Mobile Security Threats

Adi Sharabani

About me

Adi Sharabani

CEO & co-founder, Skycure

- Over 15 years of security experience
- Built and managed Watchfire's research group
- Built and led IBM's worldwide Rational security initiative, was responsible for IBM software products, developed by thousands of developers worldwide
- Author of more than 20 patents
- Fellow at Yuval Ne'eman's workshop
- High school teacher

Skycure

About Skycure

- Provides seamless security for mobile devices
- Sell to large organizations
- Backed by Pitango Venture Capital
- Team consists of elite security experts coming from IBM, Google, CheckPoint and more

Mobile Security Threats

5 Biggest Mobile Threats

Skycure

The Simple Threat

Physical Access

1

Skycure

The Known Threat

Malware

2

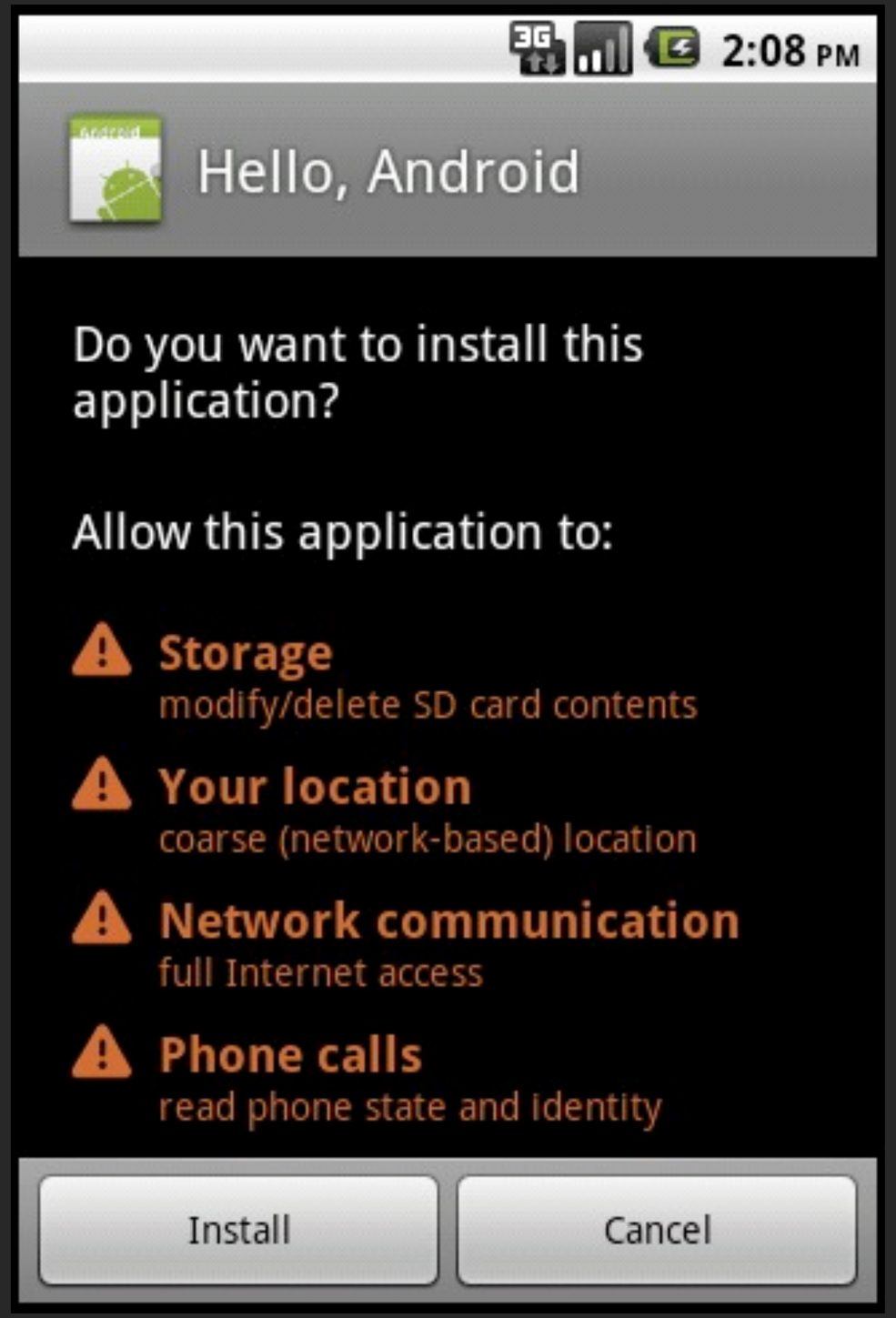
Skycure

The Known Threat

Malware

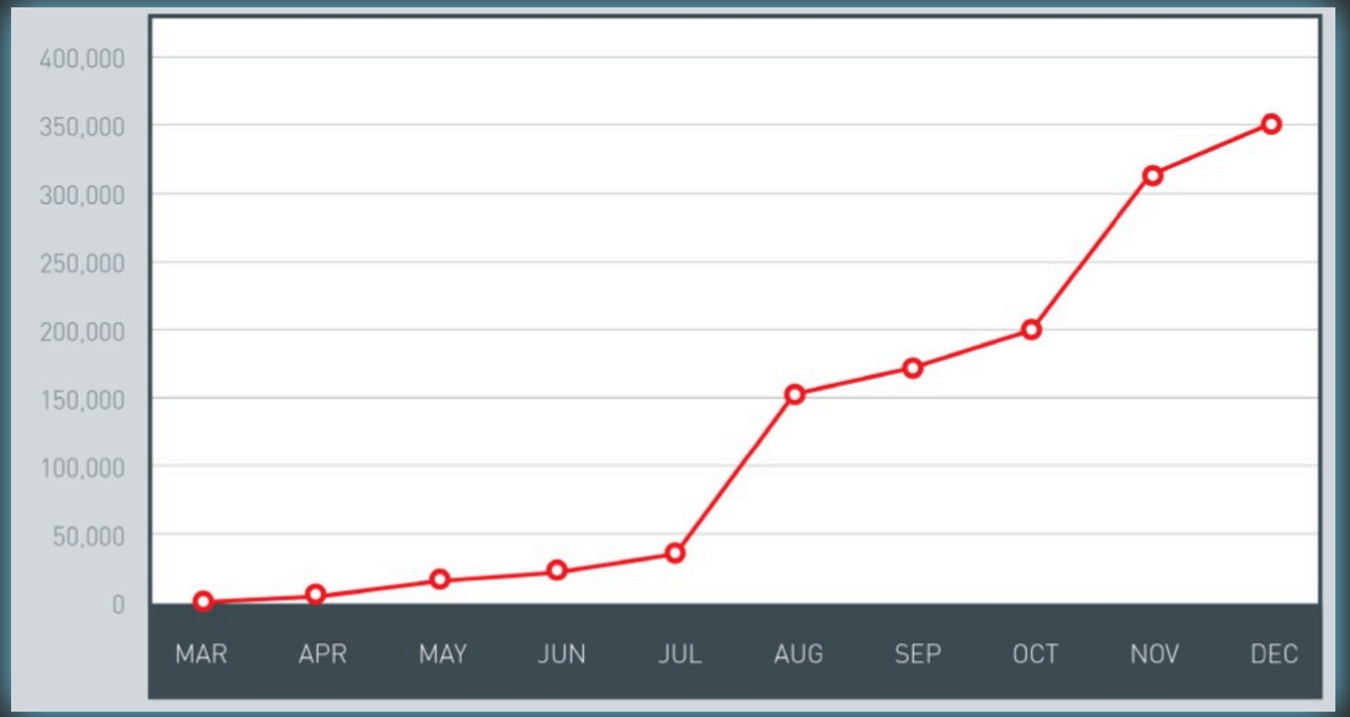
2

Skycure



2012: The year of Android malware

Android Threat Growth



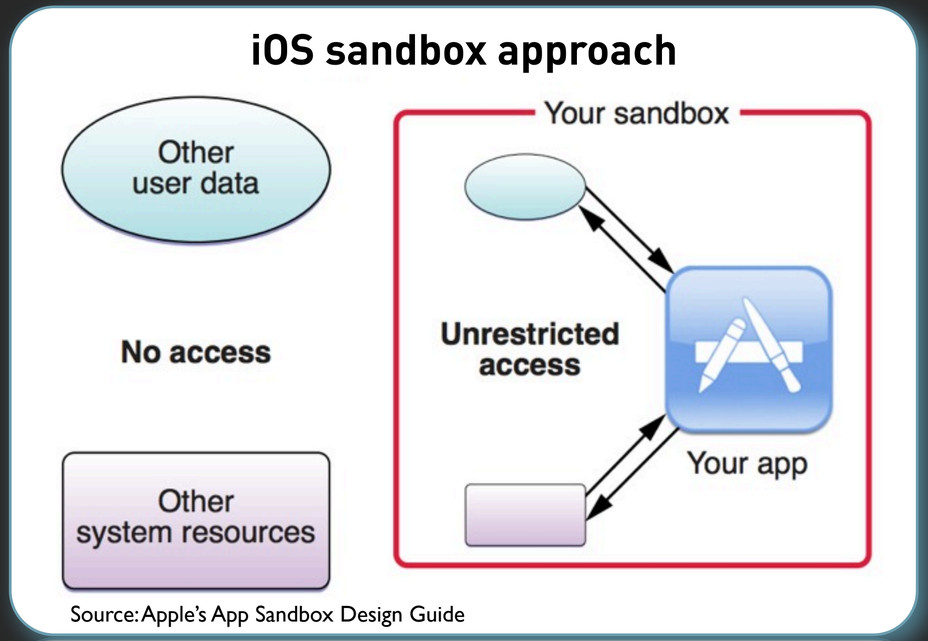
Source: Trend Micro 2012 Mobile Threat and Security Roundup

Skycure

iOS Security Model

App Characteristics

- One Store
- Heavy Screening
- App Sandboxing



Skycure

iOS Security Model

App Characteristics

- One Store
- Heavy Screening
- App Sandboxing

Profile Characteristics

- No Store
- No Screening
- No Sandboxing

Profiles break the iOS security model

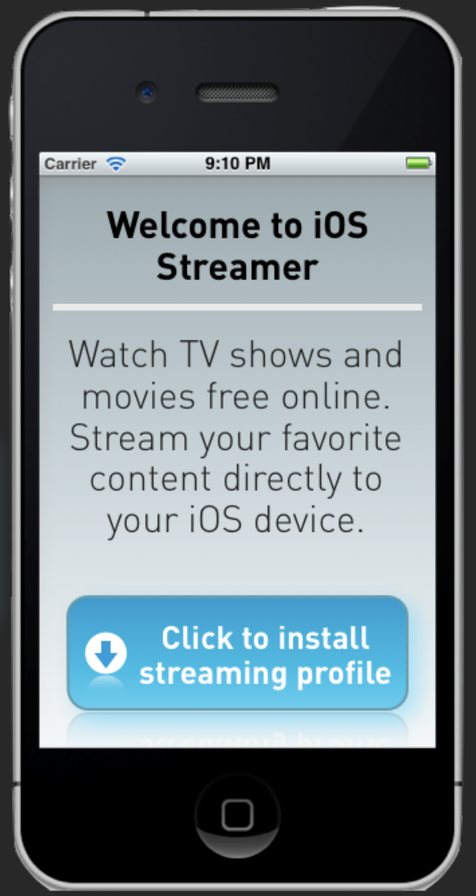
Skycure

Mobile Security Threats

Malicious Profiles

For iOS, the incarnation of malware is malicious configuration profiles.

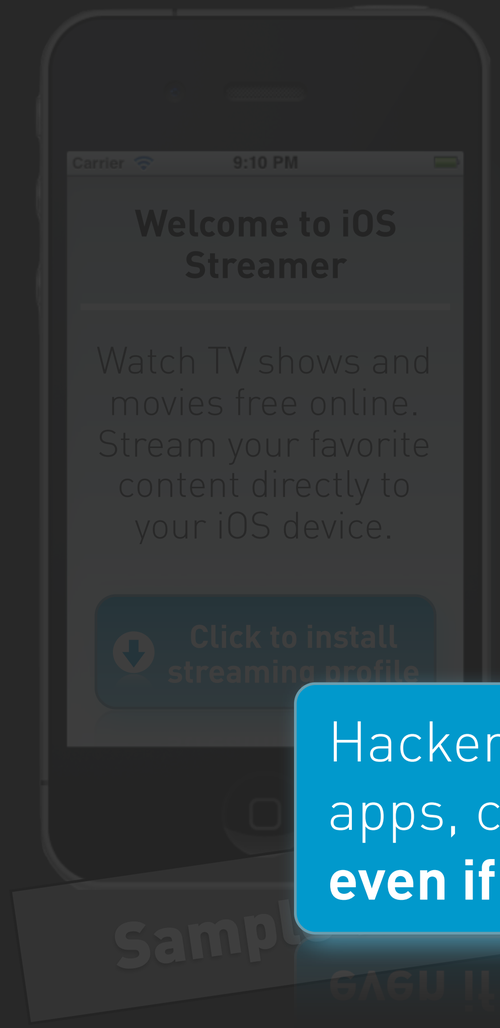
Profiles break the iOS security model



Recent relevant Skycure discovery
http://blog.skycure.com/2013/03/malicious-profiles-sleeping-giant-of.html

Skycure

2013:
The year of iOS malware



Hacker gains access to your mail, business apps, cloud services, bank accounts and more, **even if traffic is encrypted**

Skycure

The Biggest Threat

Wi-Fi Networks

3

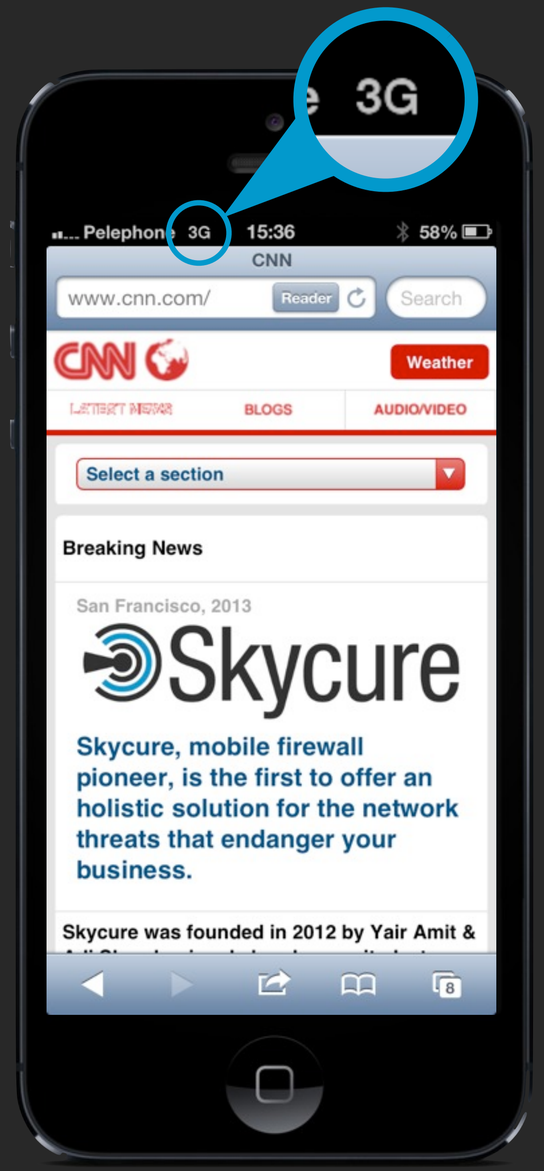
Skycure

Mobile Security Threats

Wi-Fi Attacks

Are you comfortable connecting to Wi-Fi networks?

Did you know that connecting to a public Wi-Fi could lead to **persistent** control over your device?



Skycure

History of MiTM

Wi-Fi attacks becomes more prevalent with mobile use

These attacks have two main requirements:

Attacker has to be in a nearby location	Mar 2013: Malicious iOS profiles MiTM has become fully remote
User has to actively connect to the Wi-Fi	?

Skycure

Connecting to Wi-fi networks

"I hardly connect to wi-fi networks, so I'm protected. Right?"

Skycure

Connecting to Wi-fi networks

Skycure

Wi-Fi Guessing

Auto Connect

Skycure

WiFiGate

"I have **never** connected to Wi-Fi networks, so I'm protected. Right?"

Skycure

WiFiGate

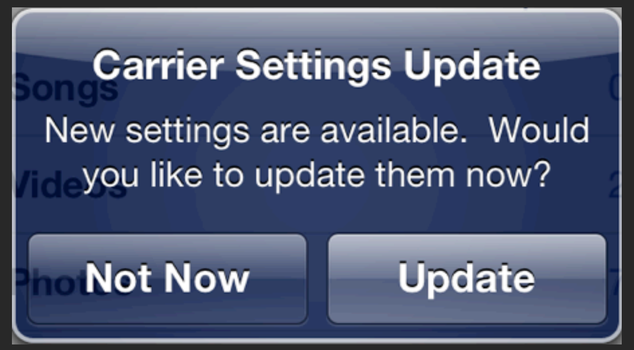
"I have never co to
Wi-Fi ne m
Right?"

Wrong!

Skycure

WiFiGate

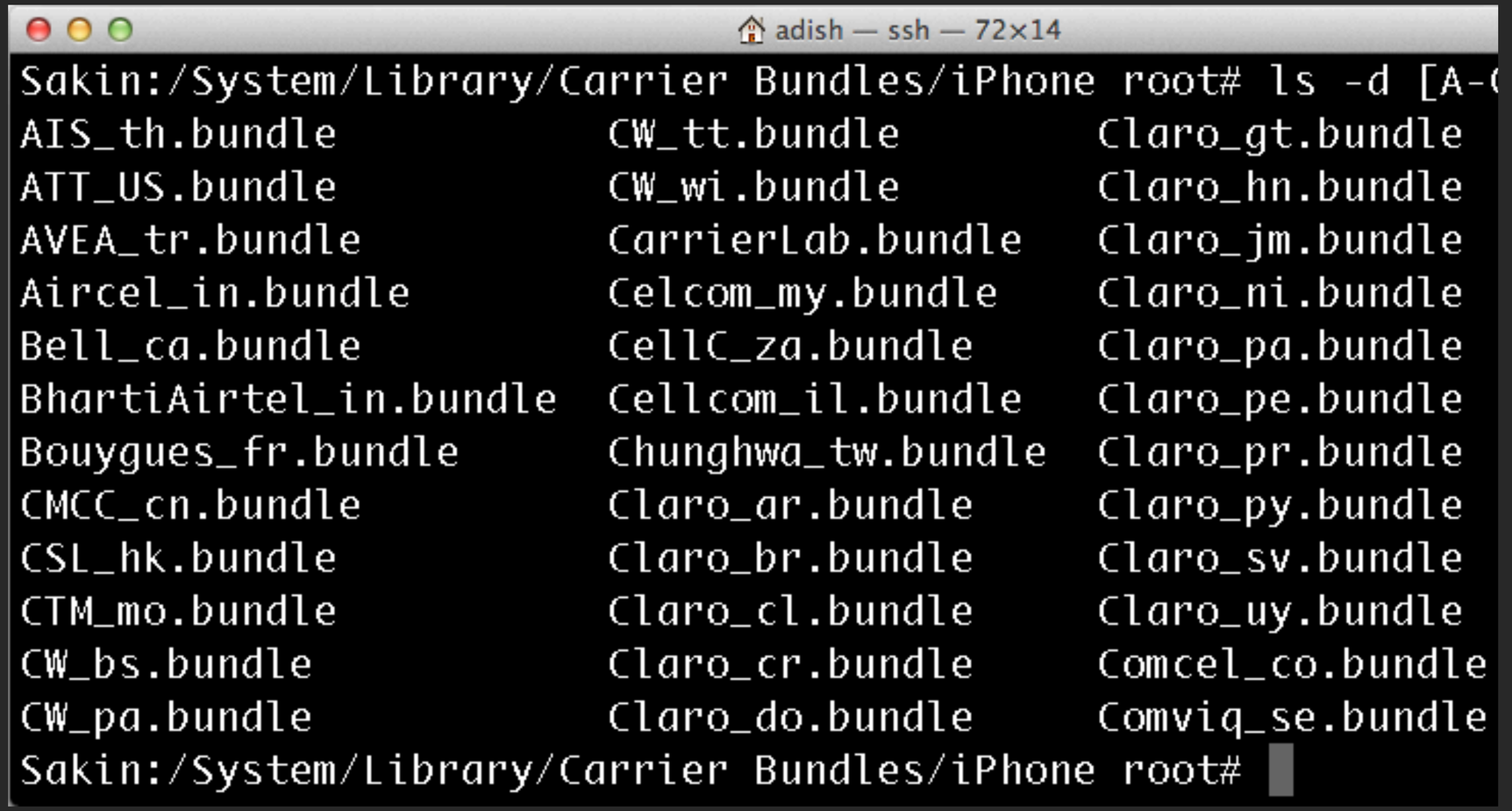
In practice, many carrier settings configures wi-fi networks on user behalf



Skycure

WiFiGate

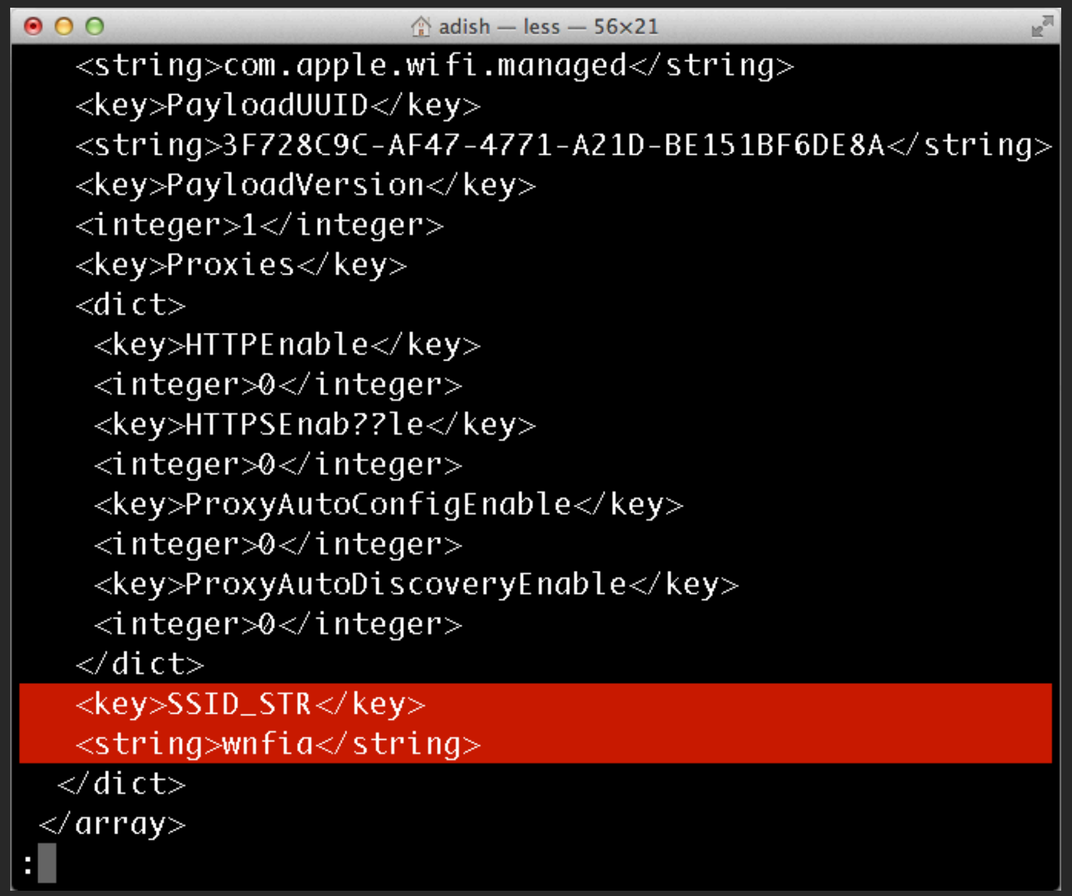
In practice, many carrier settings configures wi-fi networks on user behalf



Skycure

WiFiGate

In practice, many carrier settings configures wi-fi networks on user behalf



Setting-up such a network would automatically initiate an attack on all nearby carrier customers

Skycure

Putting the attack to test

Attack - During the cyber security conference

- Location: Smolarz Auditorium, TAU

Skycure

Putting the attack to test

Attack - During the cyber security conference

- Location: Smolarz Auditorium, TAU
- **448** devices connected to our in **2.5** hours

Skycure

Remediation

So what should you do about this?

- Users and Organizations:
  Close the Wi-Fi connection when not in use
  Use a mobile firewall protection

- Carriers and Wi-Fi network providers:
  If you need to provide Wi-Fi access, enable client-side firewall capabilities on it

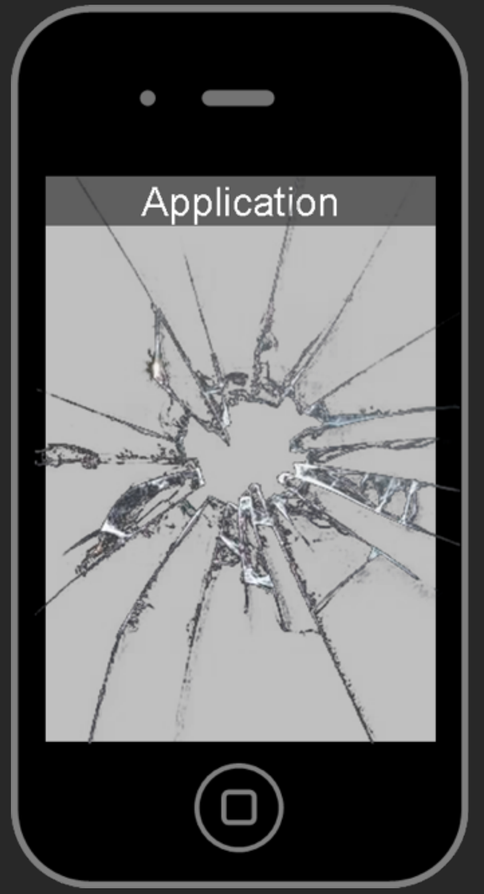
Join our beta program
contact@skycure.com

Skycure

The Growing Threat

Vulnerabilities in Apps and OS

4



Skycure

The Growing Threat

Vulnerabilities in Apps and OS

4

Skycure

The Growing Threat

Vulnerabilities in Apps and OS

4

Skycure

The Leaking Threat

Privacy

5

Skycure

The Leaking Threat

Privacy

5

Skycure

2012: Skycure uncovers a major privacy violation in the LinkedIn app

LinkedIn leaked out its users' calendar information

Skycure's discovery in the news


```
{"calendar":{"calendarOptIn":true,"values":[{"e
vents":[{"organizer":{"name":"Adi Sharabani","e
mail":"adi@skycure.com"},"id":"635D0B49-1A84-44
5E-9FCD-00F975468B90:03E3338028A54FC0945BA33119
C297A700000000000000000000000000000000","notes"
:"AT&T conference call:\n USA:1-800-225-5288\n
Passcode:4218000#","endDate":"1338559200000","s
tartDate":"1338555600000","attendees":[{"name":
"Yair Amit","email":"yair@skycure.com"}],"title
":"Confidential:  Internal financial results"}]
,"timestamp":"1338498000000"}]}}
```


- The New York Times
- Forbes
- BBC
- The Verge
- The Huffington Post
- Washington Post
- The Next Web
- Gizmodo
- Ars technica
- Apple Insider
- CSO Online
- cnet

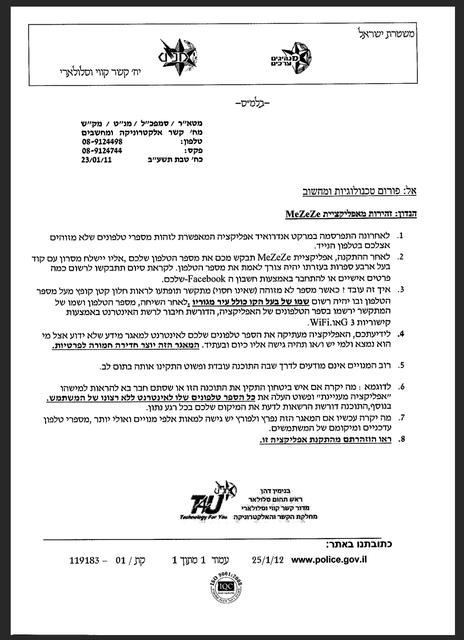
The Leaking Threat

Privacy

5

Following our work, LinkedIn changed their app to ask the user for permission to leak out the information

When it comes to organizations, the problem is still unsolved



משטרת ישראל

יחי קשר קווי וטלולארי

-בלמ"ס-

מטא"ר / סמפכ"ל / מנ"ט / מק"ש
מחי קשר אלקטרוניקה ומחשבים
טלפון: 08-9124498
מקש: 08-9124744
כחי טבת תשע"ב 23/01/11

אל: פורום טכנולוגיות ומחשוב

הנדון: זהירות מאפליקציית MeZeZe

1. לאחרונה התפרסמה במרקט אנדרואיד אפליקציה המאפשרת לזהות מספרי טלפונים שלא מזוהים אצלכם בטלפון חנייד.
2. לאחר התקנה, אפליקציית MeZeZe תבקש מכם את מספר הטלפון שלכם, אליו יישלח מסרון עם קוד בעל ארבע ספרות בסרוזו יהיה צורך לאמת את מספר הטלפון. לקראת סיום התהבקשו לרשום כמה פרטים אישיים או להתחבר באמצעות חשבון ח Facebook-שלכם.
3. אין זה עובד ! כאשר מספר לא מזוהה (שאינו חסוי) מתקשר תופתע לראות חלון קטן קופץ מעל מספר הטלפון ובו יהיה רשום **שמו של בעל הקו פולל עיר מגוריו** ,לאחר השיחה, מספר הטלפון ושמו של המתקשר ירשמו בספר הטלפונים של האפליקציה, הדורשת חיבור לרשת האינטרנט באמצעות קשוריות WiFi.ואG 3.
4. לידיעתכם, האפליקציה מעתיקה את הספר טלפונים שלכם לאינטרנט למאגר מידע שלא ידוע אצל מי חוא נמצא ולמי יש ראו תהיה גישה אליו כיום ובעתיד. **המאגר הזה יוצר חדירה חמורה לפרטיות.**
5. רוב המנויים אינם מודעים לדרך שבה התוכנה עובדת ופשוט התקינו אותה בתום לב.
6. לדוגמא : מה יקרה אם איש ביטחון התקין את התוכנה הזו או שסתם חבר בא להראות למישהו יאפליקציה מעניינת ופשוט העלה את **כל הספר טלפונים שלו לאינטרנט ללא רצונו של המשתמש.** בנוסף,התוכנה דורשת הרשאות לדעת את המיקום שלכם בכל רגע נתון.
7. מה יקרה עכשיו אם המאגר הזה נפרץ ולפורץ יש גישה למאות אלפי מנויים ואולי יותר , מספרי טלפון עדכניים ומיקומם של המשתמשים.
8. **ראו הוזהרתם פהתקנת אפליקציה זו.**

בניסן דהן
ראש החוט סלולארי
מדור קשר קווי וסלולארי
מחלקת הקשר והאלקטרוניקה

כתובתנו באתר:
www.police.gov.il 25/1/12 עמוד 1 מתוך 1 קת / 01 – 119183

Skycure

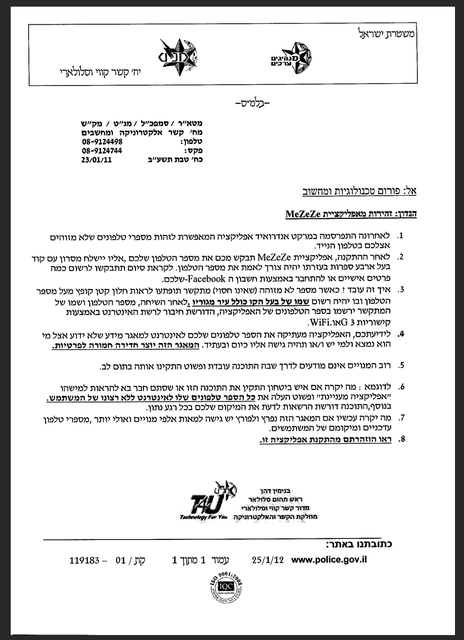
The Leaking Threat

Privacy

5

Following our work, LinkedIn changed their app to ask the user for permission to leak out the information

When it comes to organizations, the problem is still unsolved



משטרת ישראל

יחד קשר קוי וסלולארי

-כלשיט-

מטא"ר / שמפכ"ל / מנכ"ט / מקי"ש
מח' קשר אלקטרוניקה ומחשבים
טלפון: 08-9124498
מקש: 08-9124744
כח' טבת תשע"ב 23/01/11

אל: פורום טכנולוגיות ומחשוב

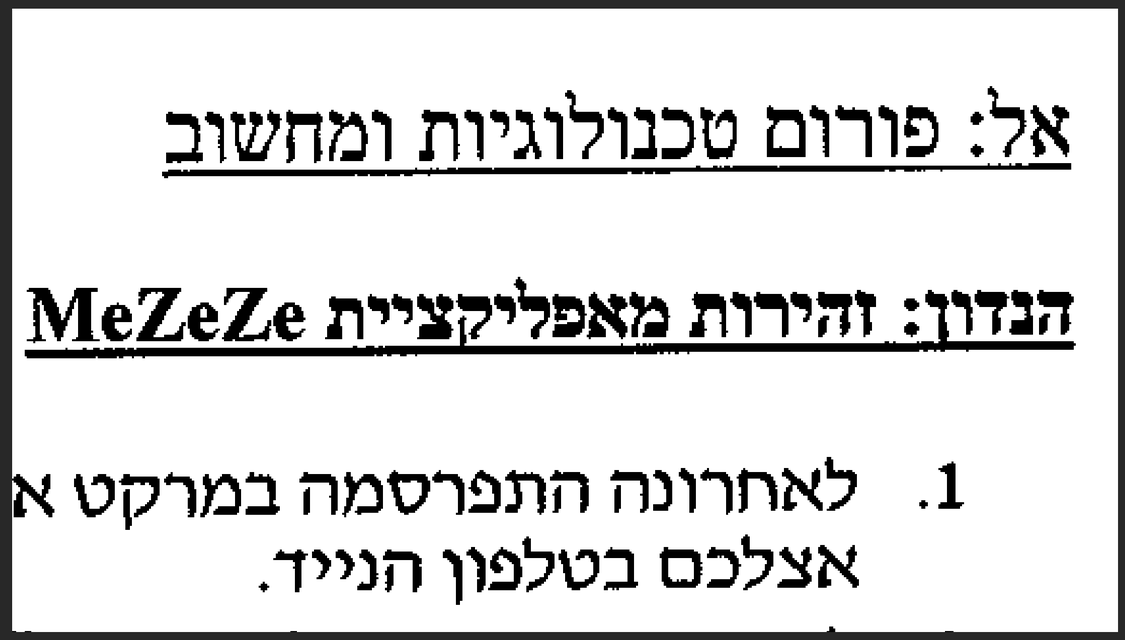
הנדון: זהירות מאפליקציית MeZeZe

1. לאחרונה התפרסמה במרקט אנדרואיד אפליקציה המאפשרת לזהות מספרי טלפונים שלא מזוהים אצלכם בטלפון הנייד.
2. לאחר התקנה, אפליקציית MeZeZe תבקש מכם את מספר הטלפון שלכם, אליו יישלח מסרון עם קוד בעל ארבע ספרות בתוכנו יהיה צורך לאמת את מספר הטלפון. לקראת סיום תתבקשו לרשום כמה פרטים אישיים או להתחבר באמצעות חשבון ה Facebook-שלכם.
3. אין זה עובד ! כאשר מספר לא מוזהה (שאינו חסוי) מתקשר תופתע לראות חלון קטן קופץ מעל מספר הטלפון ובו יהיה רשום **שמו של בעל הקו בקול ערב מנוירו** ,לאחר השיחה, מספר הטלפון ושמו של המתקשר ירשמו בספר הטלפונים של האפליקציה, החדשנית חיבור לרשת האינטרנט באמצעות קישוריות 3 WiFi ,nG.
4. לידיעתכם, האפליקציה מעתיקה את הספר טלפונים שלכם לאינטרנט למאגר מידע שלא ידוע אצל מי הוא נמצא ולמי יש ראו תהיה גישה אליו כיום ובעתיד. **המאגר הזה יוצר חדירה חמורה לפרטיות.**
5. רוב המנויים אינם מודעים לדרך שבה התוכנה עובדת ופשוט התקינו אותה בתום לב.
6. לדוגמא : מה יקרה אם איש ביטחון התקין את התוכנה הזו או שסתם חבר בא להראות למישהו יאפליקציה מעניינת' ופשוט העלה את **כל הספר טלפונים שלו לאינטרנט ללא רצונו של המשתמש**, בנוסף,התוכנה דורשת הרשאות לגישת את המיקום שלכם בכל רגע נתון.
7. מה יקרה עכשיו אם המאגר הזה נפרץ ולפורץ יש גישה למאות אלפי מנויים ואולי יותר , מספרי טלפון עדכניים ומיקומם של המשתמשים.
8. **ראו הוזהרתם פהתקנת אפליקציה זו.**

בכבוד רב
ראש תחום סלולאר
מדור קשר קוי ופיקוחארי
מחלקת הקשר והאלקטרוניקה

כתובתנו באתר: www.police.gov.il

119183 – 01 / קק עמוד 1 מתוך 1 25/1/12



אל: פורום טכנולוגיות ומחשוב

הנדון: זהירות מאפליקציית MeZeZe

1. לאחרונה התפרסמה במרקט א
אצלכם בטלפון הנייד.

מעתיקה את הספר טלפונים שלכם לאינטרנט למאגר מידע שלא
תהיה גישה אליו כיום ובעתיד. **המאגר הזה יוצר חדירה חמורה**

Skycure

A Few Tips

1. Enable “Find Phone” features
2. Do not automatically click “Continue”
3. Be cautious when using public Wi-Fi networks
4. Always update your software
5. Follow me on Twitter:

   My Twitter @AdiSharabani

Contact us contact@skycure.com
Website http://www.skycure.com
Blog http://blog.skycure.com
Twitter @SkycureSecurity

Skycure

Backup Slides

Skycure