

RSA® Conference 2016

San Francisco | February 29 – March 4 | Moscone Center

Threats of Greatest Consequence Heading into 2016



Connect Protect

Mario Vuksan
CEO, ReversingLabs

@reversinglabs



Stories of Greatest Consequence

- Business Email Compromise (BEC)
- Evolving Ransomware
- Repackaging Trusted Mobile Applications
- Open Source Vulnerabilities in Internet of Things (IoT)

The logo consists of the letters 'BEC' in a bold, white, sans-serif font. The letter 'B' is partially cut off on the left by a vertical white line. The letter 'E' is partially cut off on the left by a vertical white line and has a horizontal white bar extending from its top right. The letter 'C' is partially cut off on the right by a vertical white line.

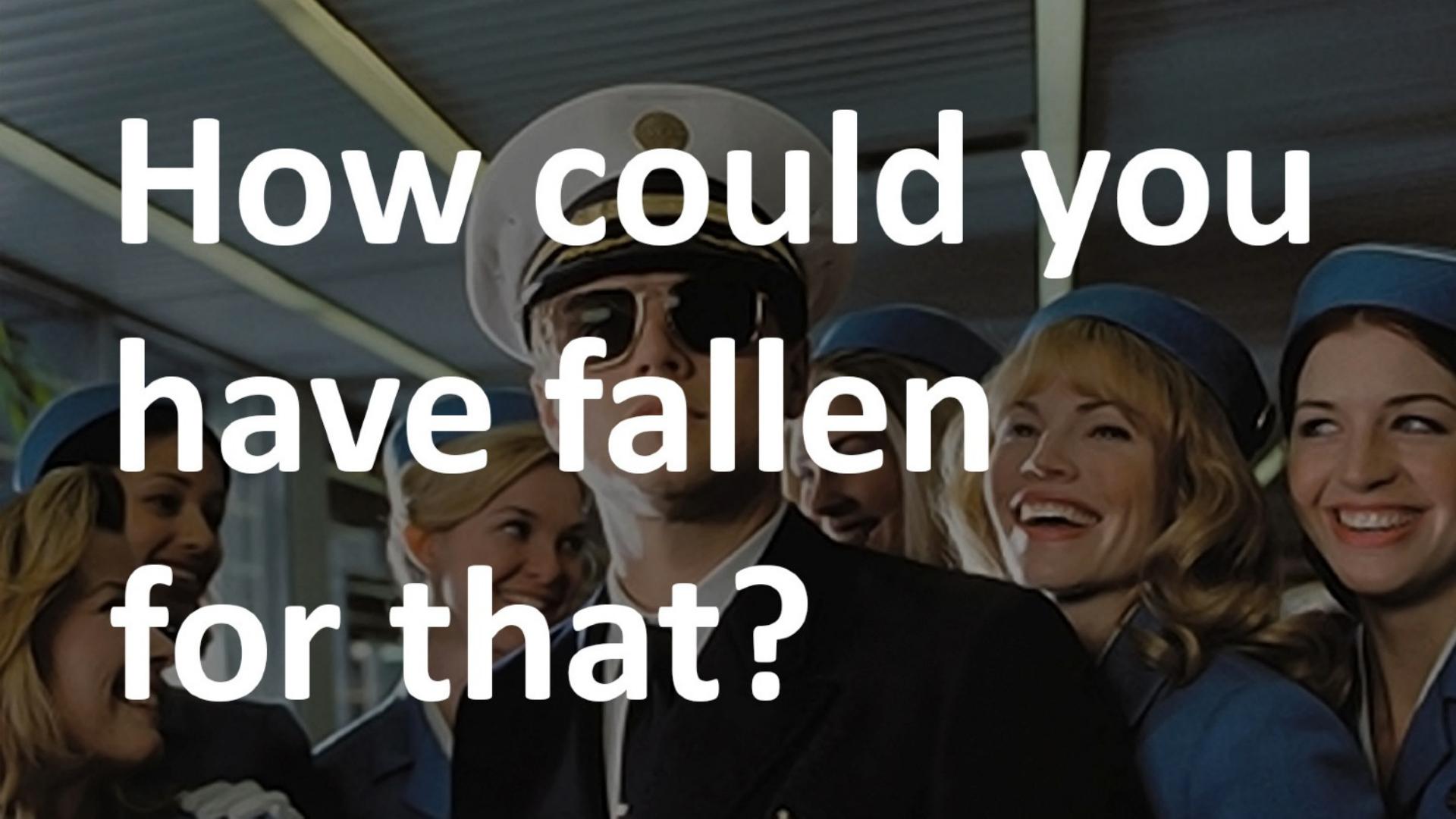
BEC

(Business Email Compromise)





I am your CEO. Send money ASAP!

A photograph showing a group of women in blue flight attendant uniforms and hats looking towards the left. In the foreground, a man wearing a dark tuxedo and a bow tie is looking back at them. The background shows the interior of an airplane with overhead bins.

How could you
have fallen
for that?



BEC

EFFECT



BEC

EFFECT

- Underestimated loss



EFFECT

- Global network spanning
70+ Countries

- Underestimated loss



BEC

EFFECT



- \$ 2.5 B+
in FBI registered claims
the last two years

- Global network spanning
70+ Countries
- Underestimated loss



#RSAC

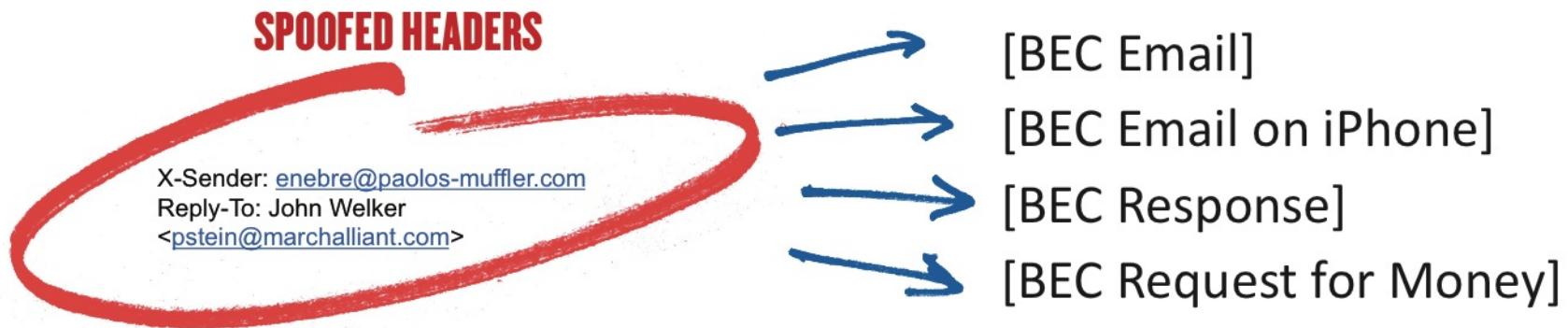
BEC

Is BEC Phishing?



BEC

Scam:
CEO to Anyone in Finance => *Send money fast!*





BEC

From: John Welker <john.welker@polaristech.com>
Reply-To: John Welker <john.welker@polaristech.com>
Date: Monday, February 7, 2016 at 3:07 PM
To: Peter Sangster <Peter.Sangster@polaristech.com>
Subject: Outgoing Vendor's Payment

Peter,

**Are you in the office? I need you to complete a payment today,
I will forward you the instructions soon.**

**Thanks,
John Welker**

Sent from my iPad



BEC

Sent: Tuesday, February 08, 2016 at 8:10 AM
From: "Peter Sangster" <Peter.Sangster@polaristech.com>
To: "John Welker" <john.welker@polaristech.com>
Subject: Re: Outgoing Vendor's Payment

Hi John,

**Sorry for the late response back on this,
my son was up sick all last night and kept my wife and I up.
Do you have the information for the transfer?**

Thanks a bunch!

Peter Sangster

Director of Finance
Polaris Technologies



BEC

From: John Welker <john.welker@polaristech.com>
Reply-To: John Welker <john.welker@polaristech.com>
Date: Tuesday, February 8, 2016 at 10:36 AM
To: Peter Sangster <Peter.Sangster@polaristech.com>
Subject: Re: Outgoing Vendor's Payment

Morning Peter.. How are you?

**I will be sending the infomation for the transfer shortly,
how long will this take to complete once processed?**

**PS: I would need the confirmation # or copy of transfer sheet once
completed so i can confirm with vendor.**

**Advise,
John Welker**

Sent from my iPad



BEC

Sent: Tuesday, February 08, 2016 at 9:40 AM
From: "Peter Sangster" <Peter.Sangster@polaristech.com>
To: "John Welker" <john.welker@polaristech.com>
Subject: Re: Outgoing Vendor's Payment

Hey John,

**Given that everything goes through fine,
the transfer should go through pretty quick.
Once I get the confirmation I can send it over.**

Regards,

Peter Sangster

Director of Finance
Polaris Technologies



BEC

From: John Welker <john.welker@polaristech.com>
Reply-To: John Welker <john.welker@polaristech.com>
Date: Tuesday, February 8, 2016 at 10:48 AM
To: Peter Sangster <Peter.Sangster@polaristech.com>
Subject: Re: Outgoing Vendor's Payment

Okay, here you go:

Bank Name: Chase Bank

Banks Address: 1000 Irvine Ave, Newport Beach, CA 92660

Account Name: James Maxwell Scott

Account Number: 873153008

Routing Number: 732271348

Swift Code: CHASUS33XXX

Amount: \$96,500.00

Let me know when done,

Thanks.

John Welker

Sent from my iPad



BEC

From: Peter Sangster <Peter.Sangster@polaristech.com>
Date: Tuesday, February 8, 2016 at 10:49 AM
To: John Welker <john.welker@polaristech.com>
Subject: Re: Outgoing Vendor's Payment

**Awesome, thanks John!
I'll process this ASAP.**

Regards,

Peter Sangster

Director of Finance
Polaris Technologies



BEC

Money → Mules → International
or financial
Shell laundromat
Companies

Romantic Scams;
Unwitting accomplices;
People who fell on bad time;
and other motives



BEC

HOW DOES IT WORK

- Forged headers
- iPad / iPhone with human (not machine) on the other side
- Weak link (person) and a broken process (easy access to money)
- Fraudsters hiding behind anonymizing VPN services
- Distributed cells and specialized operations

PHISHERS → MULE HERDERS → SHELL COMPANY EXPERTS →
ANONYMIZERS → LAUNDERERS



EVOLVING RANSOMWARE

DEFENSE

- Backup sensitive data
- Use cloud applications offering document backups
- Help Industry/FBI take down actions
- Ransom is not Theft (it is more serious crime)
 - How do nations deal with kidnappers?

Evolving Ransomware

Ransom





**HOLLYWOOD
PRESBYTERIAN
MEDICAL CENTER**



EVOLVING RANSOMWARE

- + Hollywood Hospital paying 9.000 Bitcoin Ransom
- + German Hospitals paying Ransom

STARTING COUPLE YEARS AGO:

Medical practices
reaching out to
Optiv, Mandiant, etc.



Guess
what's the reasonable
recommendation?



EVOLVING RANSOMWARE

Security in Health Care

- Underfunded; ransom is cheaper than security program
- Cash strapped: shut it down and great financial loss can happen
- Serve the public: what all can go wrong if patients are not taken care of
- Equipment that can be serviced only by manufacturers
- Can't add AV or other tools, can't patch them

EVOLVING RANSOMWARE



Fraud → Ransom → Extortion
(banks) (users) (businesses)

Use of non-performing over-harvested Botnet accounts

Operate full Stack Service

Your computer was automatically blocked. Reason: Pirated software

Your computer is now blocked. 94 files have been temporarily blocked. The files will be deleted after 48 hours. If you do not pay, the blocked files will be permanently removed from your computer. If the EHE has two ways to pay a fine:

1. You can pay your fine online through Bitcoin. Bitcoin is available. Click the link below to find the nearest vendor. Your computer will be unblocked as soon as the payment is received. It may take up to 48 hours. Your computer will be unlocked within 4-6 working days.

To regain access transfer bitcoins to the following address
188Q5bAqLdgbqfUWtB9VwHhDzg

After the payment is finalized enter Transfer ID below.

Amount:	Transfer ID:
BTC 0.619	<input type="text"/>
PAY FINE	

If the fine is not paid, a warrant will be issued for your arrest

A screenshot of a mobile application interface. At the top, there's a circular icon containing a yellow seal or logo. To its right, the word "FBI" is written in large, bold, black letters. Below this, in smaller text, it says "FEDERAL BUREAU OF INVESTIGATION". The main body of the screen contains several lines of text in a black sans-serif font. The first line reads "Your device was used to visit websites containing pornography." The second line, which is bolded, reads "Following violations were detected:" followed by a bulleted list: "• Child pornography", "• Zophobia pornography", "• Child abuse", and "• Bulk-spamming". At the bottom, another bolded line reads "Your device also contains:" followed by a bulleted list: "• Video files with pornography content", "• Elements of violence", and "• Child pornography".



EVOLVING RANSOMWARE

EVOLVED PROCEDURE

**Successful SPAM Bots
Document Macro lures
with Exploits
(NEW AND OLD)**

Leverage Advanced Trojan

(LOCKY / DRIDEX)

- SSL, multiple tunneling libraries
- Robust updates and frequently changing DGA

**Target critical
infrastructure and
Get Greedy**



**Leverage best
distribution methods
(UPATRE)**

- Source code obfuscation → perfect evasion
- Standardized AV/Sandbox evasion libraries

**Drop a quality
Ransomware Trojan**



EVOLVING RANSOMWARE

DEFENSE

- Backup sensitive data
- Use cloud applications offering document backups
- Help Industry/FBI take down actions
- Ransom is not Theft (it is more serious crime)
 - How do nations deal with kidnappers?

Rerepackaging — Trusted — Mobile Apps



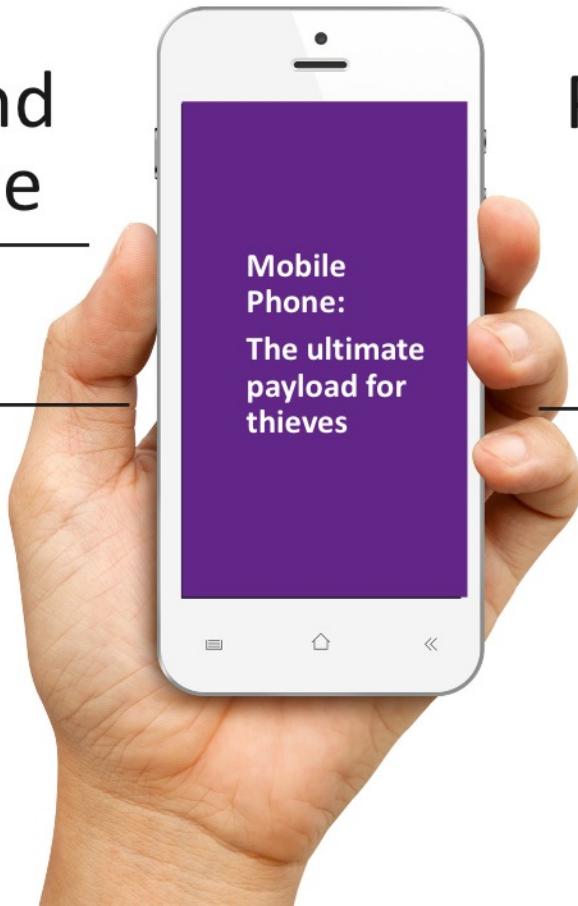
Mobile Phone: The ultimate payload for thieves

Access to personal info and personal finance

←

Access to company:
one click to
Oracle, SAP, VPNs

←



Private info:
pictures,
messages,
contacts

→



REPACKAGING TRUSTED MOBILE APPS

Rewriting Apps: Evolution from Games to Banking

**ABUSE OF
“TRUSTED APP” ECOSYSTEM
IS DANGEROUS**

- Modifying internal or MDM approved apps by insiders
- MITM vector for government surveillance
- Unsuspected data leakage



REPACKAGING TRUSTED MOBILE APPS

Fake Banking Apps and RATs

CREDIT AGRICOLE
CREDIT ACRIGOLE

The case with Google Play and Credit Agricole



REPACKAGING TRUSTED MOBILE APPS

google.com

URL <https://play.google.com/store/apps/details?id=com.ZoPro.agr2>
 File Name com.ZoPro.agr2.apk
 Date 2014-02-01 07:25 p.m.
 Malware false

Tags Android, apk, Google, Play, Store, Credit agricole Mon Budget, com.ZoPro.agr2, finance, application

Application Description Le Crédit Agricole propose d'aider ses clients dans la maîtrise de leur budget. L'application vous permet de connaître la situation de vos comptes, de gérer votre budget, d'optimiser vos dépenses et planifier vos projets en toute liberté et en quelques secondes dans le mobile, dans un magasin ou sur la terrasse du 2019 un café. Fonctionnant aussi bien en mode connecté que déconnecté, cette application articule autour de sept grandes fonctions : accès à la liste de vos comptes, fonctionnement simple, association d'un revenu à un dépense, gestion des budgets, suivi des dépenses, gestion des projets et gestion des alertes.

ADDITIONAL INFORMATION

Updated	Size	Installs
January 25, 2016	46M	1,000,000 - 5,000,000
Current Version	Requires Android	Content Rating
8.0.1	2.3.3 and up	Everyone Learn more
Interactive Elements	Permissions	Report
Users interact	View details	Flag as inappropriate
Offered By	Developer	
CREDIT AGRICOLE TECHNOLOGIES ET SERVICES	Visit website	
Offered By	Email	MonBudget.CreditAgricole@ca-technologies.fr

Released Jan 12, 2014

Application Name Credit agricole Mon Budget

Application Version 1.1



REPACKAGING TRUSTED MOBILE APPS

google.com

URL <https://play.google.com/store/apps/details?id=com.ZoPro.agr2>

File Name com.ZoPro.agr2.apk

Date 2014-02-01 07:25 p.m.

Malware false

Tags Android, apk, Google, Play, Store, Credit agricole Mon Budget, com.ZoPro.agr2, finance, application

Application Description Le Crédit Agricole propose d'aider ses clients dans la maîtrise de leur budget.

L'application vous permet de connaître la situation de vos comptes, de gérer votre budget, d'optimiser vos dépenses et planifier vos projets en toute liberté et en quelques secondes dans le mobile, dans un magasin ou sur la terrasse du 2019un café.

Fonctionnant aussi bien en mode connecté que déconnecté, cette application articule autour de sept grandes fonctions :

Accéder à la liste de vos comptes.

Associer une dépense à venir, lui associer une phare.

Un simple clic ou faire des rapprochements simples.

Avec la fonctionnalité de gestion des ressources mensuelles.

Un système de suivi et de dépassement de budget.

Finis les mauvaises habitudes de dépense.

Mieux comprendre son comportement budgétaire.

Avec les tableaux de bord alliant dépenses et comptes.

Etre accompagné par le Crédit Agricole Mon Budget.

Offrir la possibilité de court/moyen terme (ex : vacances, cadeaux).

Permettre de gagner de l'argent que vous devez régler.

La gestion de budget implique.

C'est pourquoi au sein même de l'application il existe un service de conseil.

Le Relèvement du 2019identifiant.

Cette fonction est disponible.

Caisses régionales du Crédit Agricole.

Agences et les numéros du 2019urgence (opposition carte, assurances diverses) sont.

Accessibles en cas de besoin.

ADDITIONAL INFORMATION

Updated

January 25, 2016

Size

46M

Installs

1,000,000 - 5,000,000

Current Version

8.0.1

Requires Android

2.3.3 and up

Content Rating

Everyone

Learn more

Interactive Elements

Users Interact

Permissions

View details

Report

Flag as inappropriate

Offered By

CREDIT AGRICOLE TECHNOLOGIES ET SERVICES
SERVICES

Developer

Visit website
Email MonBudget.CreditAgricole@ca-technologies.fr

Released Jan 12, 2014

Application Name Credit agricole Mon Budget

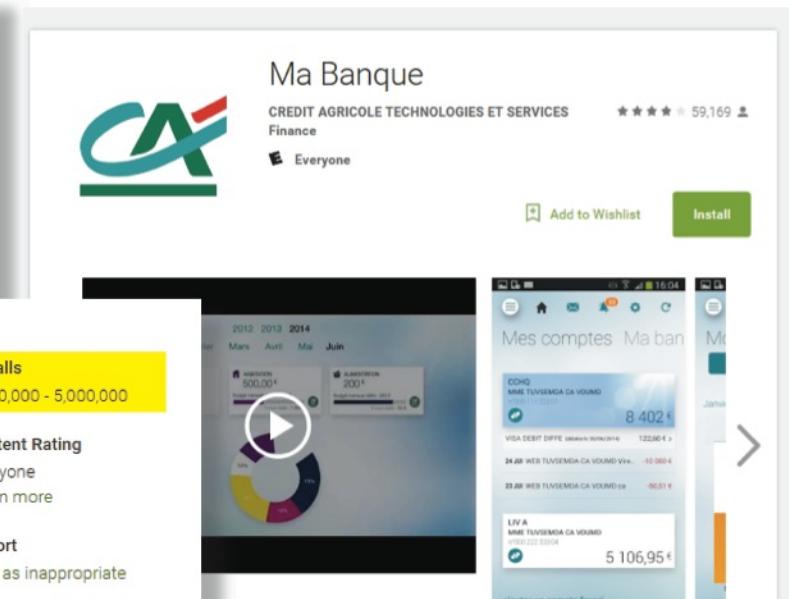
Application Version 1.1



REPACKAGING TRUSTED MOBILE APPS

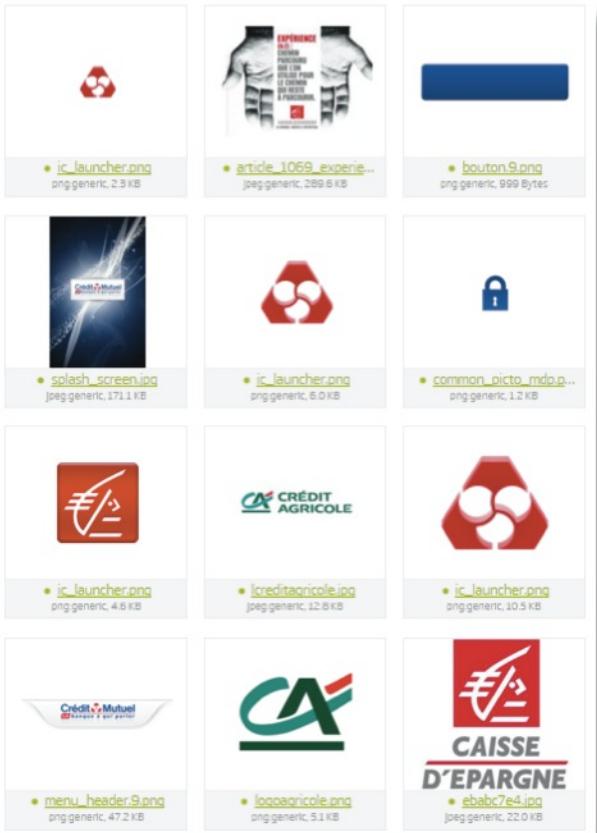
google.com

URL	https://play.google.com/store/apps/details?id=com.ZoPro.agr2
File Name	com.ZoPro.agr2.apk
Date	2014-02-01 07:25 p.m.
Malware	false
Tags	Android, apk, Google, Play, Store, Credit agricole Mon Budget, com.ZoPro.agr2, finance, application
Application Description	<p>Le Crédit Agricole propose d'aider ses clients dans la maîtrise de leur budget. L'application vous permet de connaître la situation de vos comptes, de gérer votre budget, d'optimiser vos dépenses et planifier vos projets en toute simplicité et en quelques secondes dans le confort, dans un magasin ou sur la terrasse du 2019un café.</p> <p>Fonctionnant aussi bien en mode connecté que déconnecté, cette application offre de nombreuses fonctionnalités :</p> <ul style="list-style-type: none"> Accéder à la liste de vos comptes. Effectuer un dépôt ou un retrait, lui associer une photo. Effectuer des rapprochements simples. Avec la fonctionnalité de suivi des dépenses mensuelles grâce à un système de classement de dépenses. Finir les mauvaises habitudes de dépenses. Mieux comprendre son comportement budgétaire. Utiliser les tableaux de bord alliant dépenses et revenus. Offrir la possibilité de faire des économies sur les achats moyens (ex : vacances, cadeaux). Offrir la gestion de budget impliquant plusieurs personnes au sein d'une famille. Obtenir pourquoi au sein d'une famille il existe des blocages de l'accès à l'application. Obtenir un relevé d'un mois d'activité identique à celui des agences régionales du Crédit Agricole et des numéros d'urgence (opposition carte, assurances diverses) sont également accessibles en cas de besoin.
Released	Jan 12, 2014
Application Name	Credit agricole Mon Budget
Application Version	1.1





REPACKAGING TRUSTED MOBILE APPS



Capabilities

- Address Book
- Advertising
- Bluetooth
- Calendar
- Calling Services
- Camera
- Device Identity
- Gaming
- Location Services
- Messaging
- Microphone
- Motion
- Networking
- NFC
- Notifications
- Social
- Storage
- System
- User Identity

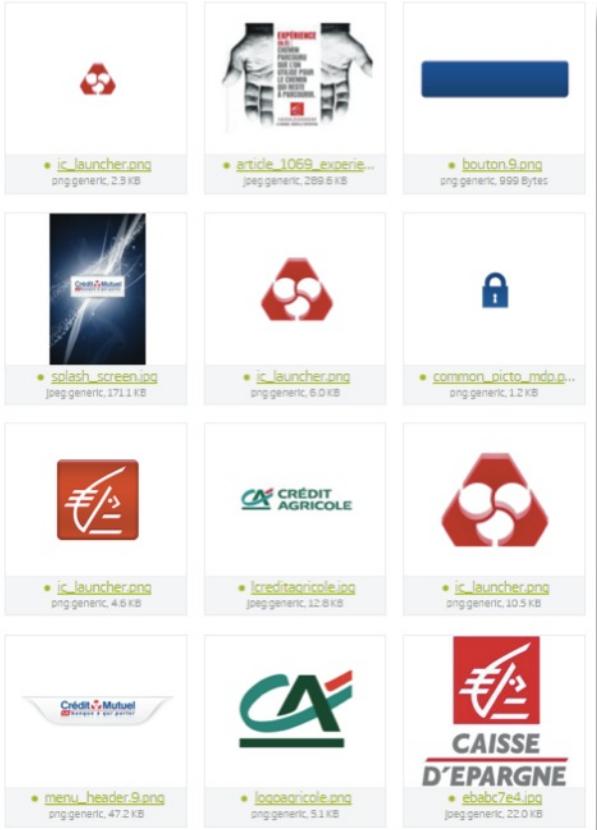


SIGNER: CREDIT ACRIGOL

Serial Number	1D643155
Issuer	Common Name
Version	1
Digest Algorithm	sha1
Digest Encryption	rsaEncryption
Encrypted Digest	1982D61B4C09FD5E28F6F17226F424F7B 415F1ECD76D20673FDCD005B8A40AF34D 9C6A5A17A2601C141600434B425E722A0 EC3F42F2EE9540BA38DAC7F9D0A21894D 362948F402E4915E8ACEF3991B739D5E0



REPACKAGING TRUSTED MOBILE APPS



Capabilities

Address Book
Advertising
Bluetooth
Calendar
Calling Services
Camera
Device Identity
Gaming
Location Services
Messaging
Microphone
Motion
Networking
NFC
Notifications
Social
Storage
System
User Identity



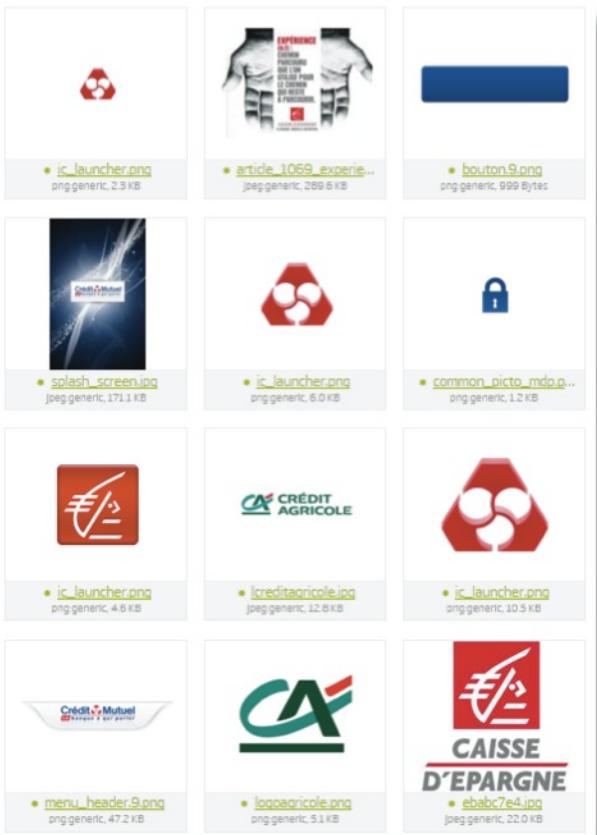
Google Play

SIGNER: CREDIT AGRICOLE

Serial Number	1D643155
Issuer	Common Name
Version	1
Digest Algorithm	sha1
Digest Encryption	rsaEncryption
Encrypted Digest	1982D61B4C09FD5E28F6F17226F424F7B 415F1ECD76D20673FDCD005B8A40AF34D 9C6A5A17A2601C141600434B425E722A0 EC3F42F2EE9540BA38DAC7F9D0A21894D 362948F402E4915E8ACEF3991B739D5E0



REPACKAGING TRUSTED MOBILE APPS



Capabilities

Address Book
Advertising
Bluetooth
Calendar
Calling Services
Camera
Device Identity
Gaming
Location Services
Messaging
Microphone
Motion
Networking
Notifications
Social
Storage
System
User Identity



SIGNER: CREDIT AGRICOL

Serial Number	11549155
Issuer	Common Name
Version	1
Digest Algorithm	sha1
Digest Encryption	rsaEncryption
Encrypted Digest	1982D61B4C09FD5E28F6F17226F424F7B 415F1ECD76D20673FDCD005B8A40AF34D 9C6A5A17A2601C141600434B425E722A0
	EC3F42F2EE9540BA38DAC7F9D0A21894D 362948F402E4915E8ACEF3991B739D5E0



REPACKAGING TRUSTED MOBILE APPS

Caisse_d_Epargne_Mobile.apk

Size: 65.9 KB

Format: binary / archive

Identification: android:generic

Threat: • Android.Trojan.Androrat

Severity: *****

Do you want to install an update to this existing application? Your existing data will not be lost. The updated application will get access to:

New

All

Privacy

- approximate location (network-based)
- precise location (GPS and network-based)

- modify or delete the contents of your SD card
- read the contents of your SD card

Device Access

- full network access
- view network connections

Cancel

Install



SIGNER: ANDROID DEBUG

Serial Number 30FC3EFO

Issuer Country Name US

Organization Name Android

Common Name Android Debug

Version 1

Digest Algorithm sha1

Digest Encryption... rsaEncryption

Capabilities

Address Book

Advertising

Bluetooth

Calendar

Calling Services

Camera

Device Identity

Gaming

Location Services

Messaging

Microphone

Motion

Networking

NFC

Notifications

Social

Storage

System

User Identity



REPACKAGING TRUSTED MOBILE APPS

Caisse_d_Epargne_Mobile.apk

Size: 65.9 KB

Format: binary / archive

Identification: android:generic

Threat: • Android.Trojan.Androrat

Severity: *****

Do you want to install an update to this existing application? Your existing data will not be lost. The updated application will get access to:

New

All

Privacy

- approximate location (network-based)
- precise location (GPS and network-based)
- modify or delete the contents of your SD card
- read the contents of your SD card

Device Access

- full network access
- view network connections

Cancel

Install



SIGNER: ANDROID DEBUG		
Serial Number	30FC3EFO	
Issuer	Country Name	US
	Organization Name	Android
	Common Name	Android Debug
Version	1	
Digest Algorithm	sha1	
Digest Encryption	rsaEncryption	

Capabilities

Address Book

Advertising

Bluetooth

Calendar

Calling Services

Camera

Device Identity

Gaming

Location Services

Messaging

Microphone

Motion

Networking

NFC

Notifications

Social

Storage

System

User Identity



REPACKAGING TRUSTED MOBILE APPS

Caisse_d_Epargne_Mobile.apk

Size: 65.9 KB

Format: binary / archive

Identification: android:generic

Threat: • Android.Trojan.Androrat

Severity: *****

Do you want to install an update to this existing application? Your existing data will not be lost. The updated application will get access to:

New

All

Privacy

- approximate location (network-based)
- precise location (GPS and network-based)

- modify or delete the contents of your SD card
- read the contents of your SD card

Device Access

- full network access
- view network connections

Cancel

Install



SIGNER: ANDROID DEBUG	
Serial Number	30F0-7FO
Issuer	Country Name: US
	Organization Name: Android
	Common Name: Android Debug
Version	1
Digest Algorithm	sha1
Digest Encryption	rsaEncryption

Capabilities

Address Book

Advertising

Bluetooth

Calendar

Calling Services

Camera

Device Identity

Gaming

Location Services

Messaging

Microphone

Motion

Networking

NFC

Notifications

Social

Storage

System

User Identity

Open Source Vulnerabilities in IoT



If you want
to steal a car,

you'll hack
keyless entry



HARD

reverse the hardware



EASY

use open source
vulnerability exploits



OPEN SOURCE VULNERABILITIES IN IOT

IOT IS LARGELY BASED ON ANDROID & LINUX

Vulnerability disclosure
in open source outpaces vendor specific
vulnerabilities

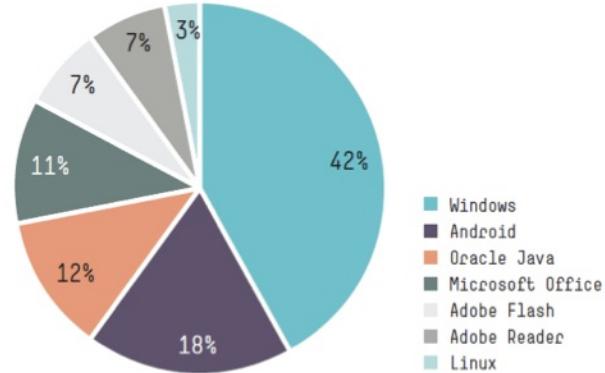


Figure 15. Top 20 discovered exploit samples by targeted platform

Vulnerabilities in
Third Party libraries
on the rise

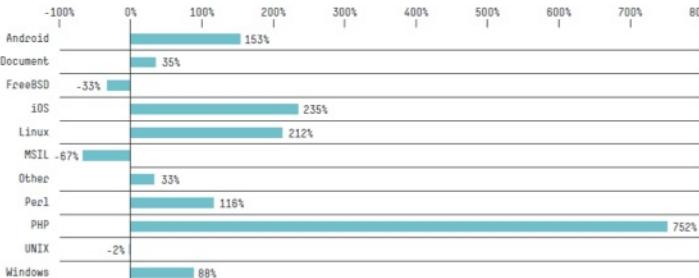


Figure 20. Yearly growth in newly discovered malware samples by platform (ReversingLabs)



OPEN SOURCE VULNERABILITIES IN IOT

Software is increasingly being built on top of open source components

Third party stacks and libraries are essential

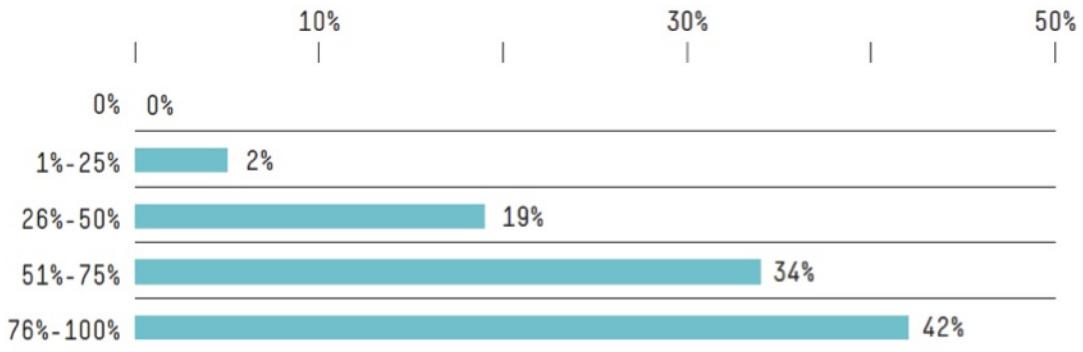


Figure 55. The percentage of open source components in applications new to the dataset in 2015



OPEN SOURCE VULNERABILITIES IN IOT

Software is increasingly being built on top of open source components

Third party stacks and libraries are essential



Figure 55. The percentage of open source components in applications new to the dataset in 2015



OPEN SOURCE VULNERABILITIES IN IOT

ALLEGED OPEN SOURCE RISK:

- Predator Drone Crash Attempt by AnonSec
- Gozi Infection → NASA → Open Source Vulns for Lateral Movement
- 24 hour/7 monitoring → multiple lines of control

THIRD PARTY RISK:

- iOS: xCodeGhost
- Android: Flurry/SSL



OPEN SOURCE VULNERABILITIES IN IOT

IOT SECURITY WILL HAVE CONSEQUENCES

Who will be responsible for patching common open source/third party libraries in your custom applications?

Is IoT going to bring the end of Software Licensing as we know it?



Lessons

of Greatest Consequence
Heading into 2016





- [BEC]**
- Lock down email policies and financial oversight
 - Request dual signatures



- [Ransomware]**
- Institute critical document backup
 - Institute backup & restore functions for critical applications and databases
 - Test re-imagining and restorations for critical systems

**[Repackaging
Trusted Mobile
Applications]**

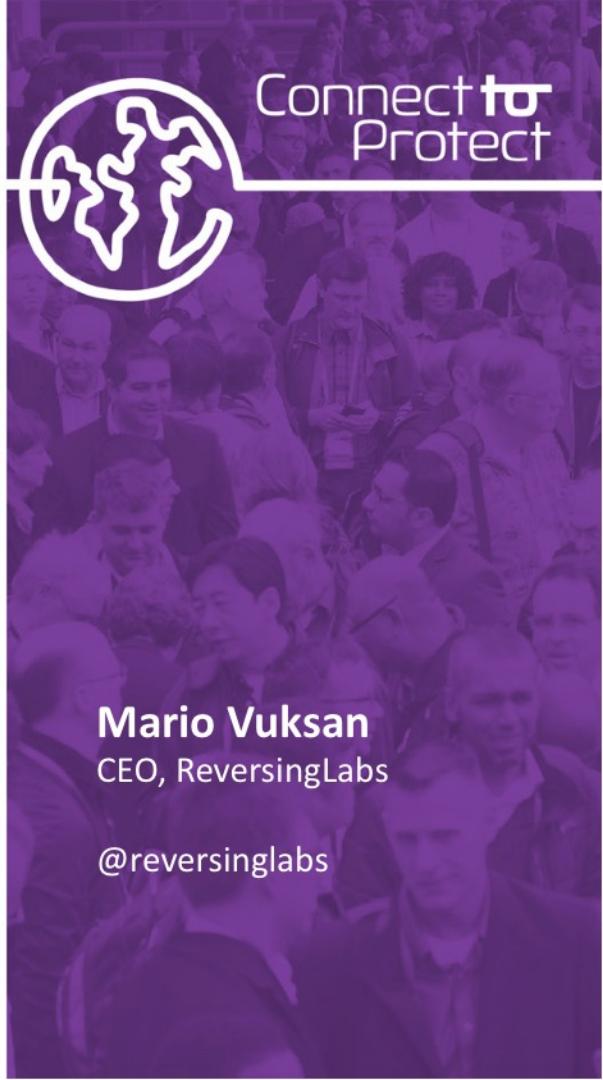
- MDM: whitelist reputable software vendors
- Demand better author reputation from App Store and Google Play

- [IoT]**
- Inventory open source and third party libraries
 - Push vendors to continually upgrade vulnerable third party libs
 - Require that IoT devices are patchable and can be re-imaged

RSA® Conference 2016

San Francisco | February 29–March 4 | Moscone Center

Thank you!



Mario Vuksan
CEO, ReversingLabs

@reversinglabs