RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

Threats of Greatest Consequence Heading into 2016

Mario Vuksan
CEO, ReversingLabs

@reversinglabs

#RSA
C

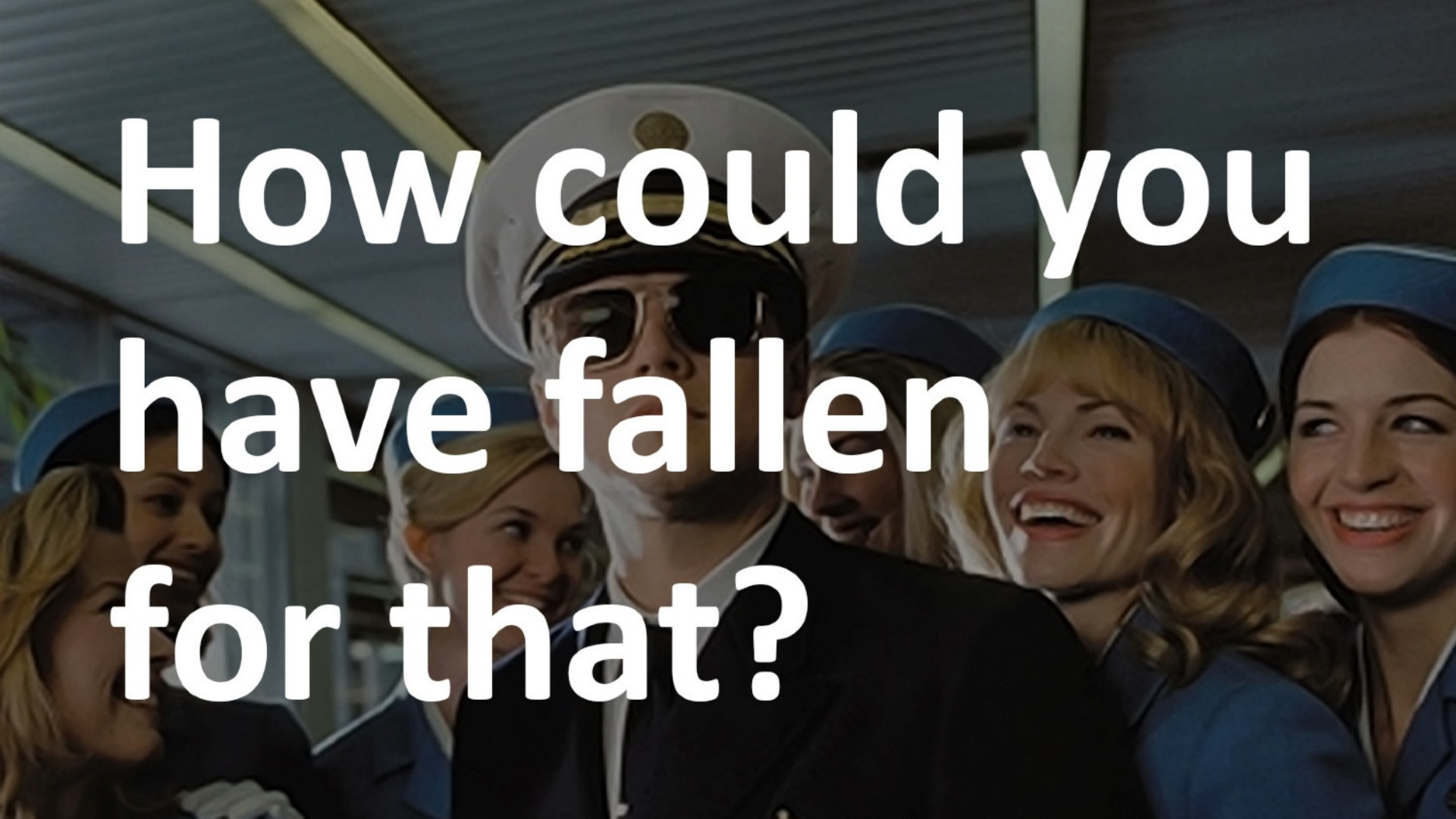
Stories of Greatest Consequence

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

BEC

(Business Email Compromise)


I am your CEO. Send money ASAP!


How could you
have fallen
for that?

BEC

EFFECT

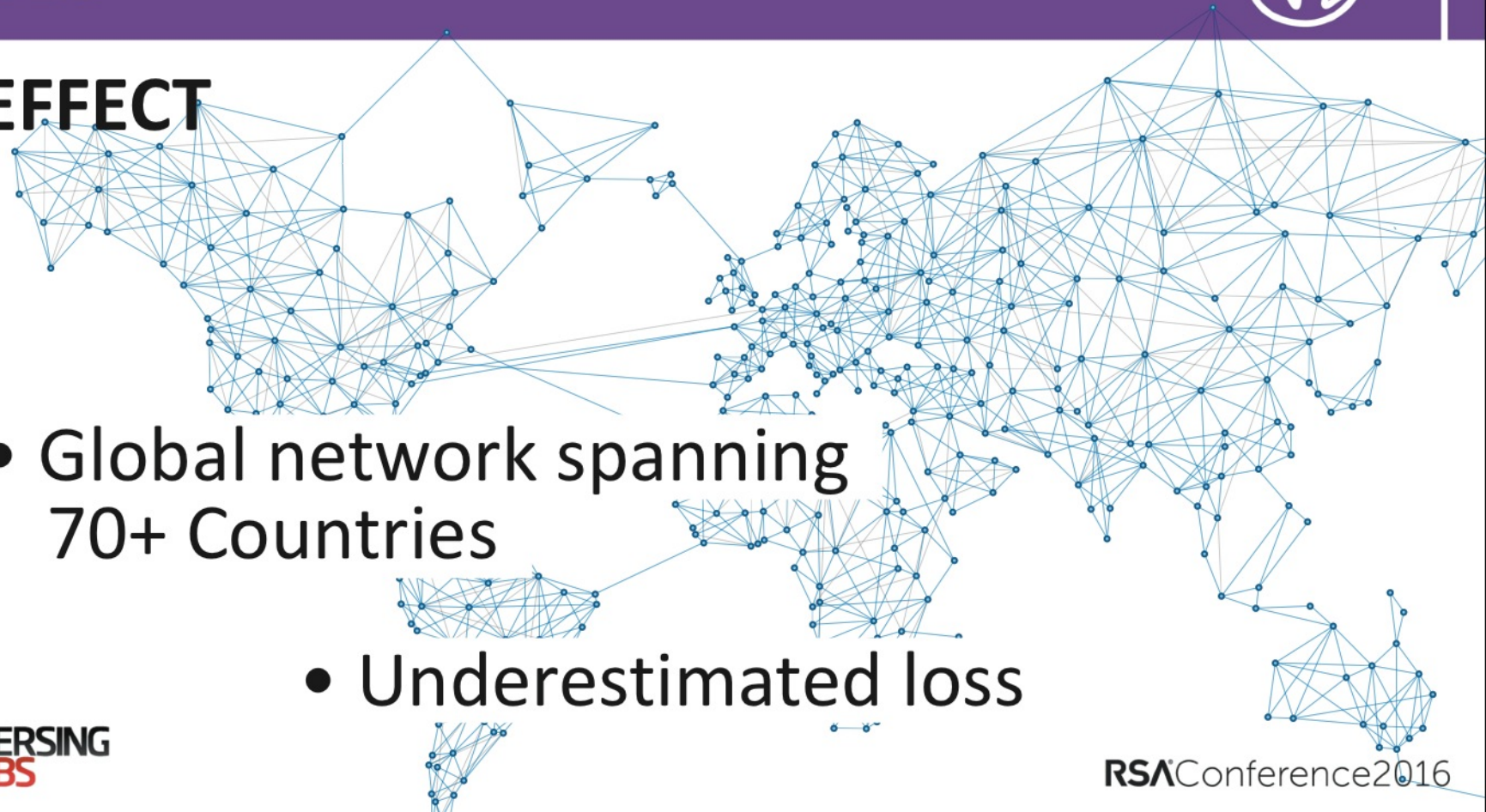
BEC

EFFECT

- Underestimated loss

BEC

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

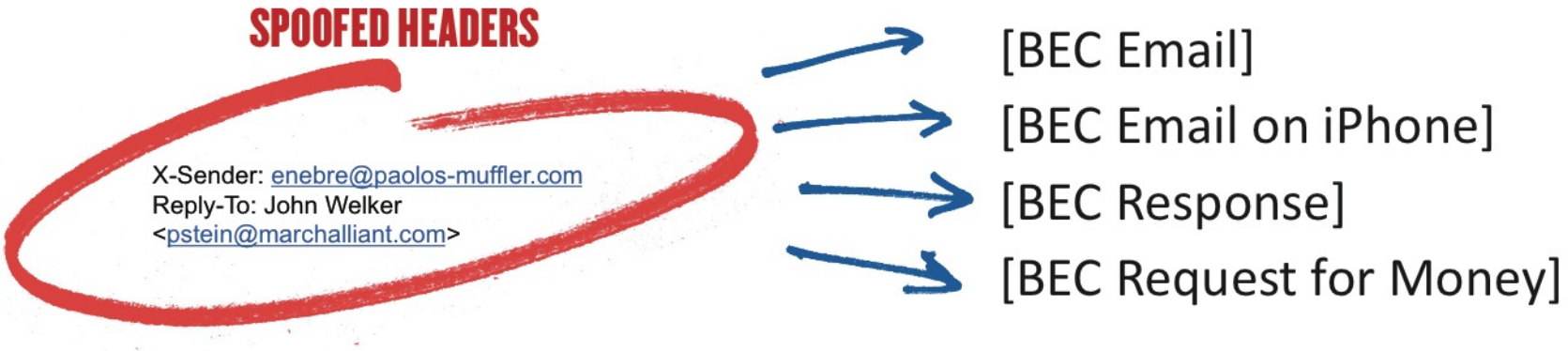
- Underestimated loss

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 financial laundromat

or

Shell 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

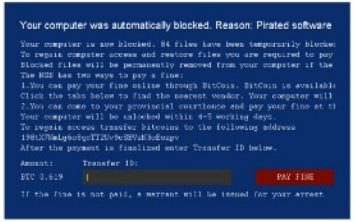
- Underfunded; ransom is cheaper than security program
- Cash strapped: shut it down and great financial loss can happen
- Serve the public: what all can go wrong if patients are not taken care of
- Equipment that can be serviced only by manufacturers
- Can’t add AV or other tools, can’t patch them

EVOLVING RANSOMWARE

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

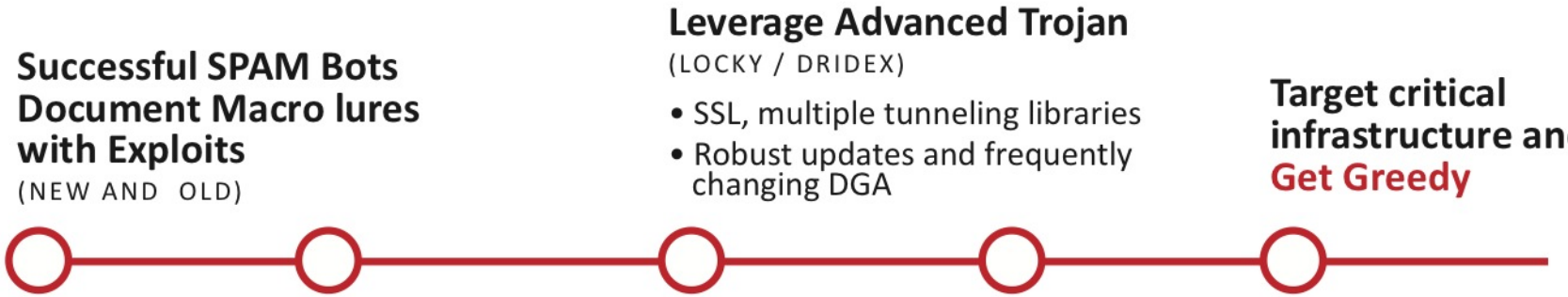
Use of non-performing over-harvested Botnet accounts

Operate full Stack Service



EVOLVING RANSOMWARE

EVOLVED PROCEDURE



EVOLVING RANSOMWARE

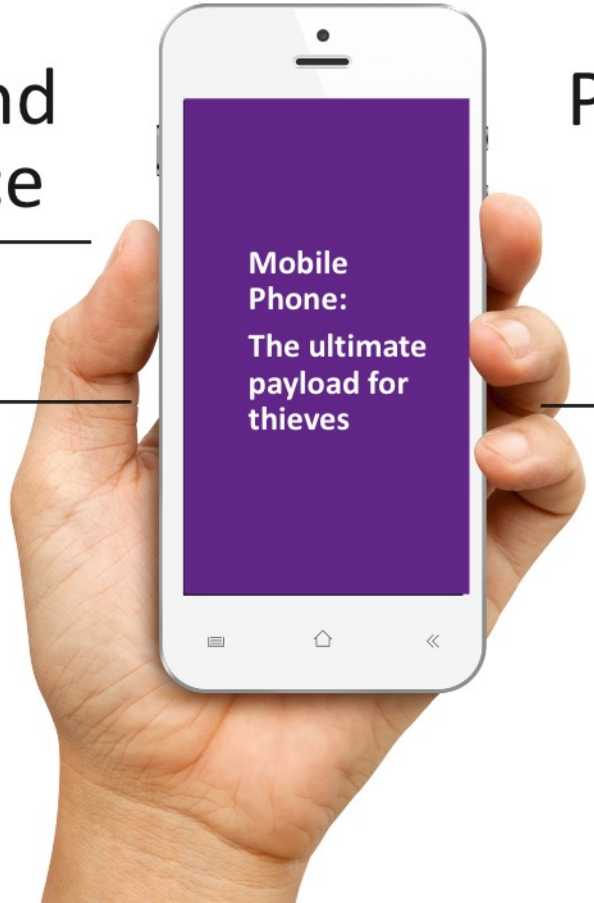
DEFENSE

- 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?

Repackaging — Trusted — Mobile Apps


Mobile Phone:
The ultimate payload for thieves

Access to personal info and personal finance

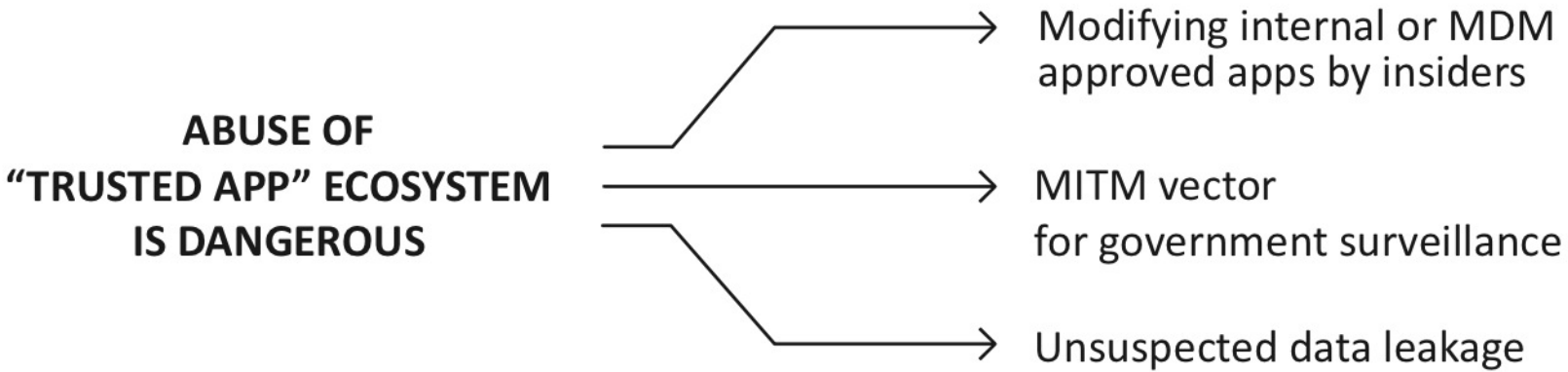


Private info: pictures, messages, contacts

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

REPACKAGING TRUSTED MOBILE APPS

Repacking Apps: Evolution from Games to Banking



Fake Banking Apps and RATs

CREDIT AGRICOLE
CREDIT ACRIGOLE

The case with Google Play and Credit Agricole

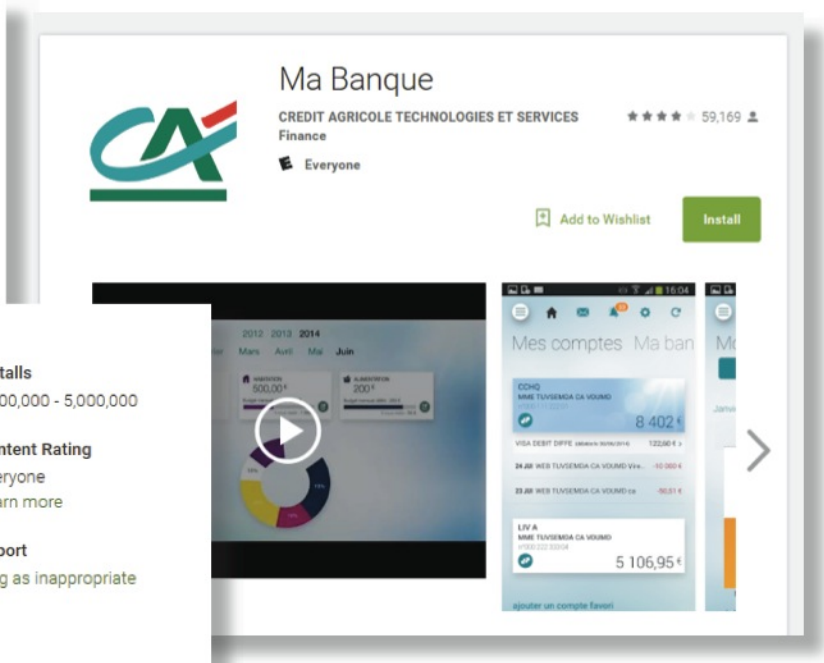
REPACKAGING TRUSTED MOBILE APPS

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 Descri...	Le Cr\xe9dit Agricole propose d\u2019accompagner ses clients dans la ma\xeetrise de leur budget. L\u2019application \xab mon budget \xbb vous permet de conna\xeetre la situation de vos comptes, de g\xe9rer votre budget, d\u2019optimiser vos d\xe9penses et planifier vos projets en toute libert\xe9 et en quelques secondes dans le m\xe9tro, dans un magasin ou \xe0 la terrasse d\u2019un caf\xe9. <p>Fonctionnant aussi bien en mode connect\xe9 que d\xe9connect\xe9, cette application s\u2019articule autour de sept grandes fonctions :<p>\u2... acc\xe9der \xe0 la vue de vos comptes. Vo... d\xe9pense \xe0 venir, lui associer une pho... d\u2019un simple clic ou faire des rapproch... tr\xe8s simple.<p>\u2022 Avec la fonctior... ressources mensuelles gr\xe2ce \xe0 un sy... d\xe9passement de budget. Fini les mauva... de mieux comprendre votre comportement ... vos budgets moyens. Cette fonction vous p... \xe9volution. Avec les tableaux de bord alli... comptes.<p>\u2022 Etre accompagn\xe9 ... \xab Mon budget \xbb vous offre la possibil... court/moyen terme (ex : vacances, cadeaux ... d\u2019\xe9pargne que vous devez r\xe9... <p>\u2022 La gestion de budget implique ... C\u2019est pourquoi au sein m\xeame de l ... d\xe9blocages de r\xe9serve de cr\xe9dit ... d\u2019un Relev\xe9 d\u2019Identit\xe9 ... d\u2019\u0153il. Cette fonction est dispor... caisses r\xe9gionales du Credit Agricole ay... d\u2019agences et les num\xe9ros d\u201... urgence (opposition carte, assurances diverses) sont \xe9galement accessibles en cas de besoin.
Released	Jan 12, 2014
Application Name	Credit agricole Mon Budget
Application Version	1.1

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 Email MonBudget.CreditAgricole@ca-technologies.fr	



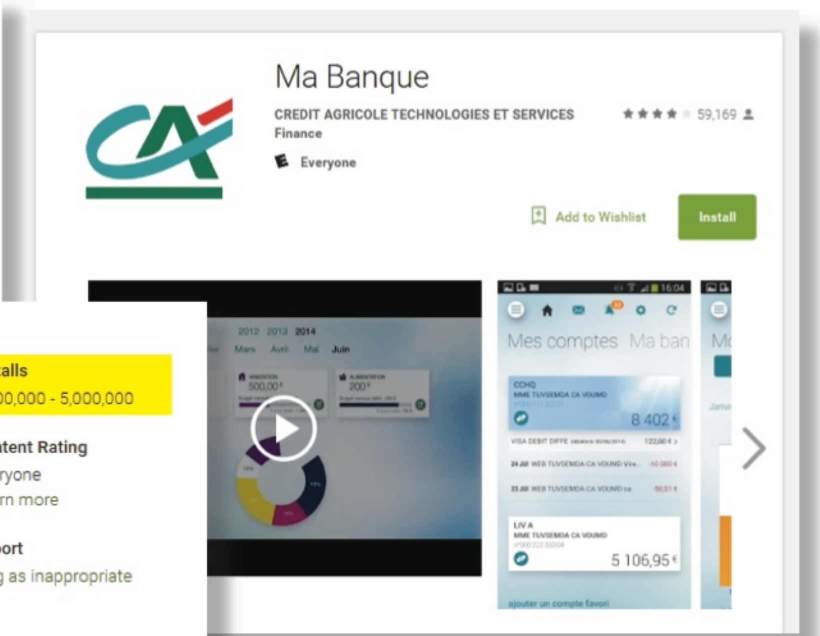
REPACKAGING TRUSTED MOBILE APPS

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 Descri...	Le Cr\xe9dit Agricole propose d\u2019accompagner ses clients dans la ma\xeetrise de leur budget. L\u2019application \xab mon budget \xbb vous permet de conna\xeetre la situation de vos comptes, de g\xe9rer votre budget, d\u2019optimiser vos d\xe9penses et planifier vos projets en toute libert\xe9 et en quelques secondes dans le m\xe9tro, dans un magasin ou \xe0 la terrasse d\u2019un caf\xe9. <p>Fonctionnant aussi bien en mode connect\xe9 que d\xe9connect\xe9, cette application s\u2019articule autour de sept grandes fonctions : <p>\u20 ... acc\xe9der \xe0 la vue de vos comptes. Vo ... d\xe9pense \xe0 venir, lui associer une pho ... d\u2019un simple clic ou faire des rapproch ... tr\xe8s simple. <p>\u2022 Avec la fonction ... ressources mensuelles gr\xe2ce \xe0 un sy ... d\xe9passement de budget. Fini les mauva ... de mieux comprendre votre comportement ... vos budgets moyens. Cette fonction vous p ... \xe9volution. Avec les tableaux de bord allia ... comptes. <p>\u2022 Etre accompagn\xe9 ... \xab Mon budget \xbb vous offre la possibil ... court/moyen terme (ex : vacances, cadeaux ... d\u2019\xe9pargne que vous devez r\xe9 ... <p>\u2022 La gestion de budget implique ... C\u2019est pourquoi au sein m\xeame de l ... d\xe9blocages de r\xe9serve de cr\xe9dit ... d\u2019un Relev\xe9 d\u2019Identit\xe9 ... d\u2019\u0153il. Cette fonction est dispo ... caisses r\xe9gionales du Credit Agricole aya ... d\u2019agences et les num\xe9ros d\u201 ... urgence (opposition carte, assurances diverses) sont \xe9galement accessibles en cas de besoin.
Released	Jan 12, 2014
Application Name	Credit agricole Mon Budget
Application Version	1.1

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



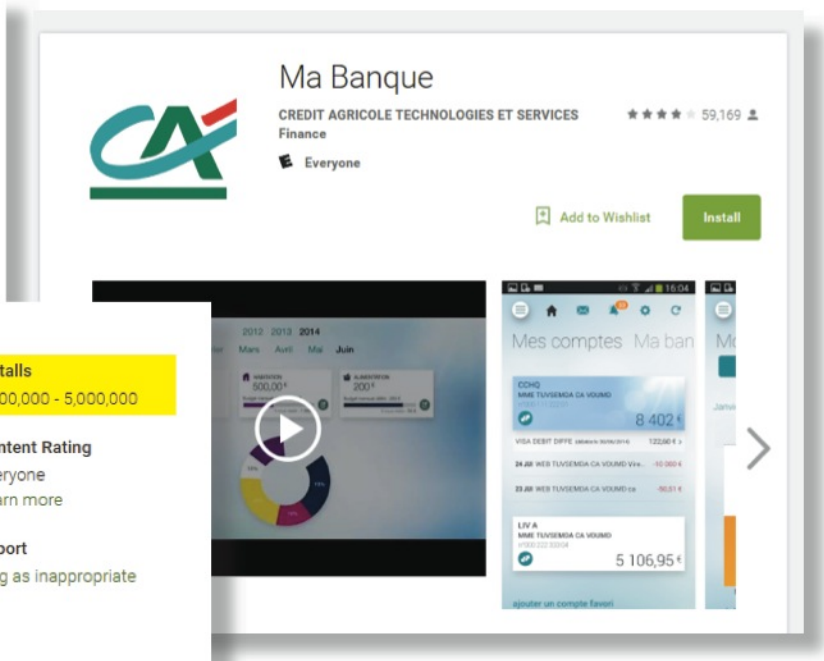
REPACKAGING TRUSTED MOBILE APPS

google.com

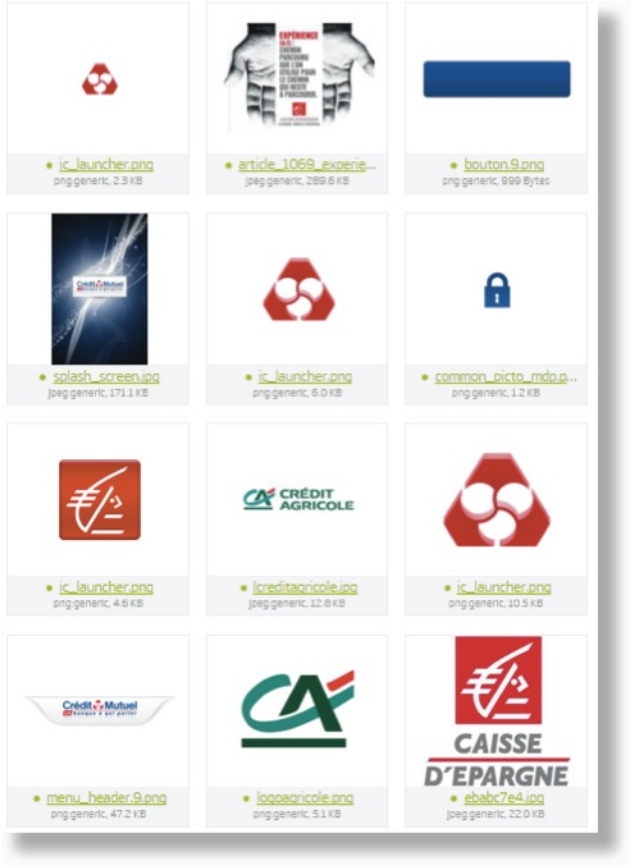
URL	https://play.google.com/store/apps/details?id=com.ZoPro.agr2
File Name	com.ZoPro.agr2.apk
Date	2014-02-01 07:25 p.m.
Malware	false
Tags	Android, .apk, Google, Play, Store, Credit agricole Mon Budget, com.ZoPro.agr2, fin...ce, application
Application Descri...	Le Cr\xe9dit Agricole propose d\u2019accompagner ses clients dans la ma\xeetrise de...ur budget. L\u2019application \xab mon budget \xbb vous permet de conna\xeetre la situation de vos comptes, de g\xe9rer votre budget, d\u2019optimiser vos d\xe9penses et planifier vos projets en toute l...t\xe9 et en quelques secondes dans le m\xe9tro, dans un magasin ou \xe0 la terrasse d\u2019un caf\xe9. <p>Fonctionnant aussi bien en mode connect\xe9 que d\xe9connect\xe9, cette application s\u201...ticule autour de sept grandes fonctions :<p>\u2... acc\xe9der \xe0 la vue de vos comptes. Vo... d\xe9pense \xe0 venir, lui associer une pho... d\u2019un simple clic ou faire des rapproch... tr\xe8s simple.<p>\u2022 Avec la fonctio... ressources mensuelles gr\xe2ce \xe0 un sy... d\xe9passement de budget. Fini les mauva... de mieux comprendre votre comportement ... vos budgets moyens. Cette fonction vous p... \xe9volution. Avec les tableaux de bord alli... comptes.<p>\u2022 Etre accompagn\xe9 ... \xab Mon budget \xbb vous offre la possibil... court/moyen terme (ex : vacances, cadeaux ... d\u2019\xe9pargne que vous devez r\xe9... <p>\u2022 La gestion de budget implique ... C\u2019est pourquoi au sein m\xeame de l... d\xe9blocages de r\xe9serve de cr\xe9dit ... d\u2019un Relev\xe9 d\u2019Identit\xe9 ... d\u2019\u0153il. Cette fonction est dispo... caisses r\xe9gionales du Credit Agricole ay... d\u2019agences et les num\xe9ros d\u201...urgence (opposition carte, assurances diverses) sont \xe9galement accessibles en cas de besoin.
Released	Jan 12, 2014
Application Name	Credit agricole Mon Budget
Application Version	1.1

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 Email MonBudget.CreditAgricole@ca-technologies.fr	



REPACKAGING TRUSTED MOBILE APPS



Capabilities

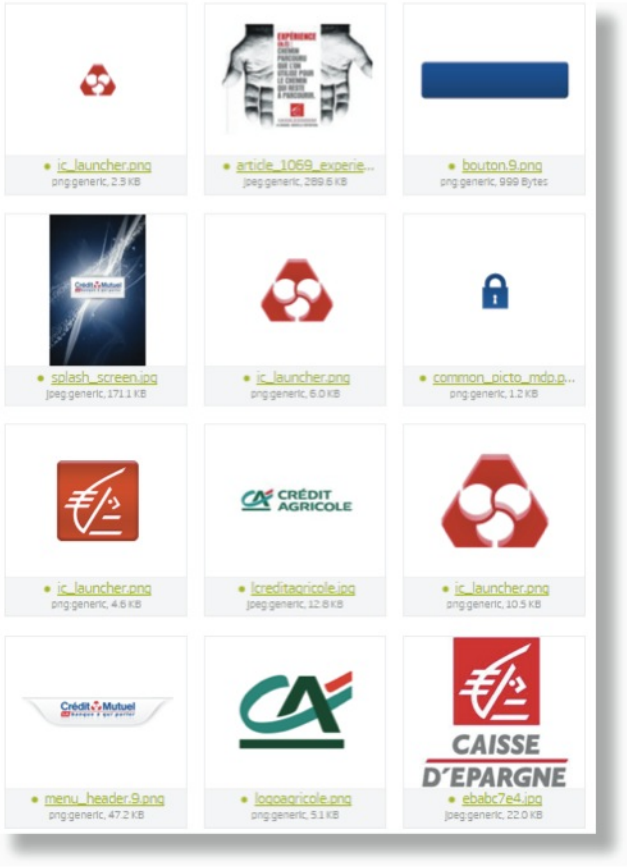
- Address Book
- Advertising
- Bluetooth
- Calendar
- Calling Services
- Camera
- Device Identity
- Gaming
- Location Services
- Messaging
- Microphone
- Motion
- Networking
- NFC
- Notifications
- Social
- Storage
- System
- User Identity

Google Play

SIGNER: CREDIT ACRIGOL

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

REPACKAGING TRUSTED MOBILE APPS



Capabilities

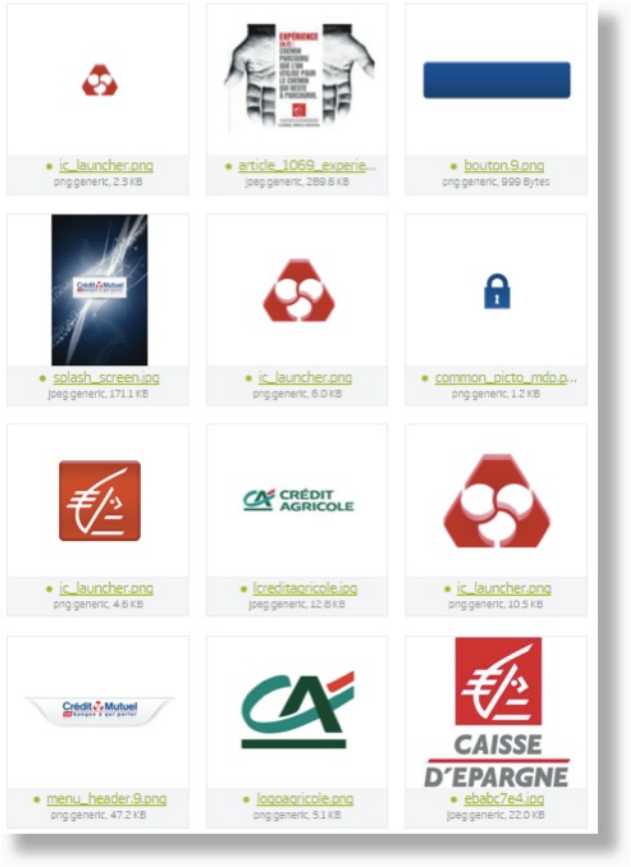
- Address Book
- Advertising
- Bluetooth
- Calendar
- Calling Services
- Camera
- Device Identity
- Gaming
- Location Services
- Messaging
- Microphone
- Motion
- Networking
- NFC
- Notifications
- Social
- Storage
- System
- User Identity

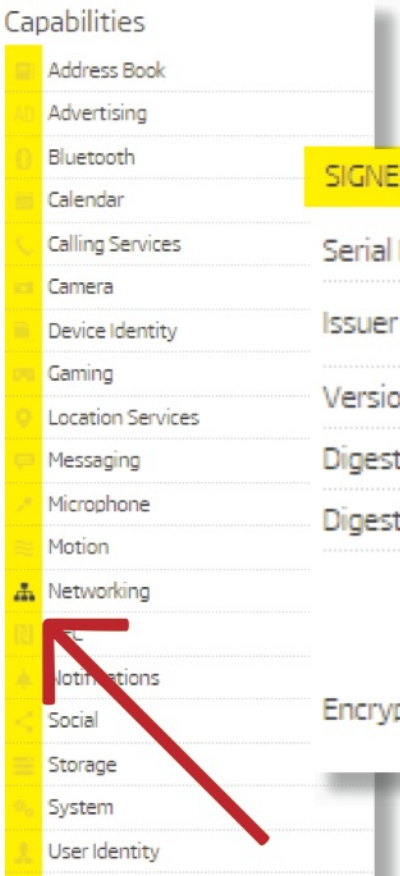
Google Play

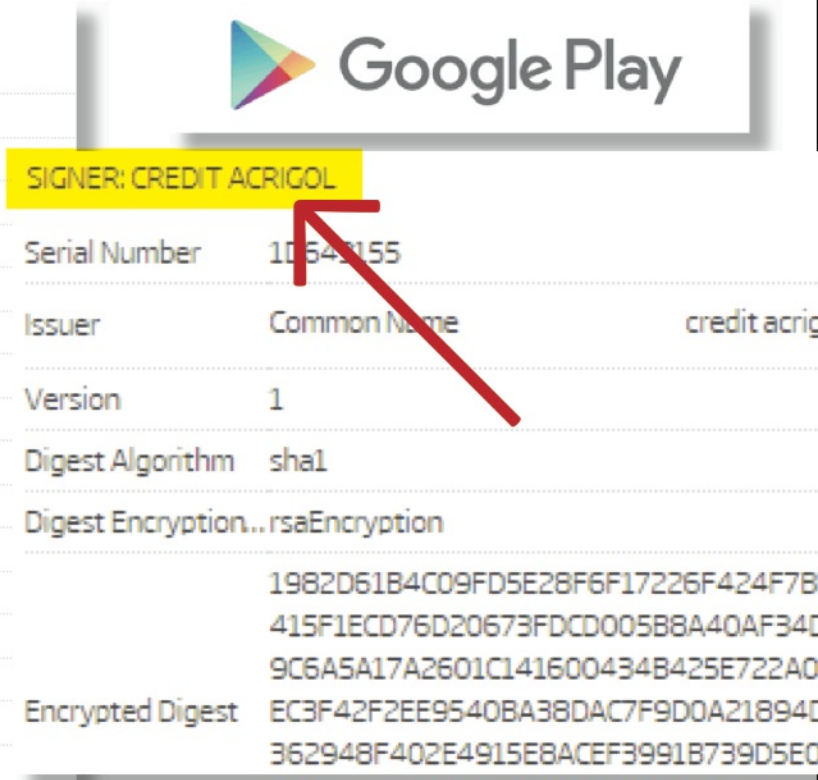
SIGNER: CREDIT ACRIGOL

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

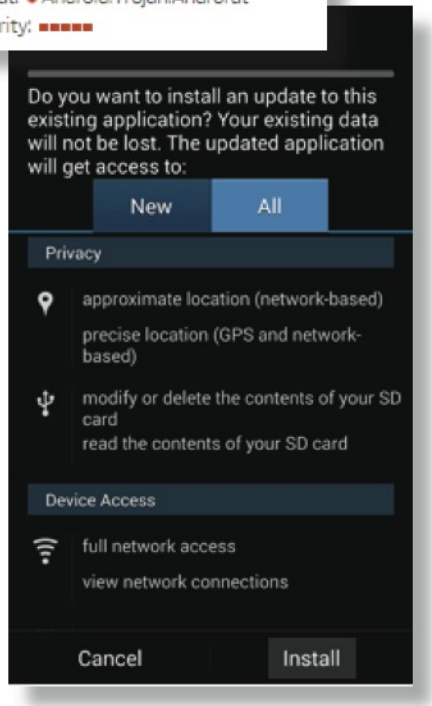
REPACKAGING TRUSTED MOBILE APPS

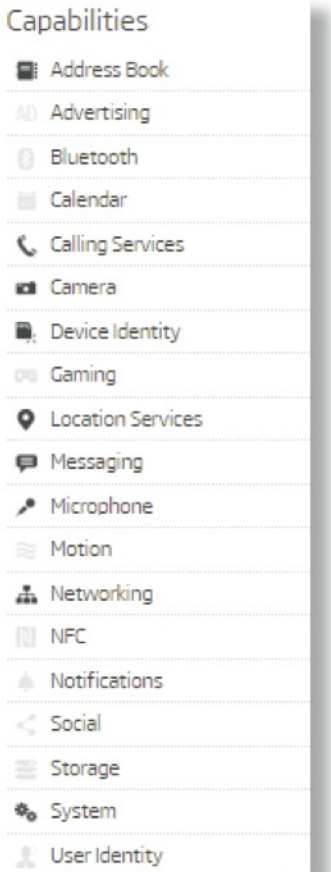




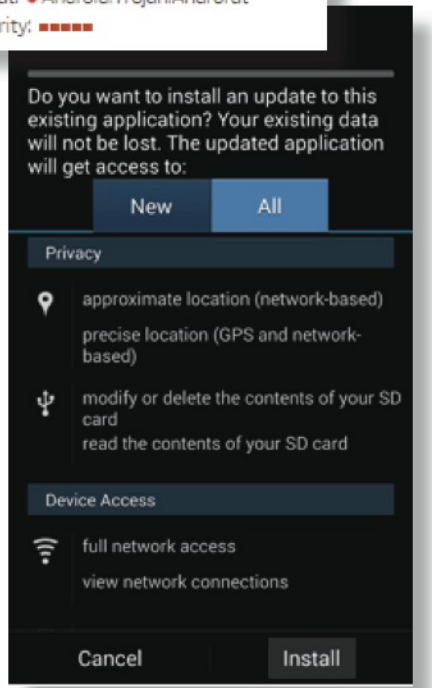


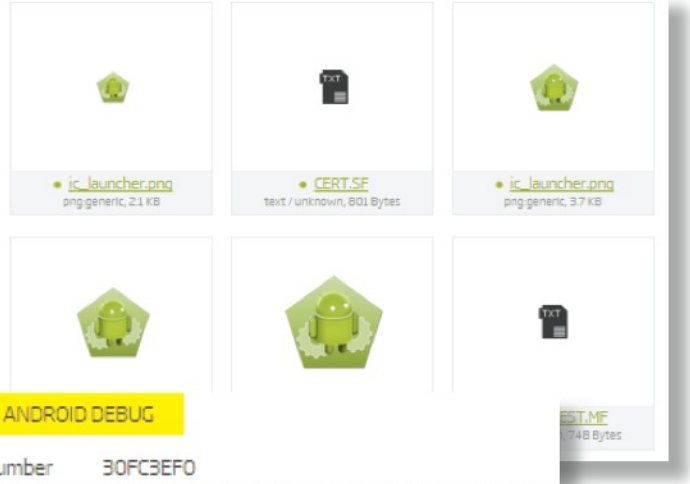
REPACKAGING TRUSTED MOBILE APPS

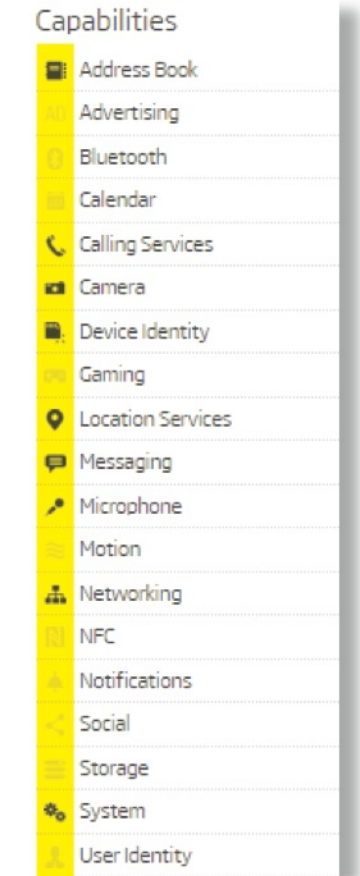




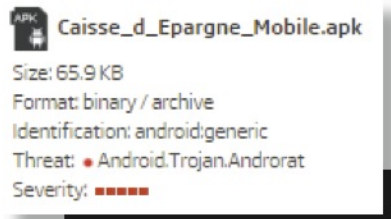
REPACKAGING TRUSTED MOBILE APPS

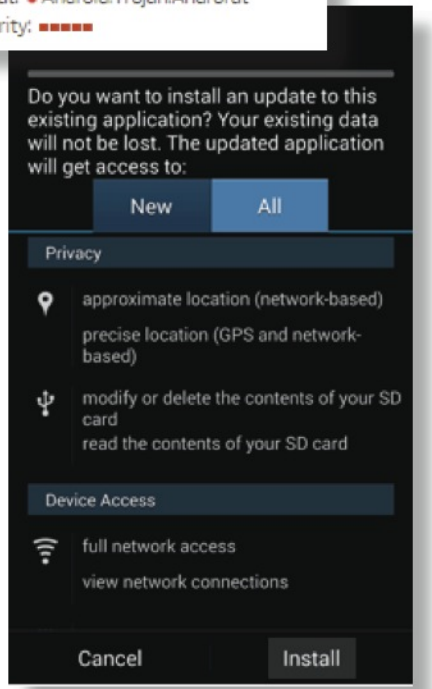


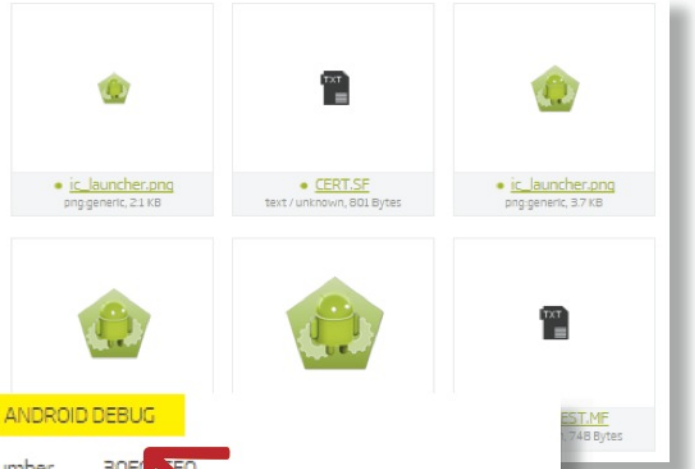


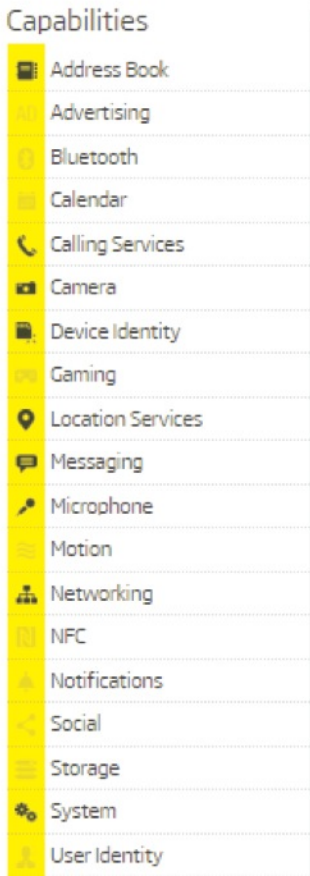


REPACKAGING TRUSTED MOBILE APPS









Open Source Vulnerabilites in IoT


If you want
to steal a car,
you'll hack
keyless entry

REVERSING LABS

RSAConference2016

REVERSING LABS

RSAConference2016

OPEN SOURCE VULNERABILITES IN IOT

IOT IS LARGELY BASED ON ANDROID & LINUX

Vulnerability disclosure
in open source outpaces vendor specific vulnerabilities

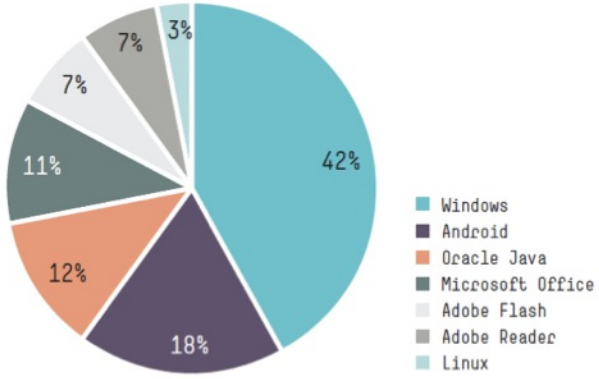


Figure 15. Top 20 discovered exploit samples by targeted platform

Vulnerabilities in
Third Party libraries
on the rise

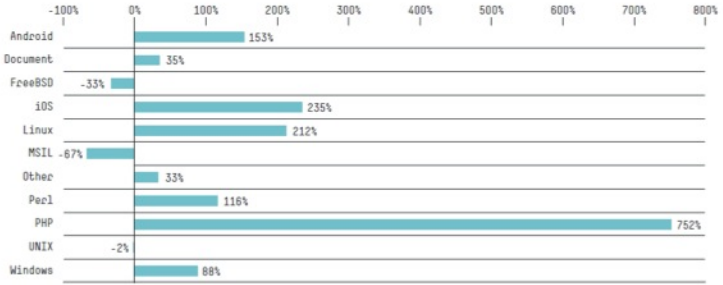


Figure 20. Yearly growth in newly discovered malware samples by platform (ReversingLabs)

REVERSING LABS

OPEN SOURCE VULNERABILITES IN IOT

Software is increasingly being built on top of open source components

Third party stacks and libraries are essential

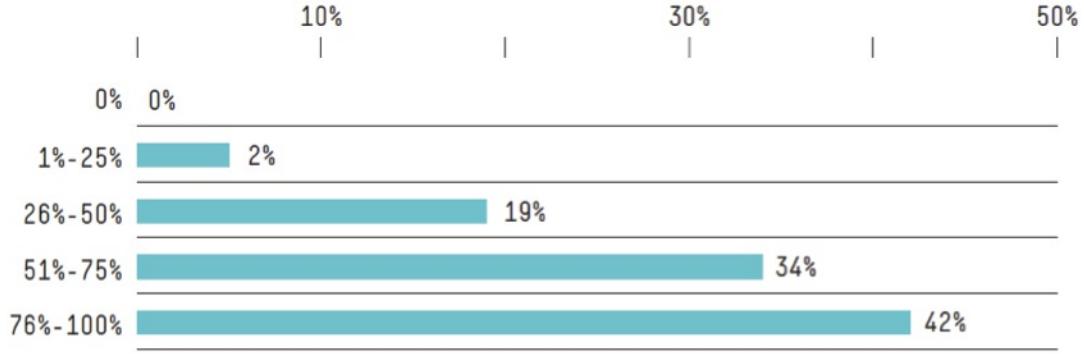


Figure 55. The percentage of open source components in applications new to the dataset in 2015

OPEN SOURCE VULNERABILITES 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 VULNERABILITES 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 VULNERABILITES 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?

RSAConference2016

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 Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

Thank you!

Mario Vuksan
CEO, ReversingLabs

@reversinglabs

#RSA
C