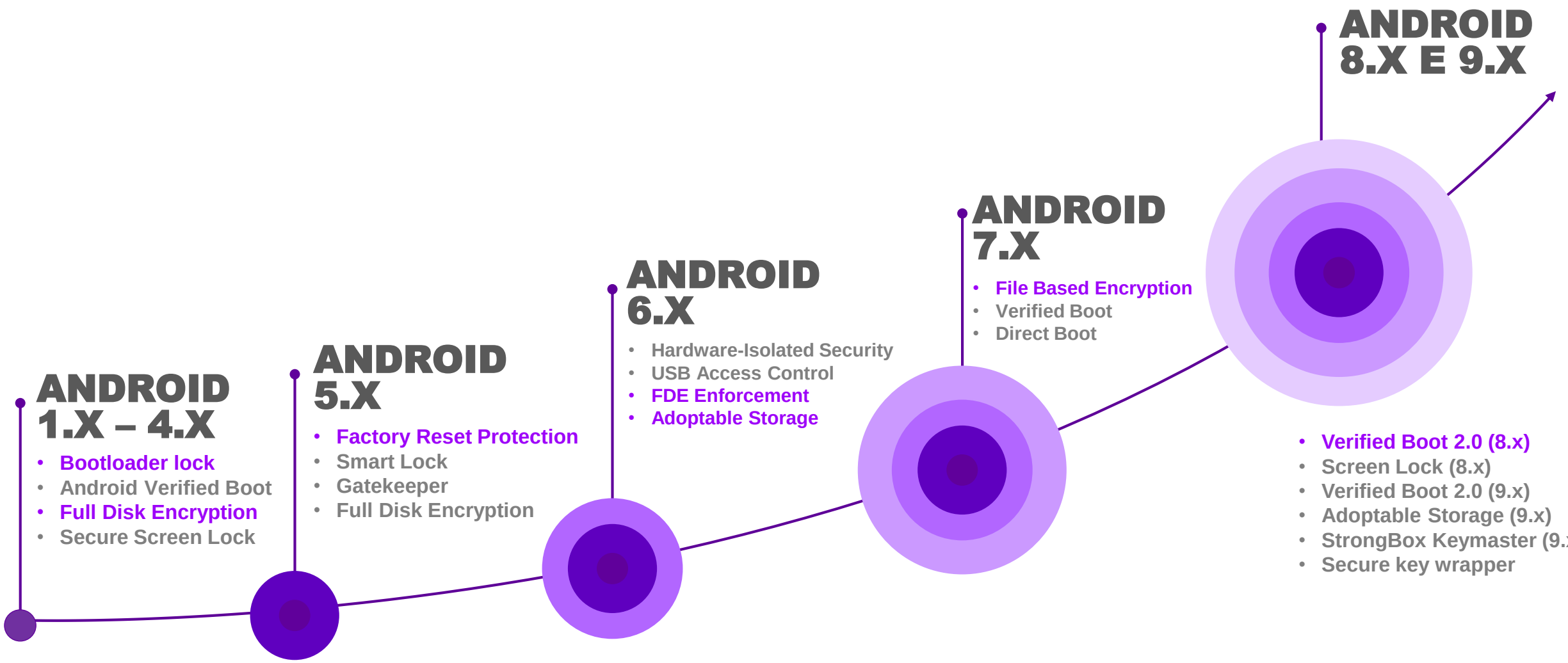
Valore:$$$

Ref: https://www.top10vpn.com/privacy-central/privacy/dark-web-market-price-index-feb-2018-us/

STATO DELL'ARTE DELLA SECURITY DEVICE MOBILI

HackInBo® Winter 2018 Edition

PRINCIPALI MISURE DI SICUREZZA ANDROID



ACQUISIZIONE DISPOSITIVO ANDROID: SFIDE

L'ETEROGENEITÀ DELL'ECOSISTEMA ANDROID RENDE IL PROCESSO DELL'ACQUISIZIONE **VENDOR-DEPENDENT.**

COME EFFETTUARE UN'ACQUISIZIONE FINO ALLA VERSIONE ANDROID 6.0 CON DISPOSITIVO BLOCCATO E FDE NON ATTIVA

Per ognuna di queste tecniche ci possono essere **delle pre-condizioni** quali:

- Conoscenza del Passcode/Pin/Pattern
- Attivazione della Modalità USB Debugging Attivo

Per versioni superiori alcune volte possibile sfruttare delle vulnerabilità documentate per effettuare l'acquisizione. A partire dalla versione 6 di **Android l'intero filesystem è cifrato di default**.

PRINCIPALI MISURE DI SICUREZZA IOS

HACK IN BO Winter 2018 Edition

IOS 1.X - 3.X

- Protezione dispositivo con PIN 4 digit

IOS 4.X – 7.X

- **Cifratura dello spazio utente (iOS 4)**
- Password policy migliorata
- Data Protection
- Keychain Migliorato
- **Autorizzazione dispositivo (iOS 7.0)**

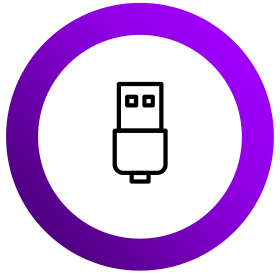
IOS 7.X E OLTRE

- **Secure Enclave (iOS 8)**
- Throttling delle password
- **Pin di default 6 Digit(iOS 9)**
- Generazione chiavi crittografiche
- **USB restricted Mode (iOS 11.4.1)**

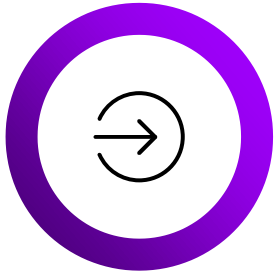
ACQUISIZIONE DISPOSITIVO IOS: SFIDE

HACK IN BO Winter 2018 Edition

L'ACQUISIZIONE FINO ALLA VERSIONE 3.X È POSSIBILE DATO CHE:



Si può **collegare il dispositivo via USB** a qualsiasi PC untrusted senza autorizzazione (autorizzazione introdotta con la versione 7.x)



Si può **installare jailbreak** che permettono di accedere come root al dispositivo bypassando anche eventualmente il PIN

I **dati non** sono **cifrati** di default

È fattibile il **cracking offline del PIN** (lunghezza minima di default 4 caratteri)

A PARTIRE DA IOS 4 L'INTERO FILESYSTEM È CIFRATO.

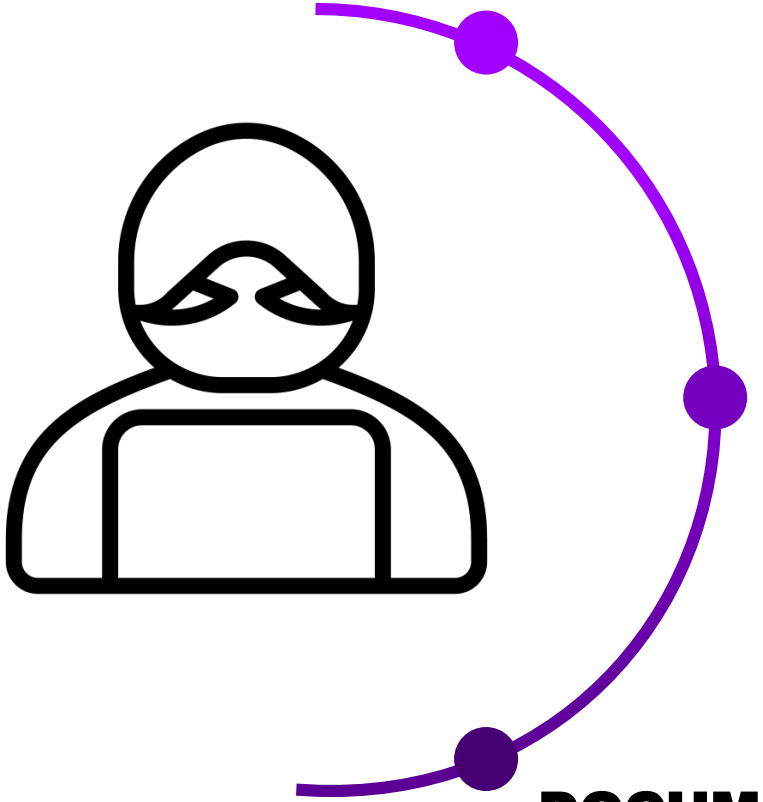
A PARTIRE DA IOS 11.4 VIENE INTRODOTTA LA MODALITÀ USB RESTRICTED MODE.

ESEMPI REALI

ACQUISTO DISPOSITIVO USATO

COSA PUÒ FARE UN ATTACCANTE? PRIMA DELL'ACQUISTO

HACK IN BO Winter 2018 Edition



SCEGLIERE LA **VERSIONE** DEL DISPOSITIVO

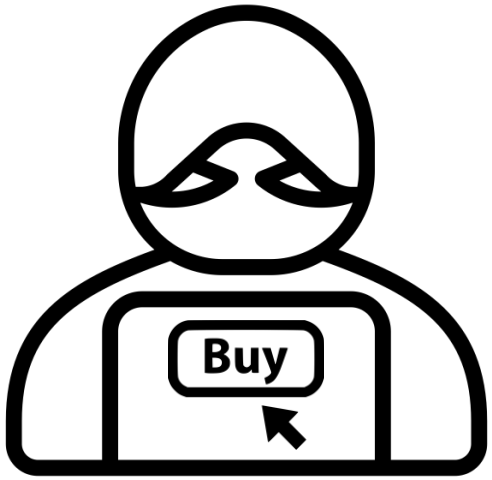
DOCUMENTARSI SU **MISURE DI SICUREZZA** PRESENTI NEL DISPOSITIVO E NELLA VERSIONE DEL SOFTWARE

DOCUMENTARSI SU **VULNERABILITÀ** DEL DISPOSITIVO

ACQUISTO DISPOSITIVO USATO

COSA PUÒ FARE UN ATTACCANTE? DOPO L'ACQUISTO

HACK IN BO Winter 2018 Edition



- VERIFICA **MECCANISMI DI LOCK**
- VERIFICA PRESENZA **FDE**
- CONTROLLO DELLA PRESENZA DI **RECOVERY MODE** MODIFICATE
- **ROOT** DEL DISPOSITIVO
- **ACQUISIZIONE** DEL DISPOSITIVO
- ANALISI DEI **DATI** ESTRATTI

ANDROID
ESEMPIO CONCRETO DI INSERZIONE TROVATA

Sistema operativo:

- Ultima versione: Android 5.1.1 (Lollipop) ← **Versione del dispositivo utilizzata per il test**
- Prima versione: 4.2.2 (Jelly Bean)

Con schermo rotto risulta difficile utilizzare il touch poiché **digitizer incollato** sul vetro, e quindi anche l'inizializzazione.

La Team Win Recovery Project (TWRP) *è una recovery modificata open-source per dispositivi Android. È dotata di interfaccia touchscreen che consente di installare firmware modificati di terze parti, ritornare al sistema operativo originale, formattare la memoria interna, modificare e cancellare file ecc. Necessita di root. Ref. Wiki*

ANDROID

ESEMPIO COSA PUÒ FARE UN ATTACCANTE
BYPASS BRUTEFORCING

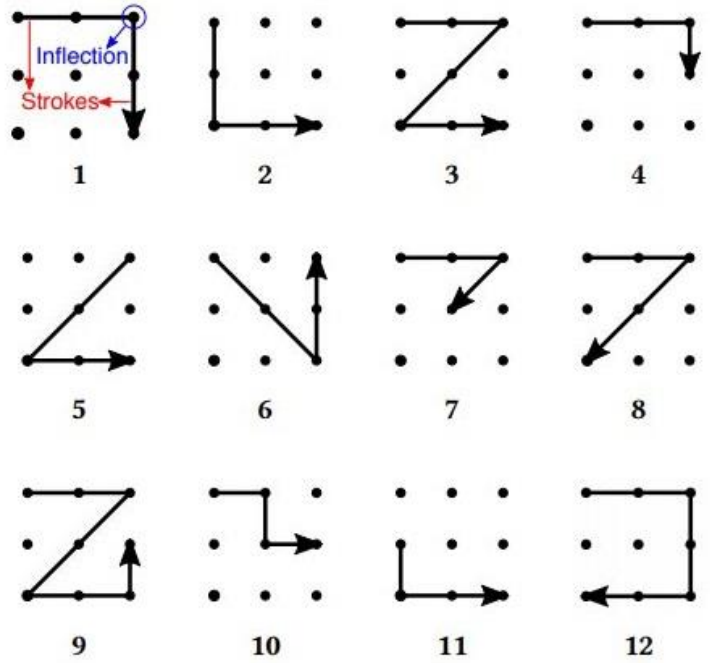
Smudge Attack

Smudge Attack

Identificare la sequenza per lo sblocco sul vetro, ad esempio tramite Vapore

Bruteforce

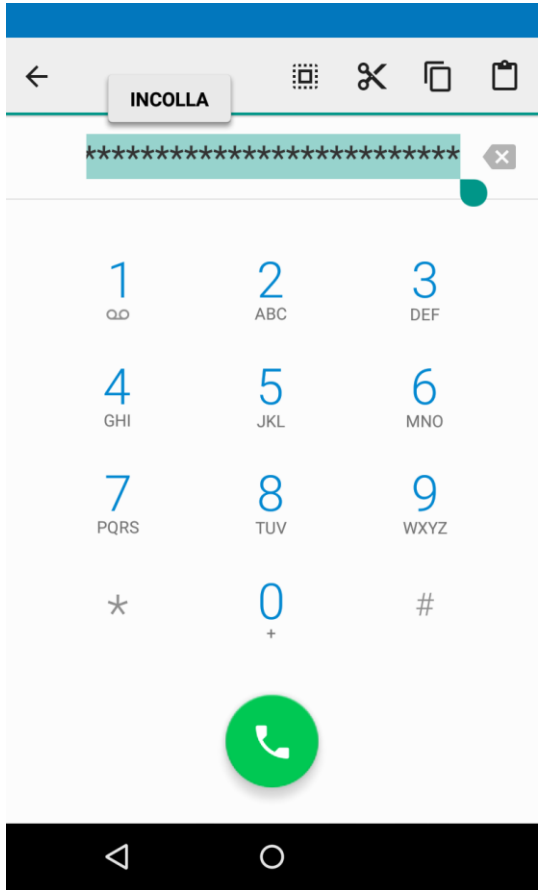
Provare una delle sequenze più frequenti di sblocco.
Reference: Marta Loge



12 sequenze di blocco più frequenti

ANDROID

ESEMPIO COSA PUÒ FARE UN ATTACCANTE CRASHING UI



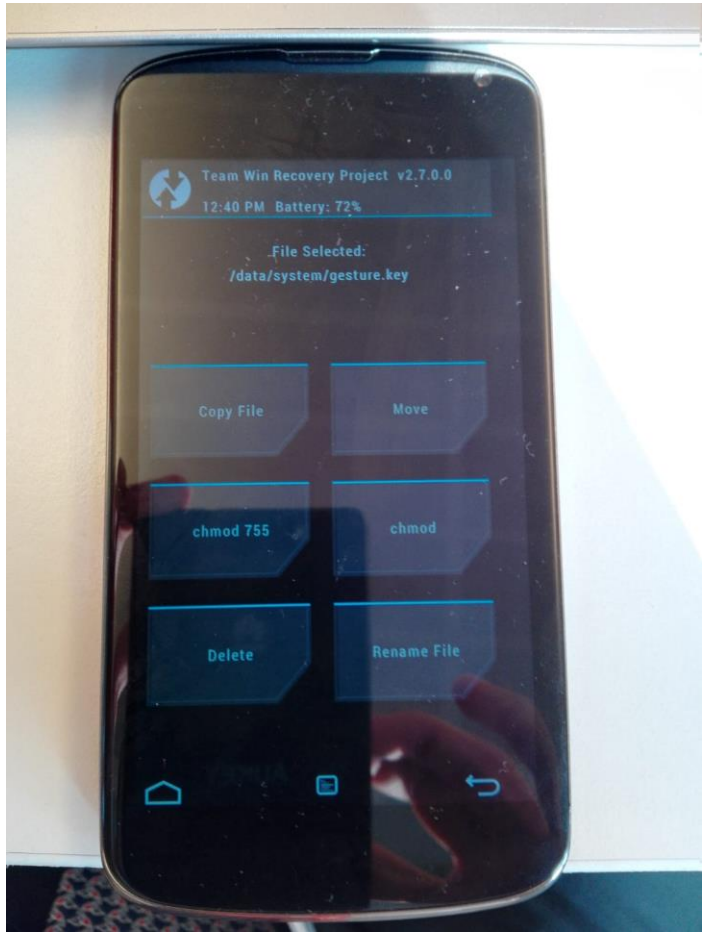
Crashing UI Lock Passaggi

1. Vai in modalità Chiamata Emergenza
2. Inserisci una stringa di caratteri molto lunga.
3. Copia questa stringa ed incollala per renderela ancora più lunga
4. Ripeti il punto 3 fino a quanto non sarà più possibile selezionare il testo per copiarlo
5. Apri l'applicazione Fotocamera (non serve sbloccare il telefono).
6. Trascina la schermata delle notifiche e clicca il tasto impostazioni.
7. Incolla più volte la stringa copiata in precedenza
8. Dopo averlo incollato più volte, il lock screen andrà in crash e potrete accedere.

Compatibilità Android 5.0 – 5.1.1 fino a build LMY48M

ANDROID

ESEMPIO COSA PUÒ FARE UN ATTACCANTE
BYPASS LOCK SCREEN



Delete file da TWRP

1. Avvio del cellulare in modalità di recovery
2. Andare in Advanced > File manager
3. Muoversi in data/system
4. Cancellare i file
   a) /data/system/locksettings.db*
   b) /data/system/gesture.key , /data/system/password.key
5. Riavviare il cellulare senza più blocco

ANDROID

ESEMPIO REALE COSA PUÒ FARE UN ATTACCANTE
ACQUISIZIONE IMMAGINE DD

```
root@mako:/ # ls -al /dev/block/platform/msm_sdcc.1/by-name/
lrwxrwxrwx root     root              2018-07-08 14:26 DDR -> /dev/block/mmcblk0p24
lrwxrwxrwx root     root              2018-07-08 14:26 aboot -> /dev/block/mmcblk0p12
lrwxrwxrwx root     root              2018-07-08 14:26 abootb -> /dev/block/mmcblk0p15
lrwxrwxrwx root     root              2018-07-08 14:26 boot -> /dev/block/mmcblk0p6
lrwxrwxrwx root     root              2018-07-08 14:26 cache -> /dev/block/mmcblk0p22
lrwxrwxrwx root     root              2018-07-08 14:26 grow -> /dev/block/mmcblk0p25
lrwxrwxrwx root     root              2018-07-08 14:26 m9kefs1 -> /dev/block/mmcblk0p8
lrwxrwxrwx root     root              2018-07-08 14:26 m9kefs2 -> /dev/block/mmcblk0p9
lrwxrwxrwx root     root              2018-07-08 14:26 m9kefs3 -> /dev/block/mmcblk0p10
lrwxrwxrwx root     root              2018-07-08 14:26 metadata -> /dev/block/mmcblk0p18
lrwxrwxrwx root     root              2018-07-08 14:26 misc -> /dev/block/mmcblk0p19
lrwxrwxrwx root     root              2018-07-08 14:26 modem -> /dev/block/mmcblk0p1
lrwxrwxrwx root     root              2018-07-08 14:26 persist -> /dev/block/mmcblk0p20
lrwxrwxrwx root     root              2018-07-08 14:26 recovery -> /dev/block/mmcblk0p7
lrwxrwxrwx root     root              2018-07-08 14:26 rpm -> /dev/block/mmcblk0p11
lrwxrwxrwx root     root              2018-07-08 14:26 rpmb -> /dev/block/mmcblk0p16
lrwxrwxrwx root     root              2018-07-08 14:26 sbl1 -> /dev/block/mmcblk0p2
lrwxrwxrwx root     root              2018-07-08 14:26 sbl2 -> /dev/block/mmcblk0p3
lrwxrwxrwx root     root              2018-07-08 14:26 sbl2b -> /dev/block/mmcblk0p13
lrwxrwxrwx root     root              2018-07-08 14:26 sbl3 -> /dev/block/mmcblk0p4
lrwxrwxrwx root     root              2018-07-08 14:26 sbl3b -> /dev/block/mmcblk0p14
lrwxrwxrwx root     root              2018-07-08 14:26 system -> /dev/block/mmcblk0p21
lrwxrwxrwx root     root              2018-07-08 14:26 tz -> /dev/block/mmcblk0p5
lrwxrwxrwx root     root              2018-07-08 14:26 tzb -> /dev/block/mmcblk0p17
lrwxrwxrwx root     root              2018-07-08 14:26 userdata -> /dev/block/mmcblk0p23
```

Prerequisiti:

- Root dispositivo
- ADB installato e autorizzato su pc per l'acquisizione
- Busybox installto sul device

1. Redirezione delle richieste

```
$ adb forward tcp:8888 tcp:8888
```

2. Apertura della shell adb:

```
$ adb shell
```

3. Acquisizione Privelegi di root:

```
$ su –
```

4. Creazione immagine dd e redirezione dell'output su porta 8888 tramite busybox:

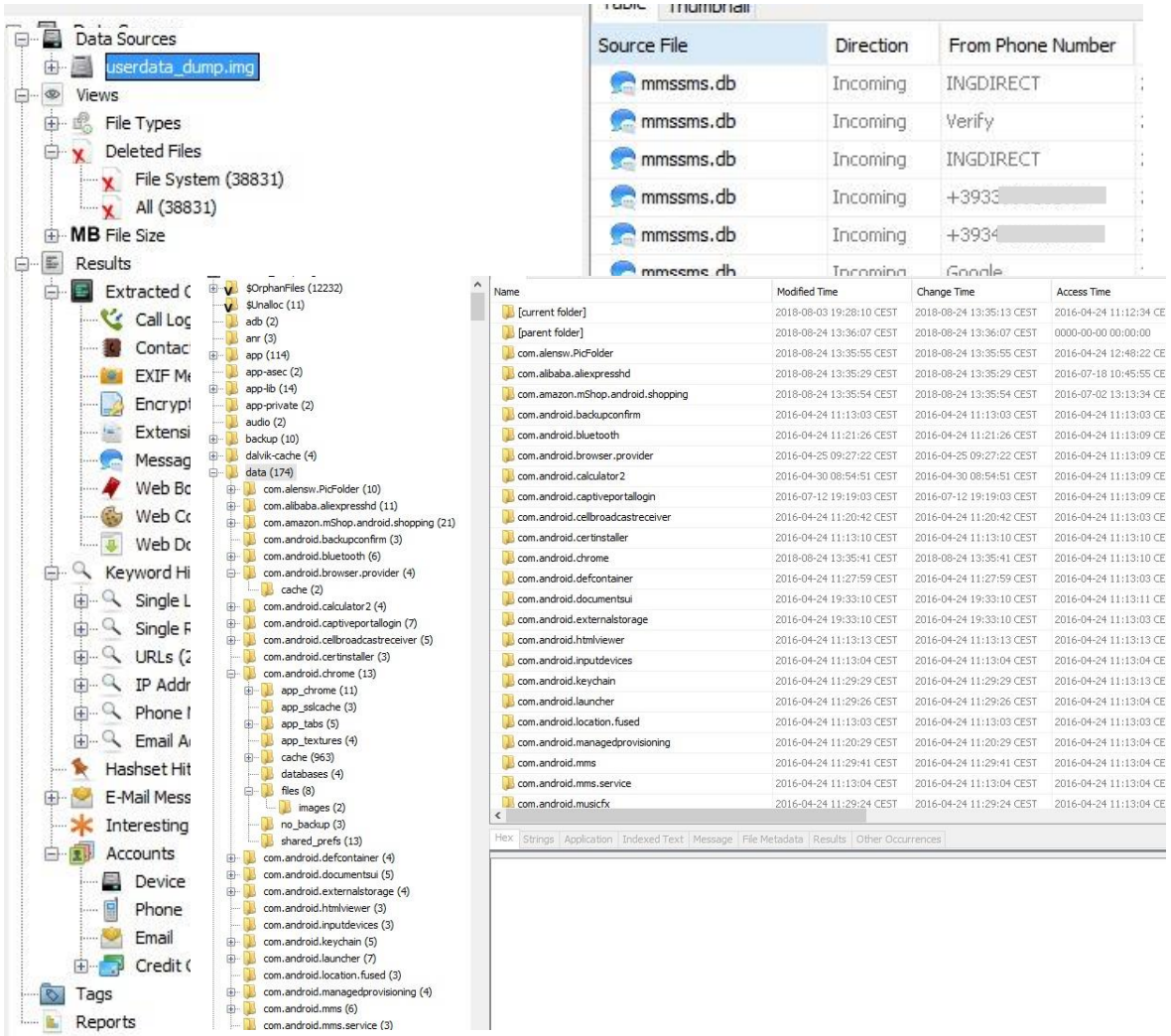
```
# dd if=/dev/block/mmcblk0p23 | busybox nc -l -p
8888
```

4. Apertura netcat su macchina host per ricezione flusso immagine dd denominata userdata_dump.img:

```
$ nc 127.0.0.1 8888 > userdata_dump.img
```

ANDROID

ESEMPIO REALE COSA PUÒ FARE UN ATTACCANTE
ANALISI DEI DATI



Apertura immagine DD appena creata con Autopsy, con possibilità di recuperare:

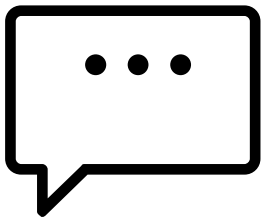
a) File cancellati
b) Alberatura completa filesystem
c) Immagini e video
d) SMS
e) Stringhe che rispettano delle keyword/pattern (Luhn valid)
f) Chiamate effettuate
g) Account presenti sul cellulare
h) Metadati EXIF (ad esempio coordinate gps)
i) Rubrica
j) Informazioni browser
k) Email scambiate
l) ….

ANDROID

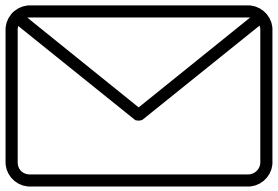
ESEMPIO REALE COSA PUÒ FARE UN ATTACCANTE RESOCONTO DATI RECUPERATI (SENZA CARVING) DA NEXUS 4 DI TEST

HACK IN BO Winter 2018 Edition

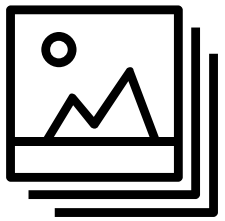
456
Contatti



189
SMS



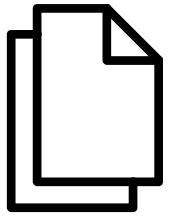
528
E-MAIL



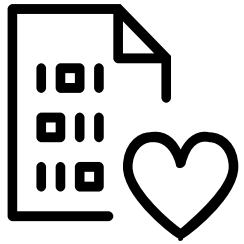
216 Immagini
13 Video
GALLERIA

Exif metadata
MAPPE

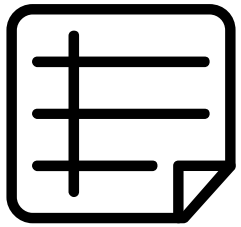
15 Bookmarks
2203 Web Cookies
1 Web Download
WEB BROWSER HISTORY



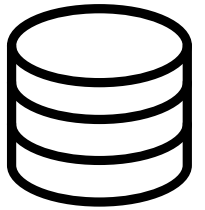
78 PDF
DOCUMENTI



DB Whatsapp
DATI DEI SOCIAL NETWORK



N/A
NOTE



38831 File
DATI ELIMINATI

ANDROID

CASO NEXUS 4 CON FACTORY RESET, GAME OVER?

```
112   * FACTORY RESET
113   * 1. user selects "factory reset"
114   * 2. main system writes "--wipe_data" to /cache/recovery/command
115   * 3. main system reboots into recovery
116   * 4. get_args() writes BCB with "boot-recovery" and "--wipe_data"
117   *    -- after this, rebooting will restart the erase --
118   * 5. erase_volume() reformats /data
119   * 6. erase_volume() reformats /cache
120   * 7. finish_recovery() erases BCB
121   *    -- after this, rebooting will restart the main system --
122   * 8. main() calls reboot() to boot main system
123   *
```

Commento che illustra la procedura di factory reset nel codice di Android 5.1.1 versione del device di test.

Ref: https://android.googlesource.com/platform/bootable/recovery/+/android-5.1.1_r2

ANDROID

RECUPERARE DATI DA DEVICE CON FACTORY RESET
DATA CARVING

STEP 1: Root del dispositivo, installazione busybox e acquisizione dell'immagine dd di userdata tramite adb.

```
MacBook-Pro-di-matteo:Desktop matteo$ foremost -i userdata_dump_wipe.img -o recover/ -t pdf,jpg,png,htm,mpeg,avi,doc,wav
Processing: userdata_dump_wipe.img
|**************************************************|
```

STEP 2: Data carving con foremost, per estrarre pdf,jpg,png,htm,mpeg,avi,doc,wav

$ foremost -i userdata_dump_wipe.img -o recover/ -t pdf,jpg,png,htm,mpeg,avi,doc,wav

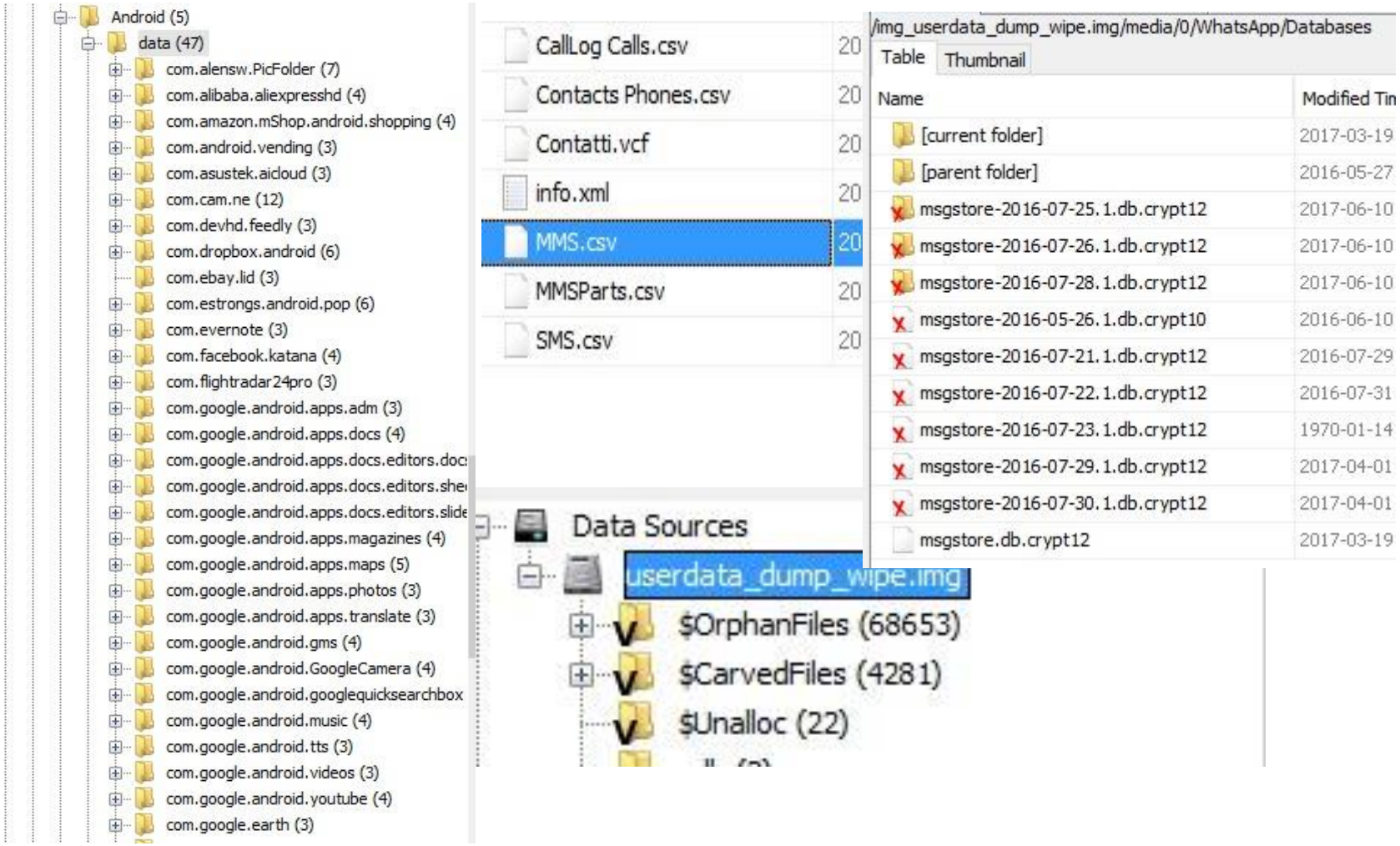
```
19711 FILES EXTRACTED

pdf:= 13
jpg:= 5824
png:= 13069
htm:= 763
rif:= 42
-----------------------------------------------------------------
```

ANDROID

RECUPERARE DATI DA DEVICE WIPED
DATA CARVING

STEP 3: Autopsy Android Analyzer e PhotoRec

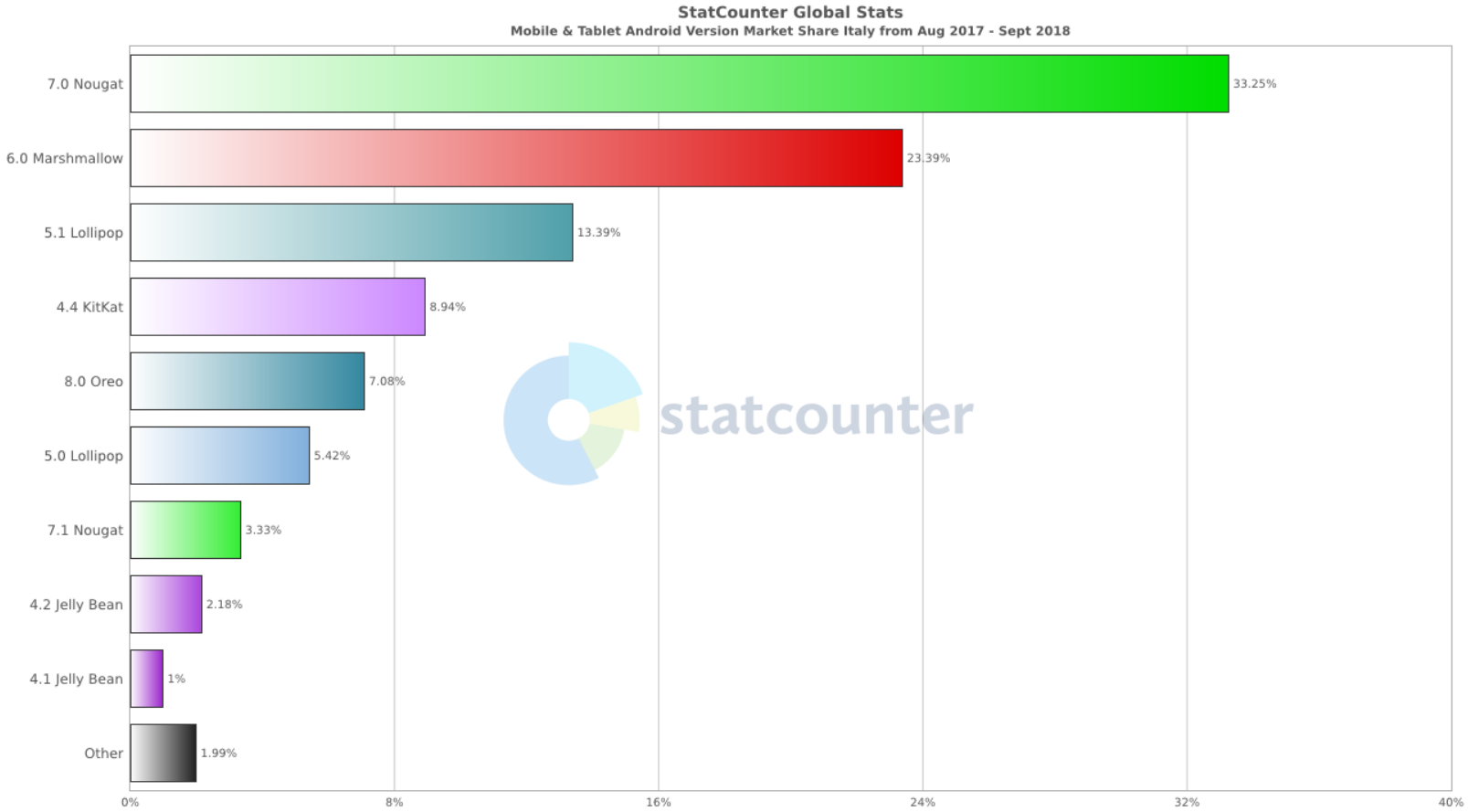


Cosa abbiamo recuperato:

- Alberatura completa filesystem
- Database
- File di backup
- Immagini, video
- Ricerche basate su pattern (e.g Luhn valid strings)
- ….

DIFFUSIONE DISPOSITIVI ANDROID

INTERVALLO TEMPORALE AGOSTO 2017 – SETTEMBRE 2018

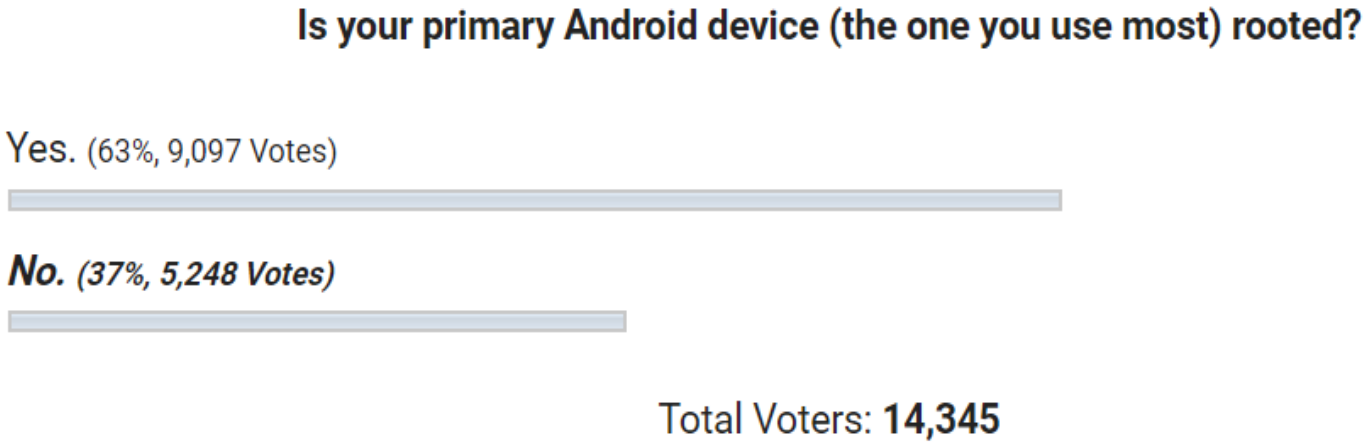


Ref: statcounter.com

- Il 31,5% dei dispositivi potenzialmente ha i dati **non cifrati di default** e quindi le operazioni di recovery potrebbero essere semplici come documentato.
- Quasi il 6% dei dispositivi potrebbe risentire del bug relativo al crash della UI della password, effettuato durante i test.

DISPOSITIVI ANDROID ROOTED

INTERVALLO TEMPORALE NOVEMBRE 2014 – ORA



Ref: https://www.androidpolice.com/2014/11/23/weekend-poll-is-your-primary-android-device-rooted-2/

IOS

ESEMPIO COSA PUÒ FARE UN ATTACCANTE

Apple Iphone 5 Schermo e touch non funzionante

EUR 11,96

6o rimaste

ebay

- **Possibilità di recupero:**
  - **Vetro e touch rotto aumenta le possibilità che utente non abbia eseguito wipe.**
  - **Possibilità di autorizzare un dispositivo (i.e. pc)**
    - **Non siano presente pin**

IOS

ESEMPIO COSA PUÒ FARE UN ATTACCANTE
CREAZIONE IMMAGINE LOGICA DEL DEVICE IOS

libimobiledevice.

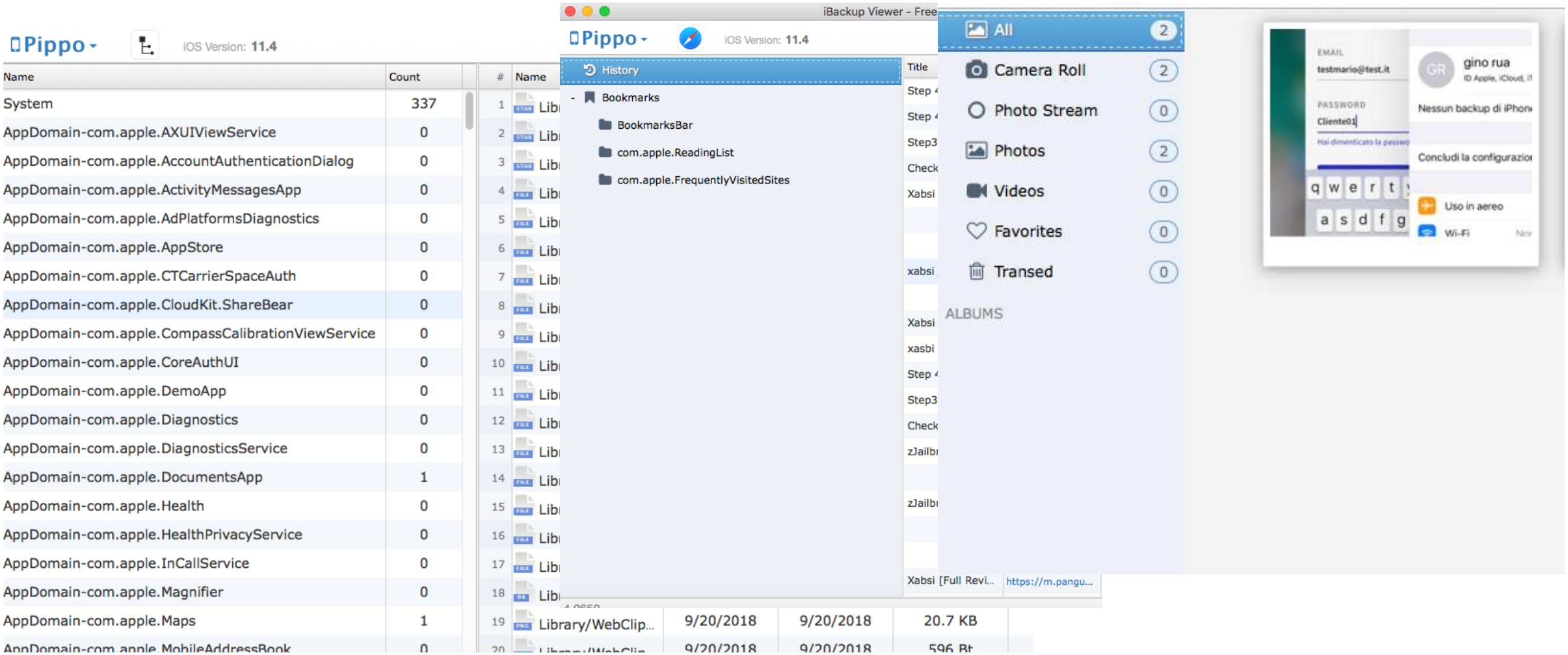
Creazione del backup con libmobidevice

$ idevicebackup2 backup –full /User/matteo/Desktop/backup_iphone_5

Una volta creato il backup è possibile navigarlo tramite software come backup explorer, iexplorer…

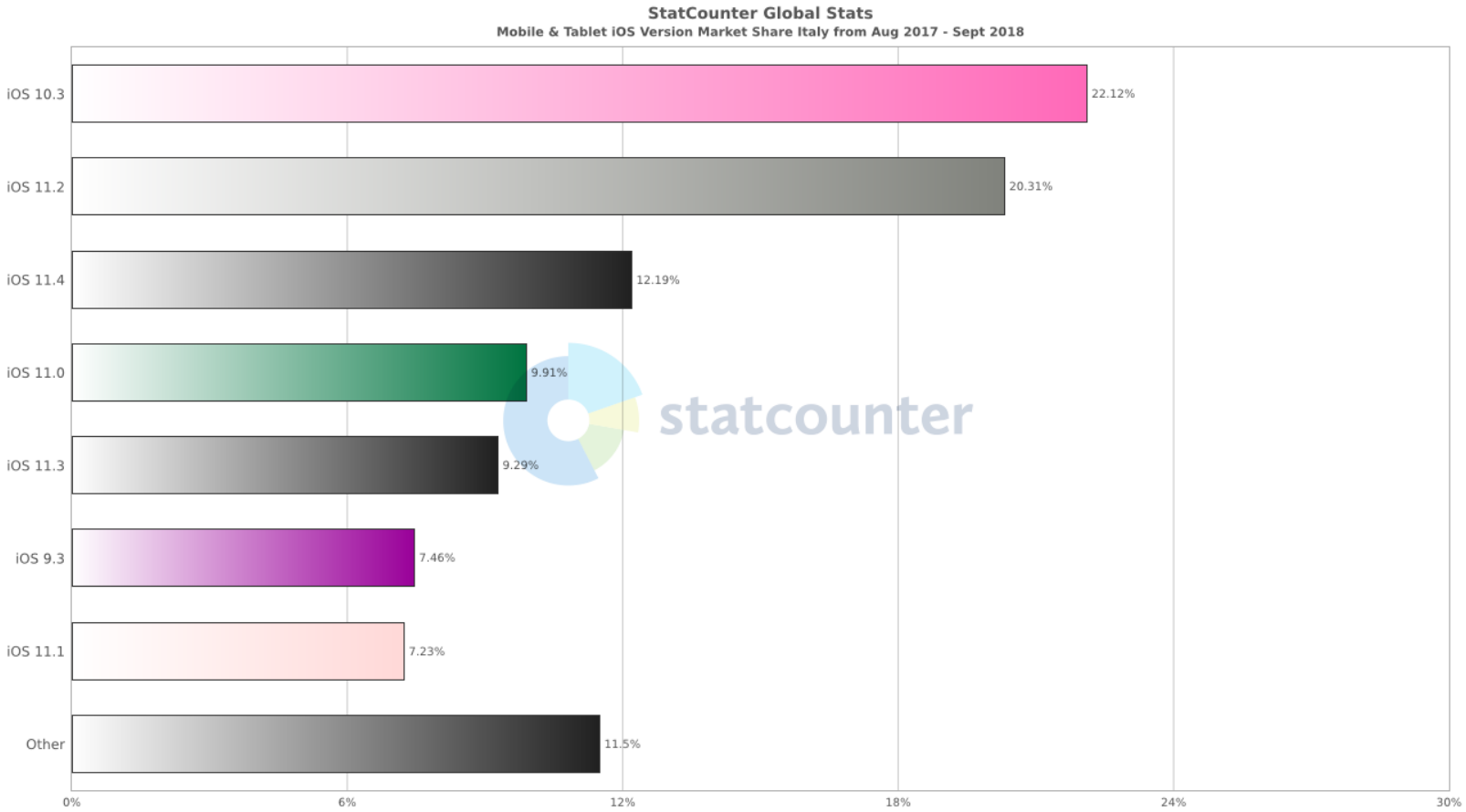
IOS

ESEMPIO COSA PUÒ FARE UN ATTACCANTE
ANALISI DEI DATI



DIFFUSIONE DISPOSITIVI IOS

INTERVALLO TEMPORALE AGOSTO 2017 – SETTEMBRE 2018



Più del 30% dei dispositivi ha una versione di iOS che permetterebbere lo sblocco della sequenza tramite tool commerciali/aziende specializzate (ad esempio Cellbrite, Grayshift)

Ref: statcounter.com

CONCLUSIONI

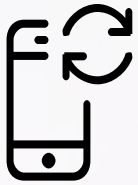
SO WHAT?

HACK IN BO® Winter 2018 Edition

01

Assicurarsi che tuo dispositivo abbia attiva la full disk encryption

02



Prima di vendere il dispositivo, effettuare la cifratura dei dati e poi il wipe

03

Evitare di vendere dispositivi di cui non si è in grado di accertarsi l'avvenuta cancellazione sicura dei dati.

04

Documentarsi su tecniche che rendono possibile il recupero dei dati sul modello del proprio dispositivo

Q&A

HackInBo® Winter 2018 Edition

HACK IN BO®
Winter 2018 Edition

THANK YOU!

MATTEO REDAELLI

m.redaelli@accenture.com

@solventred

ANNEX

TEST EFFETTUATI
CONTESTO DELLA RICERCA

HACK IN BO Winter 2018 Edition

Produttore	Modello	Sistema Operativo	Note
Sony	Xperia T3 LT30p	Android KitKat 4.4.4	Rooted
Samsung	Galaxy A5 2015 SM-A500F	Android Marshmallow 6.1	Samsung Knox 2.6
Samsung	Galaxy A5 2017 SM-A520F	Android Oreo 8.0	
LG	Nexus 4 Mako	Android Lollipop 5.1.1	Rooted, TWRP
Apple	Iphone 5s	11.4	
Apple	Iphone 5	10.3.3	Jailbreak Untethered
Apple	Iphone 6	12	Locked Device

	LOCKED_OFFLINE_SECURE_LOCKSCREEN_DELETION
	Verificare nelle condizioni iniziali specificate di seguito se è possibile cancellare i file /data/system/password.key o gesture.key, disabilitando così il lockscreen.
	SonyXperia T3
ioni Iniziali li	• Sul dispositivo è configurato il lockscreen con PIN di 6 caratteri (123456) e blocco automatico dopo 5 sec (default). • USB Debugging attivo • Autorizzazione per peering con PC fornita
d/Jailbroken	SI
ità di ione	1. Collegare dispositivo al pc via USB 2. Avviare sul pc adb a. adb kill-server b. adb start-server 3. Verificare connessione con il dispositivo a. adb devices 4. adb shell 5. su 6. rm /data/system/*.key
Risultato Atteso	Cancellazione file password.key e gesture.key
Risultato	Superato