



SMARTPHONE USATI: SCATOLE NERE DELLE NOSTRE VITE

Matteo Redaelli

Bologna, 27 Ottobre 2018

INTRODUZIONE

WHO AM I?



MATTEO REDAEELLI

 @solventred

 <https://www.forensics-matters.com> 



Formazione:

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



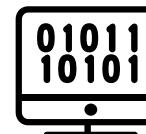
Lavoro:

Blue Team Security Consultant per **Accenture** Security



Passions:

Appassionato di Digital Forensics, Incident Response e Malware Analysis



Skills:

Developer Ruby e Python

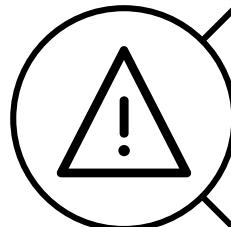


INTRODUZIONE

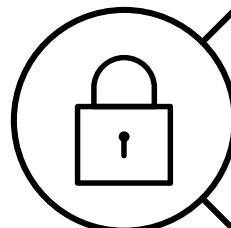
DI COSA PARLEREMO?



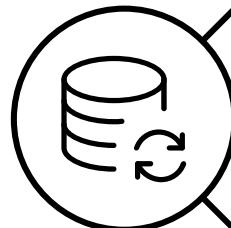
Chi può essere interessato a recuperare i dati dal nostro telefono?



A che rischi andiamo incontro?



Qual è lo stato dell'arte della sicurezza dei dispositivi mobili?



Come si possono recuperare i dati da un dispositivo mobile?

The screenshot shows a grid of three items from an online marketplace:

- iPhone 4s**
65€
Ogni 17.04 - Romentino (NO)
Apple iPhone 6s - 64GB-Arancione (Sbloccato)
- EUR 161,33**
62 offerte
+EUR 20,88 spedizione
5m rimasti (Oggi 18:25)
Da Regno Unito
- Cellulare LG D-722 Vetro Rotto Lecita Provenienza**
EUR 49,90
=Compralo Subito
o Proposta d'acquisto

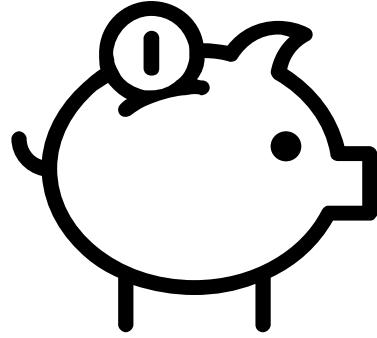
Below the second item, there is another listing:

Google Nexus 4 Mako Android 8.1 Twrp pezzi di ricambio non funzionante
EUR 20,00
0 offerte
+EUR 10,00 spedizione
2g rimasti (Martedì, 16:34)

SCENARIO DI RIFERIMENTO

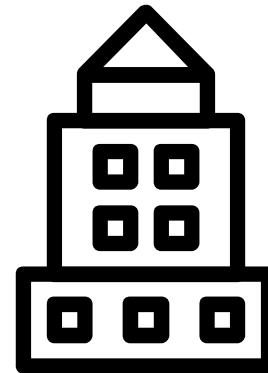
PRINCIPALI SCENARI

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 FINALITÀ MALEVOLI

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

PRINCIPALI TIPOLOGIE DI ACQUISIZIONE DEI DATI

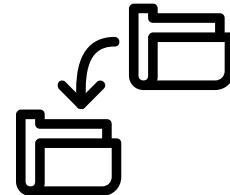
COME SI POSSONO RECUPERARE I DATI?



ACQUISIZIONE MANUALE

Visualizzazione dati direttamente sul dispositivo

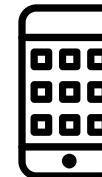
PRO: veloce, economica, non richiede connessione
CONTRO: necessita di un dispositivo totalmente integro e non lockato, tempo di acquisizione proporzionale alla mole di dati memorizzati, rischio di cancellazione accidentale dei dati, recupero dati parziale



ACQUISIZIONE LOGICA

Estrazione della struttura logica del filesystem (file, directory)

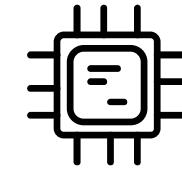
PRO: può essere eseguita tramite software di sincronizzazione e backup
CONTRO: necessita di diverse precondizioni per essere eseguita, non permette di recuperare tutti i file presenti e tutte le zone del filesystem



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

SISTEMI OPERATIVI DIFFERENTI (IOS, ANDROID E VERSIONI...)

- 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**.

NECESSITÀ DI MANTENERE INALTERATO IL DISPOSITIVO A LIVELLO HARDWARE E A LIVELLO DI DATI

- 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.

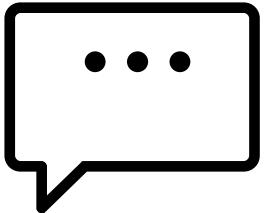
SECURITY FEATURES E TECNICHE DI ANTI FORENSICS (DATA WIPIING, DATA OBFUSCATION...)

- 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.

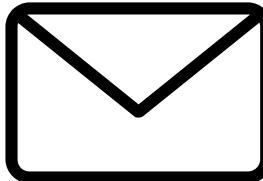
CHE DATI SI POSSONO RECUPERARE DA UN CELLULARE?



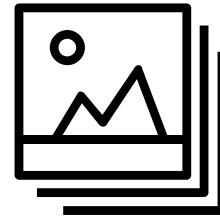
RUBRICA



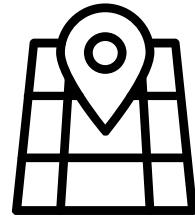
SMS



E-MAIL



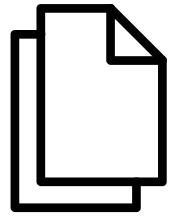
GALLERIA



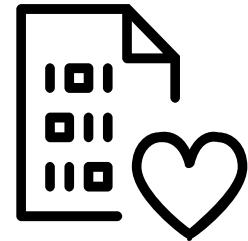
MAPPE



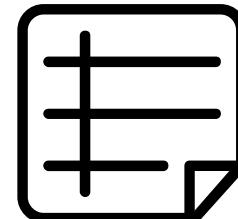
WEB BROWSER HISTORY



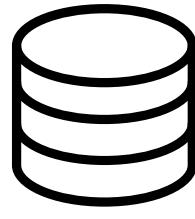
DOCUMENTI



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)

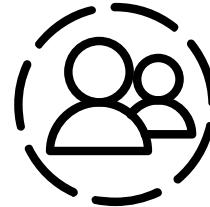


FOTO ID & PASSAPORTO

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

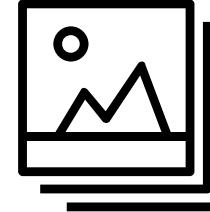
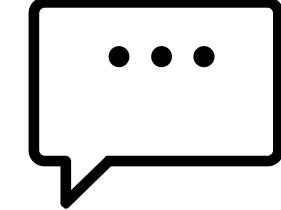


FOTO PRIVATE

Ricatti ed estorsioni
Valore: \$\$\$



SMS, CONTATTI, CHAT...

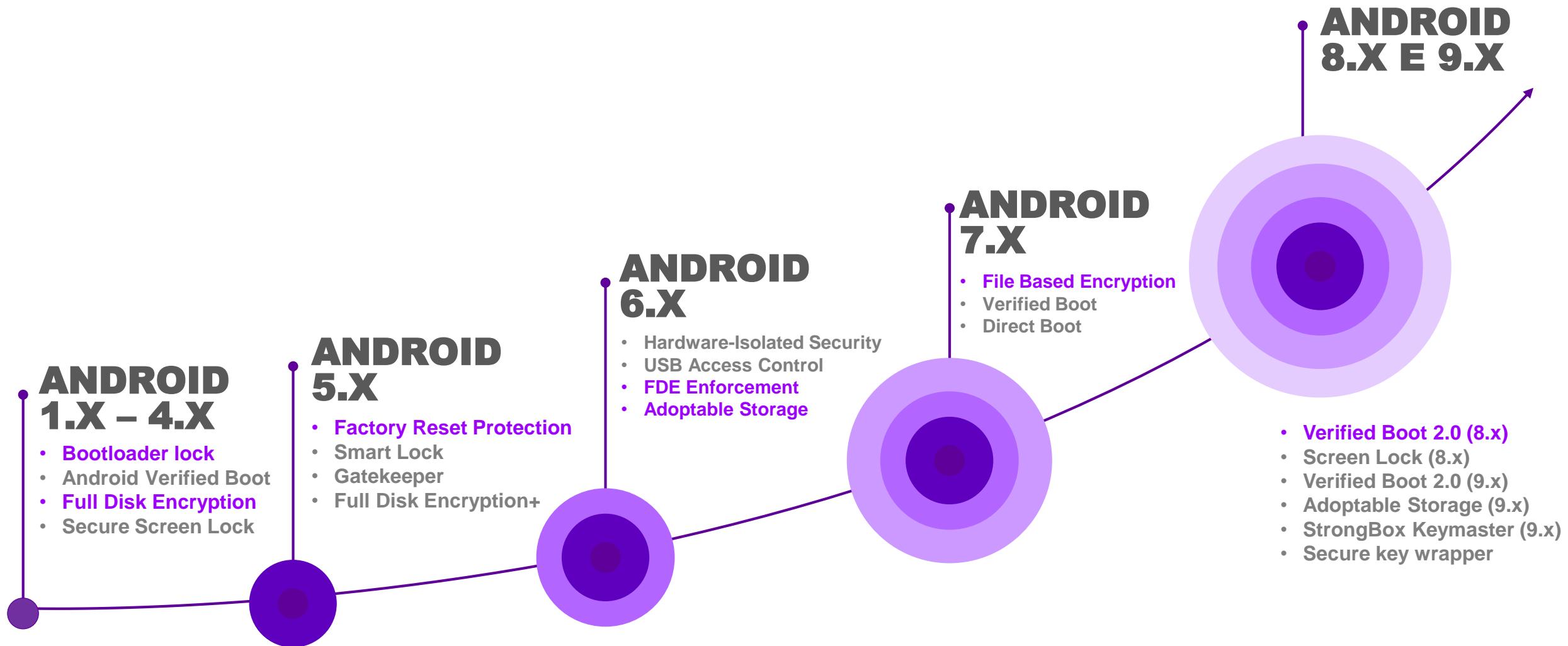
Estorsioni e ricatti, attacchi di phishing, contraffazioni...

Valore:\$\$\$



STATO DELL'ARTE DELLA SECURITY DEVICE MOBILI

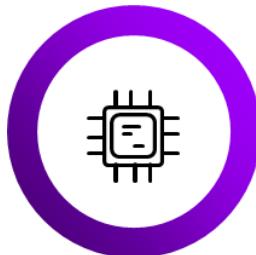
PRINCIPALI MISURE DI SICUREZZA ANDROID



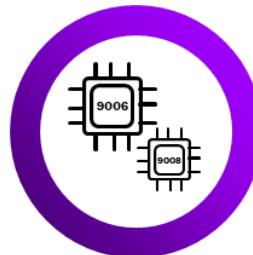
ACQUISIZIONE DISPOSITIVO ANDROID: SFIDE

L'ETERogeneità dell'ecosistema ANDROID rende il processo dell'acquisizione VENDOR-DEPENDENT

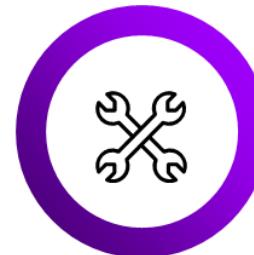
COME EFFETTUARE UN'ACQUISIZIONE FINO ALLA VERSIONE ANDROID 6.0 CON DISPOSITIVO BLOCCATO E FDE NON ATTIVA



LA TECNICA CHIP-OFF



LA MODALITÀ EDL
9006 O 9008 PER I
DISPOSITIVI CON
CHIPSET
QUALCOMM SOC.



MANTAINANCE
TOOL FORNITI
DIRETTAMENTE
DAI VENDOR



ROOTING



EXPLOITS



FORENSICS
BOOTLOADERS



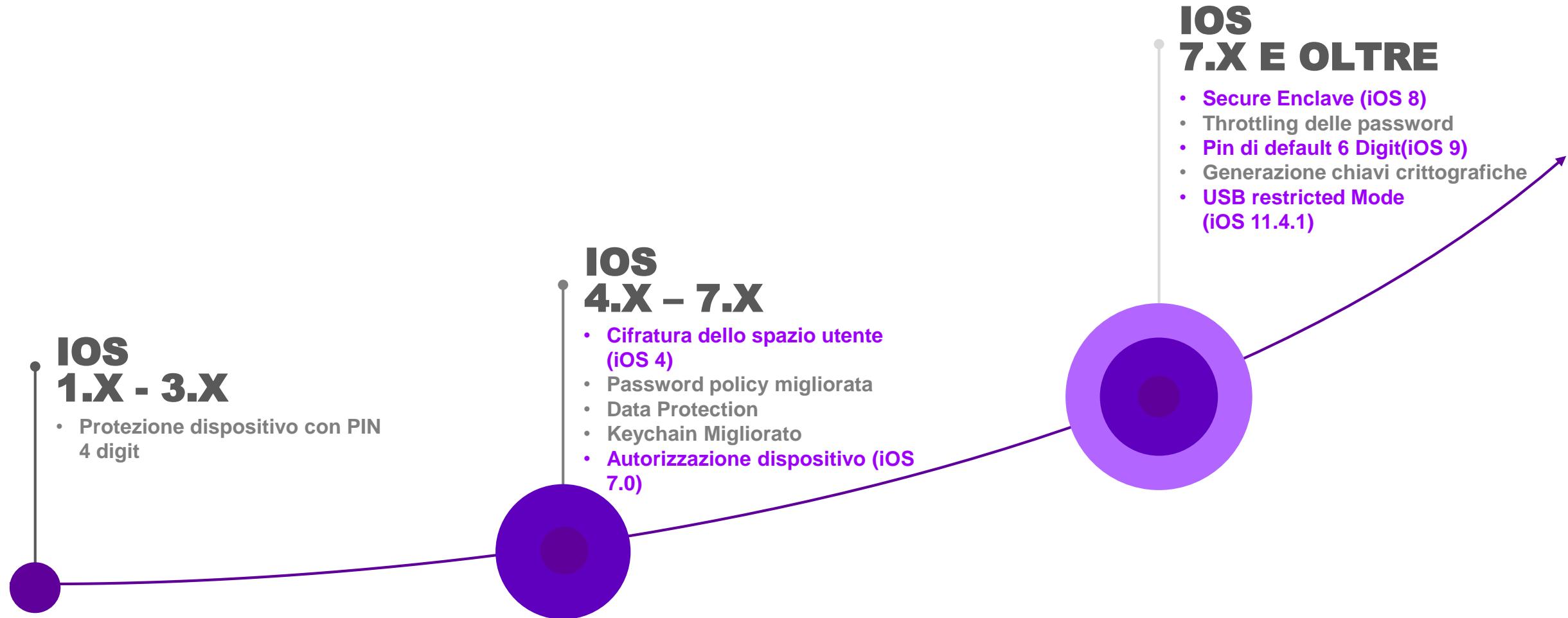
CUSTOM
RECOVERY
IMAGES

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

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

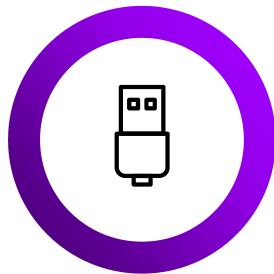
Per versioni superiori alcune volte è possibile sfruttare delle vulnerabilità documentate per effettuare l'acquisizione. A partire dalla versione 6 di Android **l'intero filesystem è cifrato di default**.

PRINCIPALI MISURE DI SICUREZZA IOS

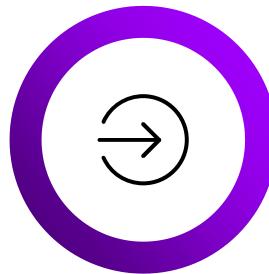


ACQUISIZIONE DISPOSITIVO IOS: SFIDE

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



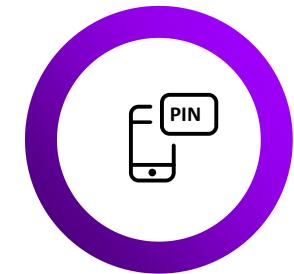
Si può **collegare il dispositivo via USB** a qualsiasi PC untrusted senza autorizzazione (autorizzazione introdotta con la versione 7.x)



Si possono **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**.

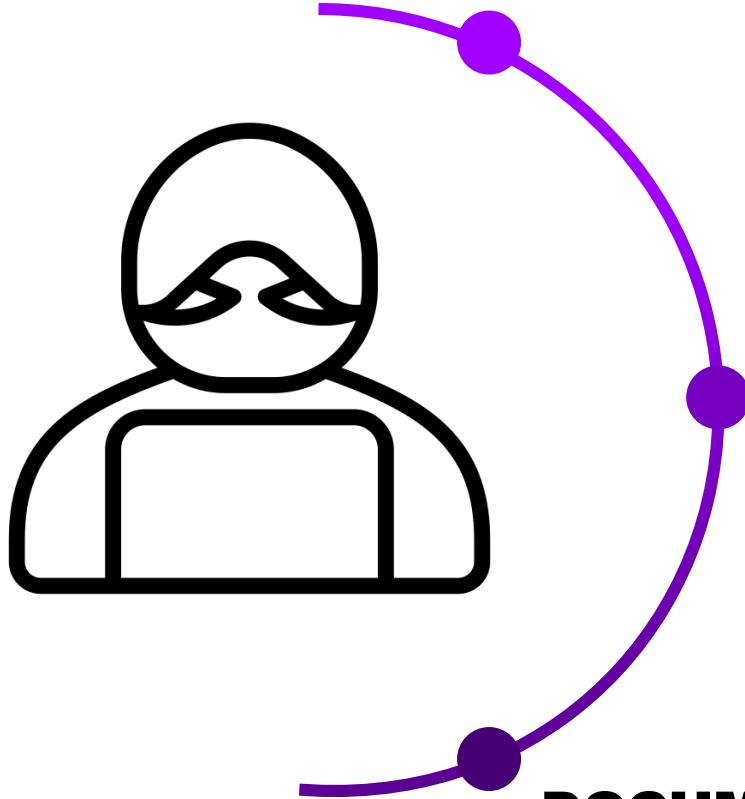
A PARTIRE DA IOS 11.4 VIENE INTRODOTTA LA **MODALITÀ USB RESTRICTED MODE**.

ESEMPI REALI

ACQUISTO DISPOSITIVO USATO

COSA PUÒ FARE UN ATTACCANTE? PRIMA DELL'ACQUISTO

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



Google Nexus 4 Mako Twrp pezzi di ricambio non funzionante

EUR 20,00

0 offerte

+EUR 10,00 spedizione

1o rimaste (Oggi 16:34)

ebay

Sistema operativo:

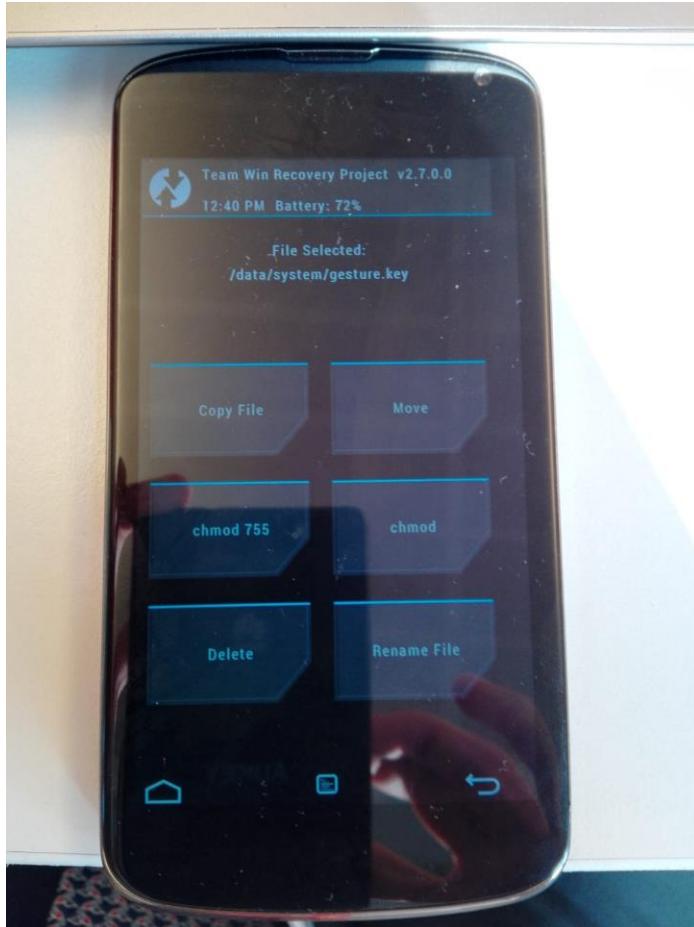
- Ultima versione: Android 5.1.1 (Lollipop) ← **Versione del dispositivo utilizzata per il test**
- Prima versione: 4.2.2 (Jelly Bean)

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

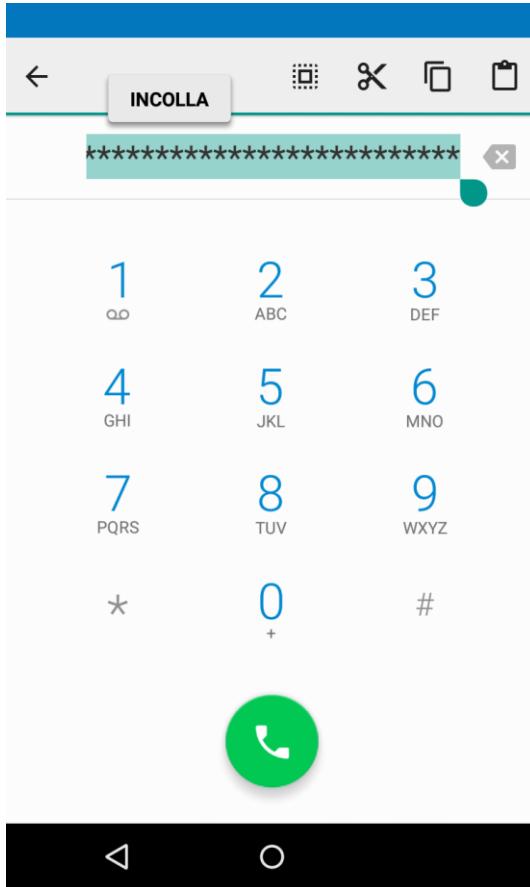
ANDROID

ESEMPIO COSA PUÒ FARE UN ATTACCANTE BYPASS 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



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 BRUTEFORCING



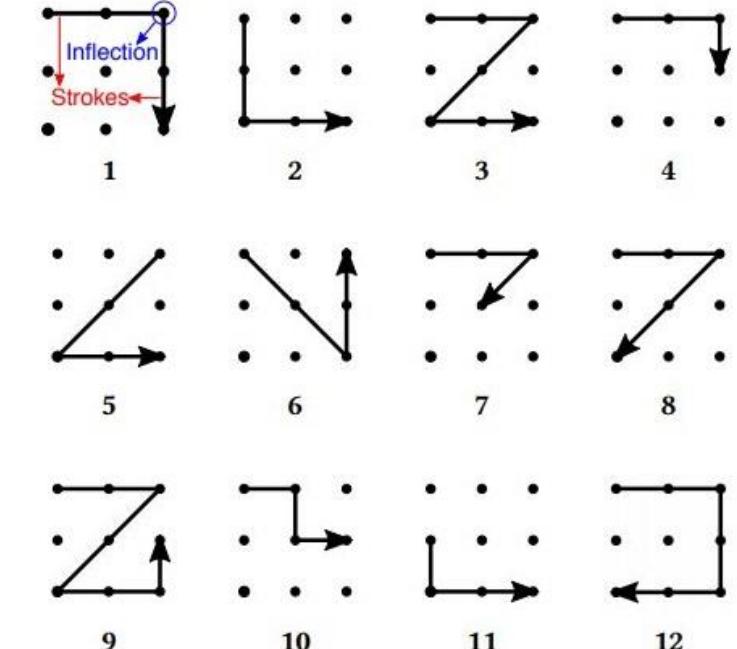
Smudge Attack

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

Smudge Attack

```
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 installato sul device

1. Redirezione delle richieste

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

2. Apertura della shell adb:

```
$ adb shell
```

3. Acquisizione Privilegi 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

The screenshot shows the Autopsy interface with the following sections:

- Data Sources:** userdata_dump.img
- Views:** File Types, Deleted Files (File System (38831), All (38831)), MB File Size.
- Results:** Extracted C, Keyword Hi, Single L, Single F, URLs (2), IP Addr, Phone !, Email A!, Hashset Hit, E-Mail Mess, Interesting, Accounts, Tags, Reports.
- File System Analysis:** Shows a tree view of extracted files from the userdata dump, including folders like orphanfiles, sunalloc, ads, ann, app, audio, backup, dalvik-cache, data, com.alensw.PicFolder, com.amazon.mShop.android.shopping, com.android.backupconfirm, com.android.bluetooth, com.android.browser.provider, com.android.calculator2, com.android.captiveportallogin, com.android.cellbroadcastreceiver, com.android.certinstaller, com.android.chrome, com.android.defcontainer, com.android.documentsui, com.android.externalstorage, com.android.htmlviewer, com.android.inputdevices, com.android.keychain, com.android.launcher, com.android.location.fused, com.android.managedprovisioning, com.android.mms, com.android.mms.service, com.android.musicfx, and shared_prefs.
- SMS Analysis:** A table titled "SMS" showing incoming messages from various phone numbers (mmssms.db) with details like direction, from phone number, and timestamp.
- File Metadata:** A table titled "File Metadata" showing file names, modified time, change time, and access time for various files.

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)

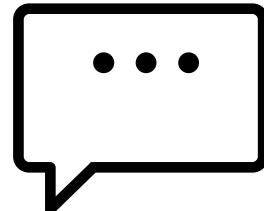


ANDROID

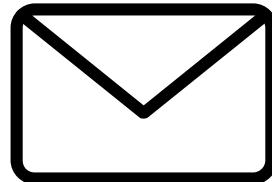
ESEMPIO REALE COSA PUÒ FARE UN ATTACCANTE
RESOCONTO DATI RECUPERATI (SENZA CARVING) DA
NEXUS 4 DI TEST



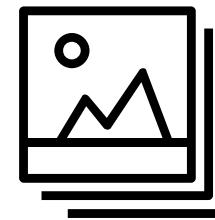
456
Contatti



189
SMS



528
E-MAIL



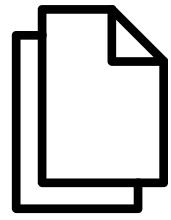
216 Immagini
13 Video
GALLERIA



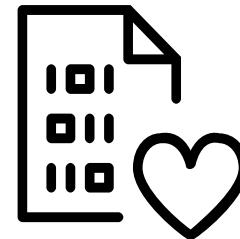
**Exif
metadata
MAPPE**



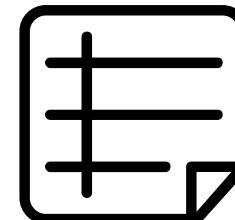
15 Bookmarks
2203 Web Cookies
1 Web Download
WEB BROWSER HISTORY



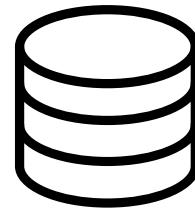
**78 PDF
DOCUMENTI**



**DB Whatsapp
DATI DEI SOCIAL
NETWORK**



**N/A
NOTE**



**38831 File
DATI
ELIMINATI**

```
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

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

The screenshot shows the Autopsy interface with three main panes:

- File System Tree:** Shows a tree view of recovered files under "Android (5)" and "data (47)".
- Data Sources:** Shows a list of data sources:
 - userdata_dump_wipe.img:** Selected and highlighted.
 - \$OrphanFiles (68653)**
 - \$CarvedFiles (4281)**
 - \$Unalloc (22)**
- Table View:** Shows a table of recovered files from "img_userdata_dump_wipe.img/media/0/WhatsApp/Databases".

Name	Modified Time
[current folder]	2017-03-19
[parent folder]	2016-05-27
msgstore-2016-07-25.1.db.crypt12	2017-06-10
msgstore-2016-07-26.1.db.crypt12	2017-06-10
msgstore-2016-07-28.1.db.crypt12	2017-06-10
msgstore-2016-05-26.1.db.crypt10	2016-06-10
msgstore-2016-07-21.1.db.crypt12	2016-07-29
msgstore-2016-07-22.1.db.crypt12	2016-07-31
msgstore-2016-07-23.1.db.crypt12	1970-01-14
msgstore-2016-07-29.1.db.crypt12	2017-04-01
msgstore-2016-07-30.1.db.crypt12	2017-04-01
msgstore.db.crypt12	2017-03-19

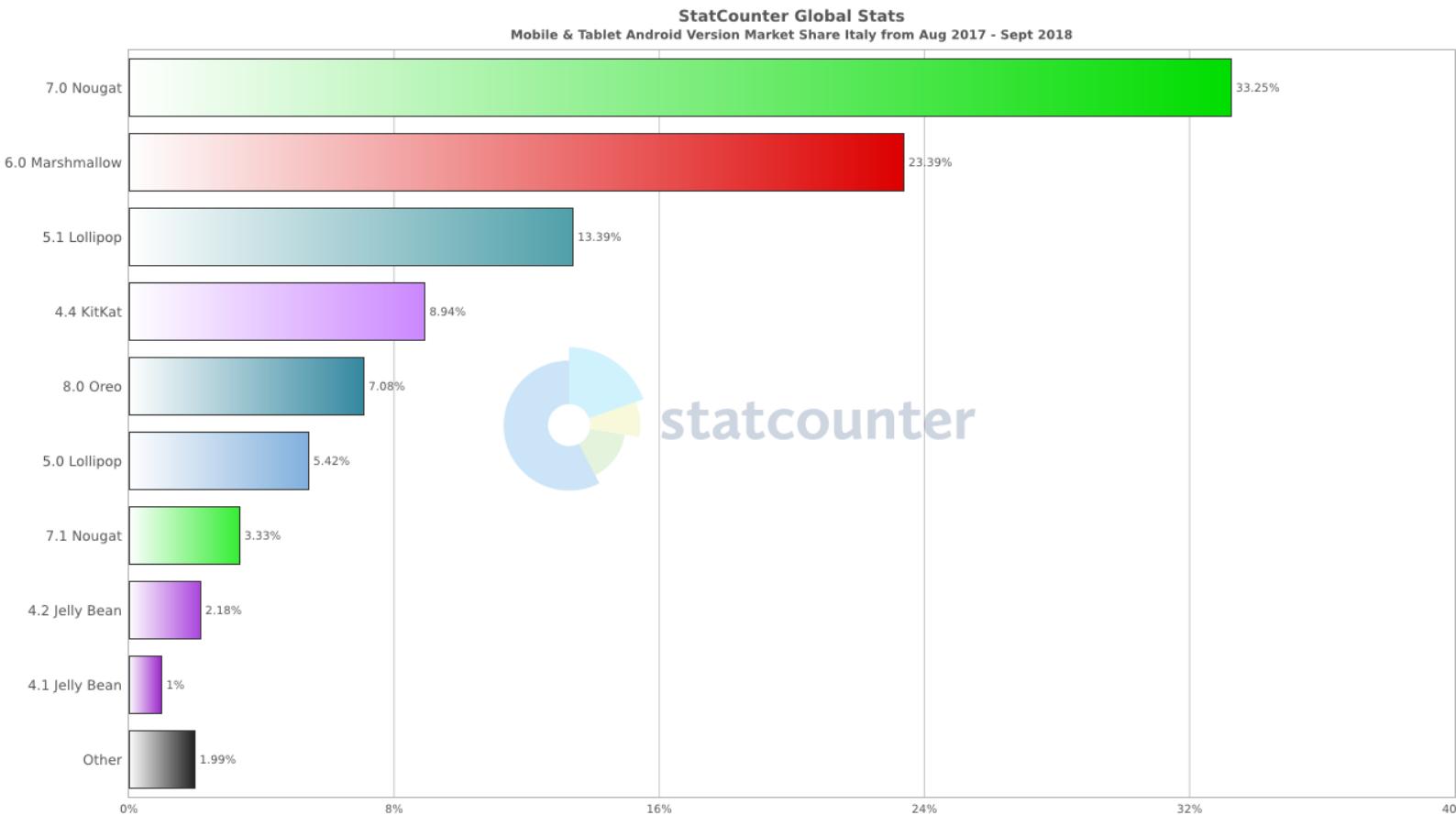


Cosa abbiamo recuperato:

- 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



- 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.

Ref: statcounter.com

DISPOSITIVI ANDROID ROOTED

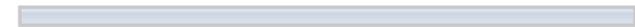
INTERVALLO TEMPORALE NOVEMBRE 2014 – ORA

Is your primary Android device (the one you use most) rooted?

Yes. (63%, 9,097 Votes)



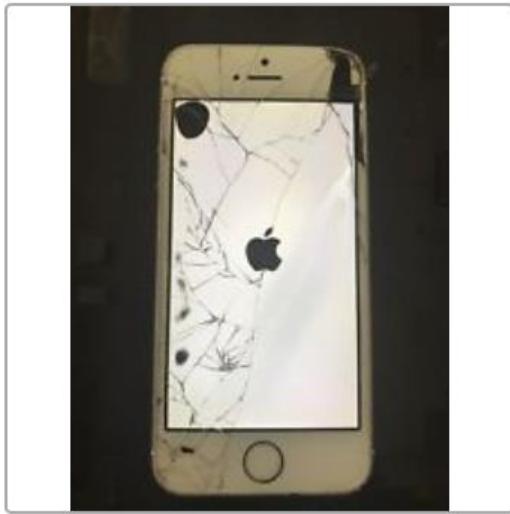
No. (37%, 5,248 Votes)



Total Voters: 14,345

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

ESEMPIO COSA PUÒ FARE UN ATTACCANTE



Apple Iphone 5 Schermo e touch non funzionante

EUR 11,96

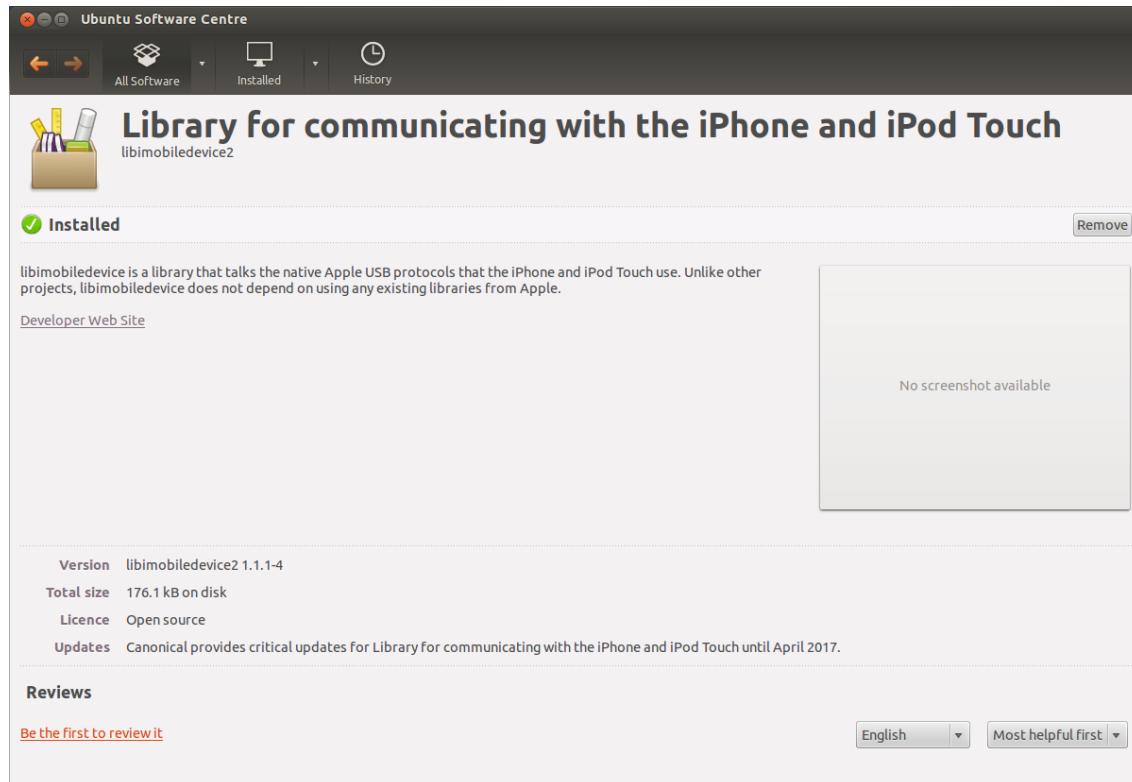


60 rimaste

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 sia presente pin

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

iOS Version: 11.4

Name	Count
System	337
AppDomain-com.apple.AXUIViewService	0
AppDomain-com.apple.AccountAuthenticationDialog	0
AppDomain-com.apple.ActivityMessagesApp	0
AppDomain-com.apple.AdPlatformsDiagnostics	0
AppDomain-com.apple.AppStore	0
AppDomain-com.apple.CTCarrierSpaceAuth	0
AppDomain-com.apple.CloudKit.ShareBear	0
AppDomain-com.apple.CompassCalibrationViewService	0
AppDomain-com.apple.CoreAuthUI	0
AppDomain-com.apple.DemoApp	0
AppDomain-com.apple.Diagnostics	0
AppDomain-com.apple.DiagnosticsService	0
AppDomain-com.apple.DocumentsApp	1
AppDomain-com.apple.Health	0
AppDomain-com.apple.HealthPrivacyService	0
AppDomain-com.apple.InCallService	0
AppDomain-com.apple.Magnifier	0
AppDomain-com.appleMaps	1
AppDomain-com.apple.MobileAddressBook	0

iBackup Viewer - Free

Pippo - iOS Version: 11.4

All

History

- Bookmarks
- BookmarksBar
- com.apple.ReadingList
- com.apple.FrequentlyVisitedSites

Camera Roll 2

Photo Stream 0

Photos 2

Videos 0

Favorites 0

Transed 0

ALBUMS

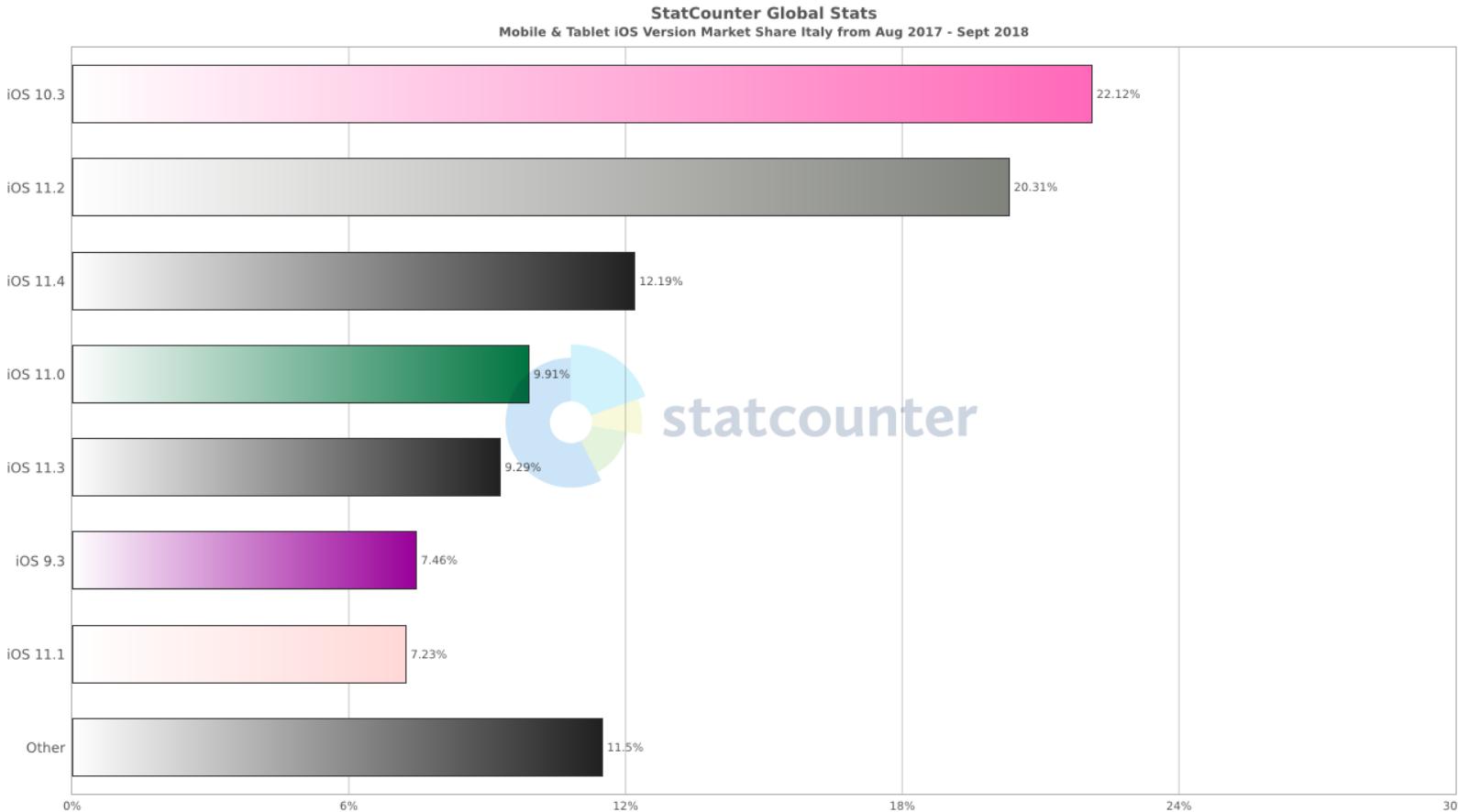
Xabsi [Full Revi... https://m.pangu...

EMAIL
testmario@test.it
gino rua
ID Apple, iCloud, i1
Nessun backup di iPhone
Concludi la configurazion

PASSWORD
Cliented1
Hai dimenticato la password
q w e r t y
a s d f g
Uso in aereo
Wi-Fi Nrr

DIFFUSIONE DISPOSITIVI IOS

INTERVALLO TEMPORALE AGOSTO 2017 – SETTEMBRE 2018



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

Ref: statcounter.com

CONCLUSIONI

SO WHAT?

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

05



Assicurarsi di aver rimosso custom recovery, mod, root, jailbreak...

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



THANK YOU!



MATTEO REDAELLI



m.redaelli@accenture.com



[@solventred](https://twitter.com/solventred)