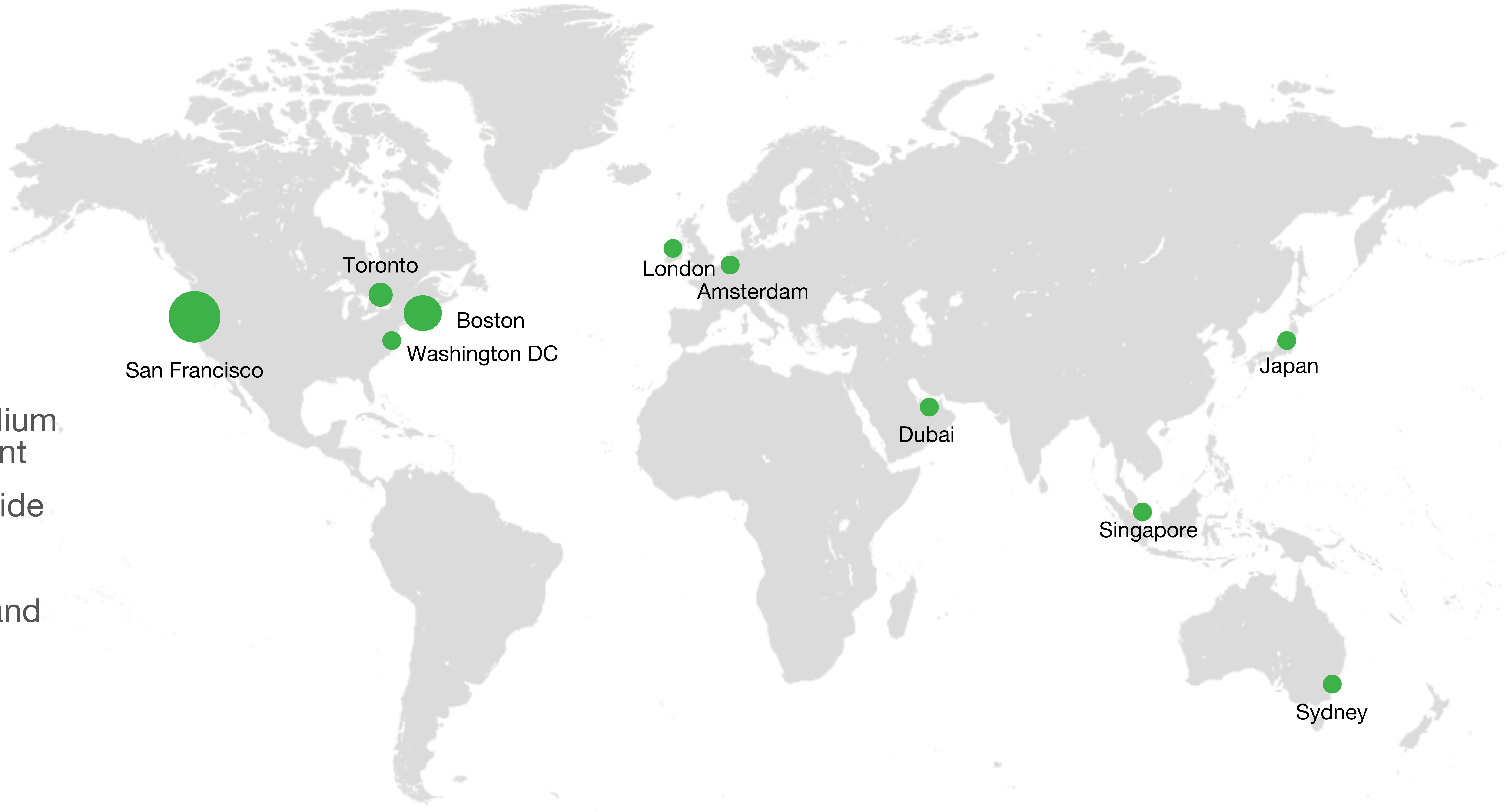
Lookout®

The State of Phishing and Apps

Lookout

- Founded in 2007
- Global presence with worldwide distribution and support
- Solutions for consumers, small-medium business, enterprise, and government
- We secure 500k businesses worldwide
- The only endpoint-to-cloud solution
- Including the largest organizations and highest levels of government



~200M
MOBILE DEVICES

140M+
APPS ANALYZED

4.5M+
DOMAIN REGISTRATIONS PROCESSED EVERY MONTH

MACHINE INTELLIGENCE

500+
PHISHING SITES/DAY

10K+
MALICIOUS APPS/DAY

Partnerships

Technology partners

Google

Microsoft

vmware

SentinelOne

Download on the App Store

BlackBerry

CiTRIX

IBM

ivanti

jamf

Carrier Partners

AT&T

vodafone

verizon

orange

NTT docomo

T · · Mobile ·

Telefónica

KDDI

Telstra

Channel Partners

TechData

IVALUE Maximizing Value of Technology Investments

carahsoft.

BYTES

NEXTGEN

GUIDEPOINT SECURITY

CTC Challenging Tomorrow's Changes

shi

OPTIV

softwareONE

CONEXIO 人をつなぐ、価値をつなぐ

SCC

FUJITSU

isec7 powered by innovation

Leading market innovation

1st

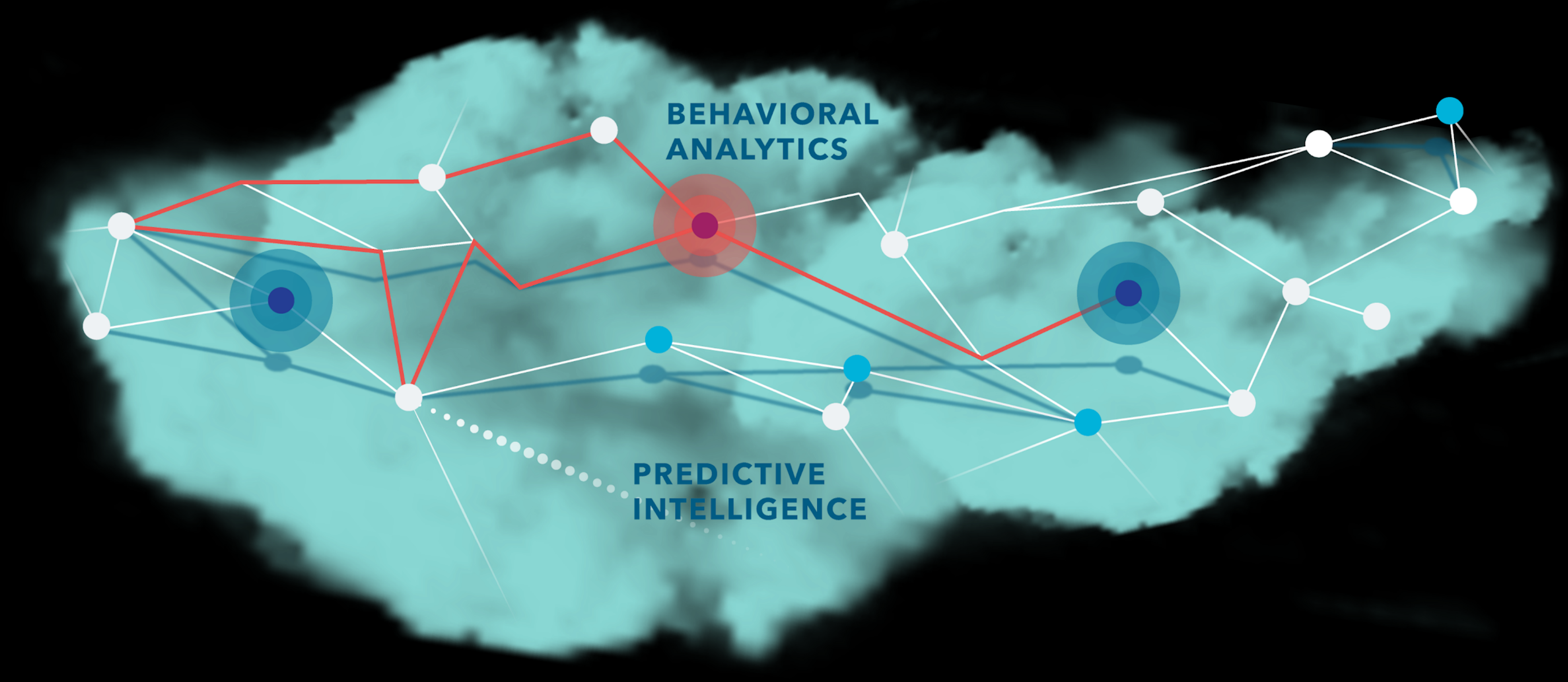
- Enterprise mobile security product
- Endpoint-to-cloud solution incl CASB and ZTNA
- Mobile phishing protection solution
- To support Zero Trust for Google and Microsoft
  - Integration with Microsoft Intune
  - Mobile security for Google BeyondCorp
- EDR built for mobile

Leveraging the largest dataset

~200M
Devices

140M+
Apps

4.5M+
Domains per month

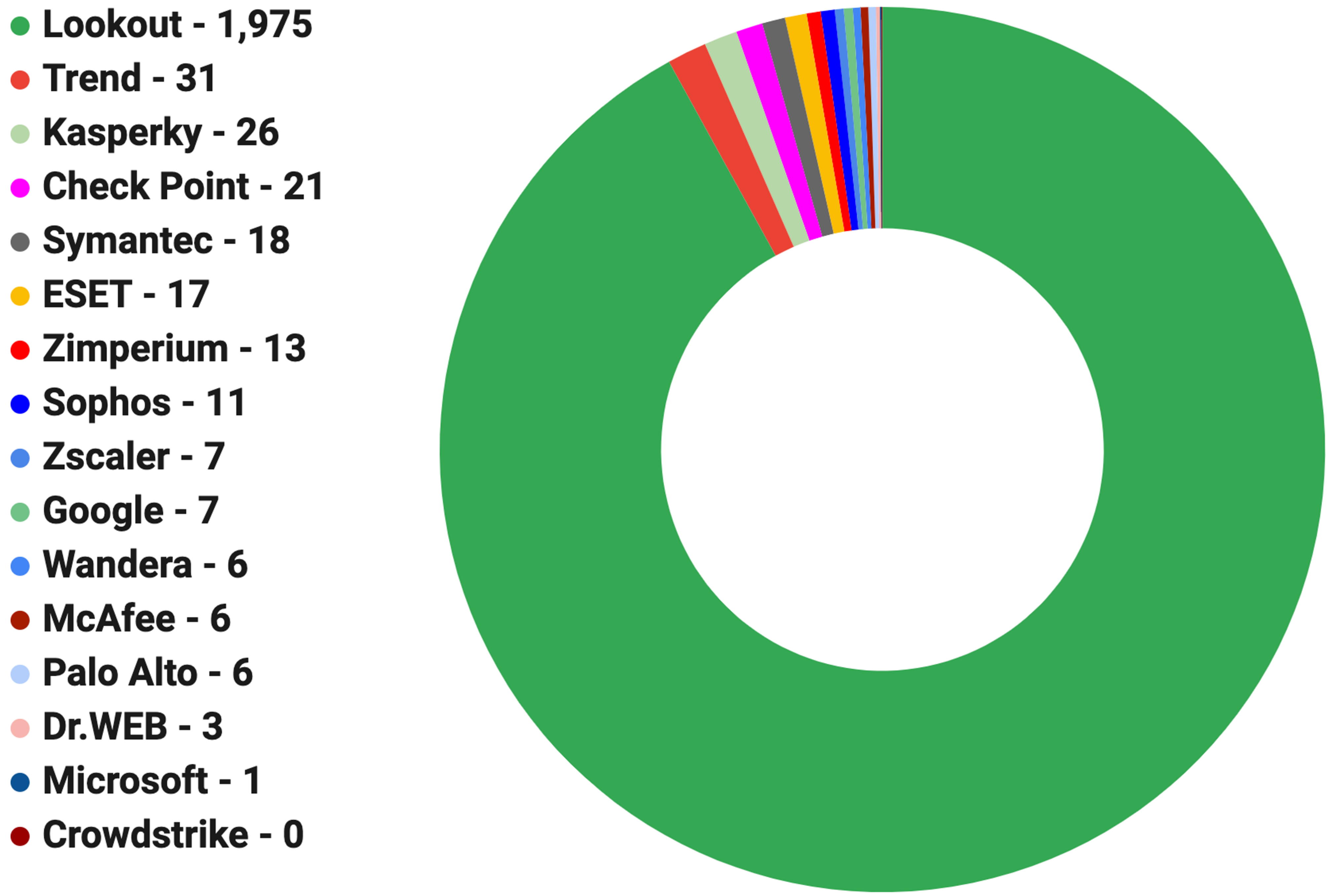


Lookout Security Graph

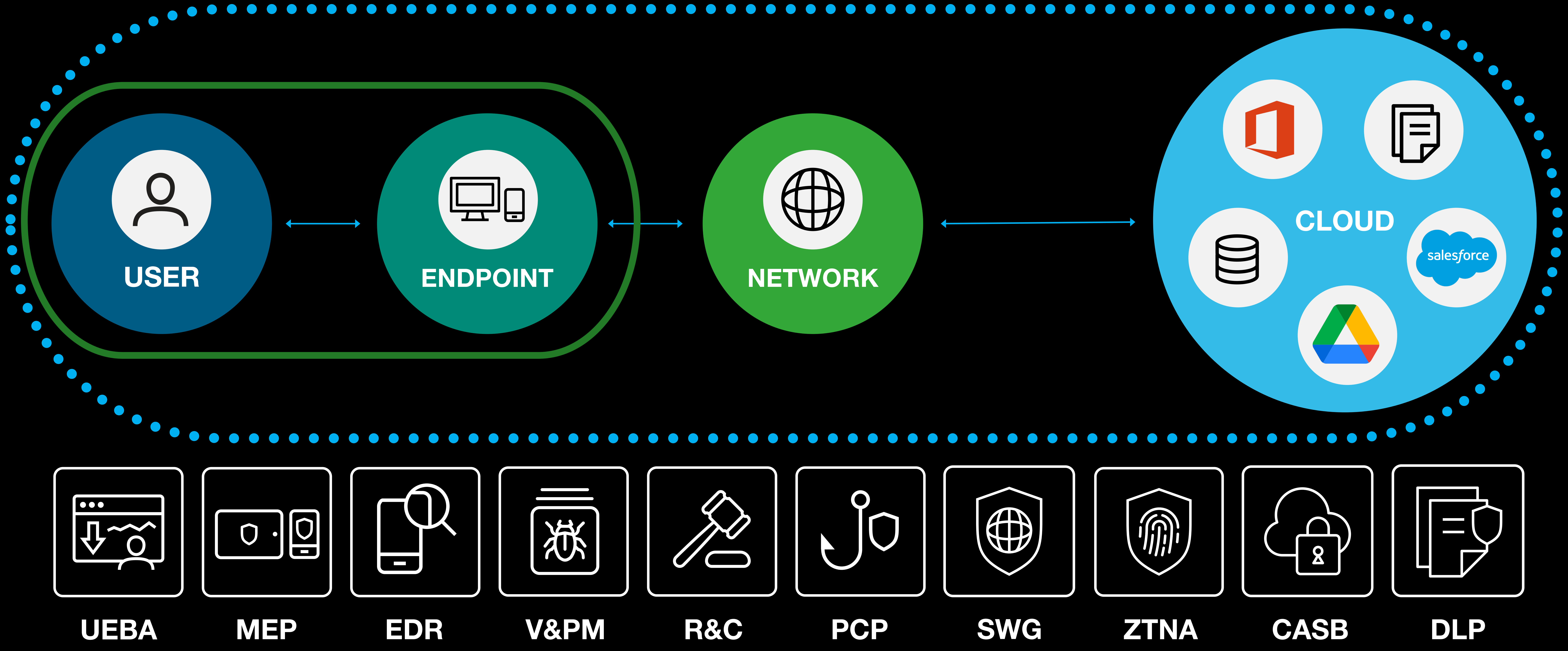
Identifying major threats

- Pegasus
- Chrysaor
- ViperRAT
- SonicSpy
- Frozen Cell
- JadeRAT
- Titan
- SpywallerV2
- Dark Caracal
- Desert Scorpion
- ViperRATv2
- Stealth Mango
- BancamarStealer
- DNC Phishing
- Monokle
- UN & NGO Phishing
- Canadian Bank Phishing
- Corona Live 1.1
- SpyNote
- SilkBean
- Goontact
- Hornbill
- SunBird

Discovering the most threat families



Delivering integrated endpoint-to-cloud security



Real World Exposure Rates

Q4 Global Mobile Exposure Rates

EMEA

Q4 2020	Android	iOS
Phishing	7.86%	8.83%
OS Vulnerabilities	1.70%	11.58%
App Threats	9.55%	4.80%
Device Risks	2.08%	4.09%
App Risk	0.02%	0.29%
Network Threats	0.19%	0.09%
Device/OS Threats	0.01%	0.00%

NORTH AMERICA

Q4 2020	Android	iOS
Phishing	4.93%	3.85%
OS Vulnerabilities	2.82%	1.19%
App Threats	19.84%	2.90%
Device Risks	7.82%	2.03%
App Risk	0.21%	0.09%
Network Threats	0.03%	0.05%
Device/OS Threats	0.01%	0.00%

ASIA PACIFIC

Q4 2020	Android	iOS
Phishing	7.88%	16.35%
OS Vulnerabilities	0.39%	1.91%
App Threats	9.47%	8.94%
Device Risks	2.65%	1.36%
App Risk	0.01%	0.06%
Network Threats	0.03%	0.11%
Device/OS Threats	0.03%	0.00%

Mobile phishing in financial services

Challenge

A phishing attack can come from anywhere

- The design of mobile UI hides details typically visible on a computer that can help us identify a phishing attack.
- Traditional anti-phishing approaches on mobile devices quickly become privacy issues because they inspect message content.
- Not protecting against mobile phishing leaves a significant gap in an organization’s security posture.

Most Targeted Industries in 2020

Telecommunications – 24.4%

Legal - 22.5%

Retail - 21.6%

Financial Services - 14.7%

Manufacturing - 12.1%

Healthcare/Pharma - 8.5%

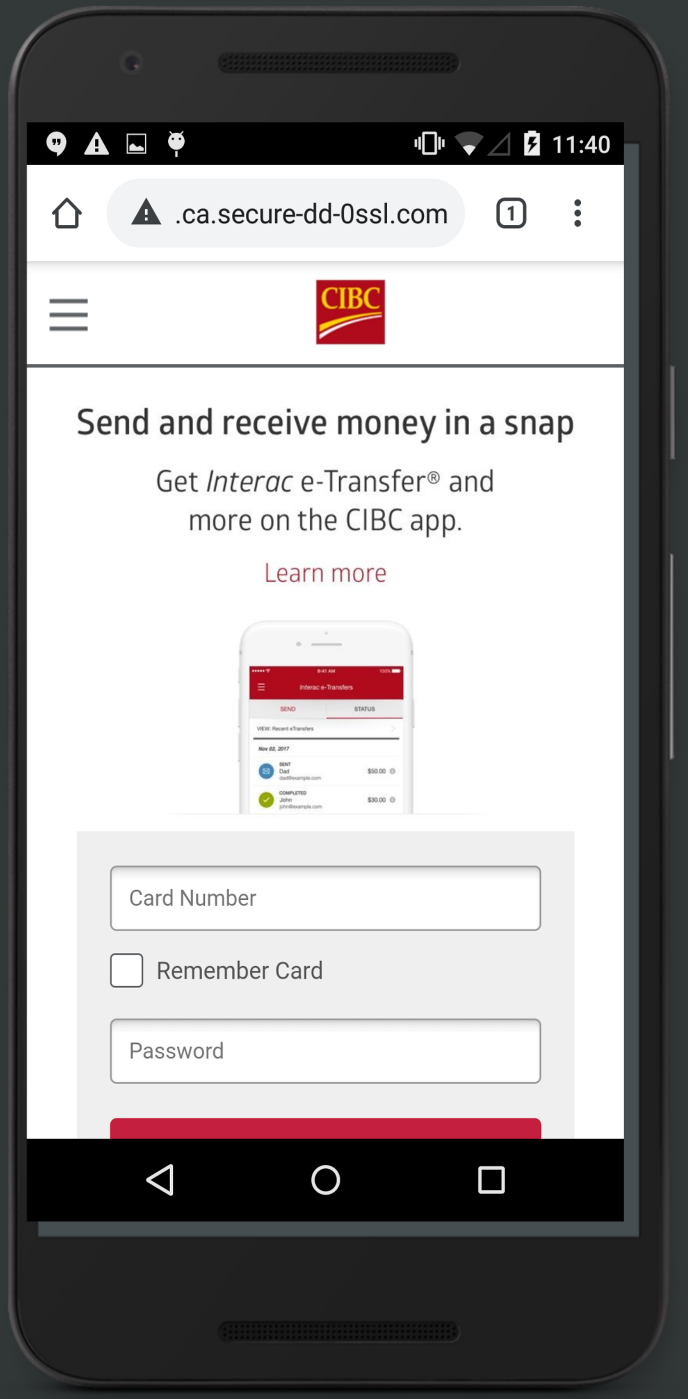
Professional Services - 7.3%

Government - 4.0%

Breaking down intent

In 2020, **14.7%** of financial services employees encountered a phishing link

46.9% were built for credential harvesting



11:40

.ca.secure-dd-0ssl.com

CIBC

Send and receive money in a snap

Get *Interac* e-Transfer® and more on the CIBC app.

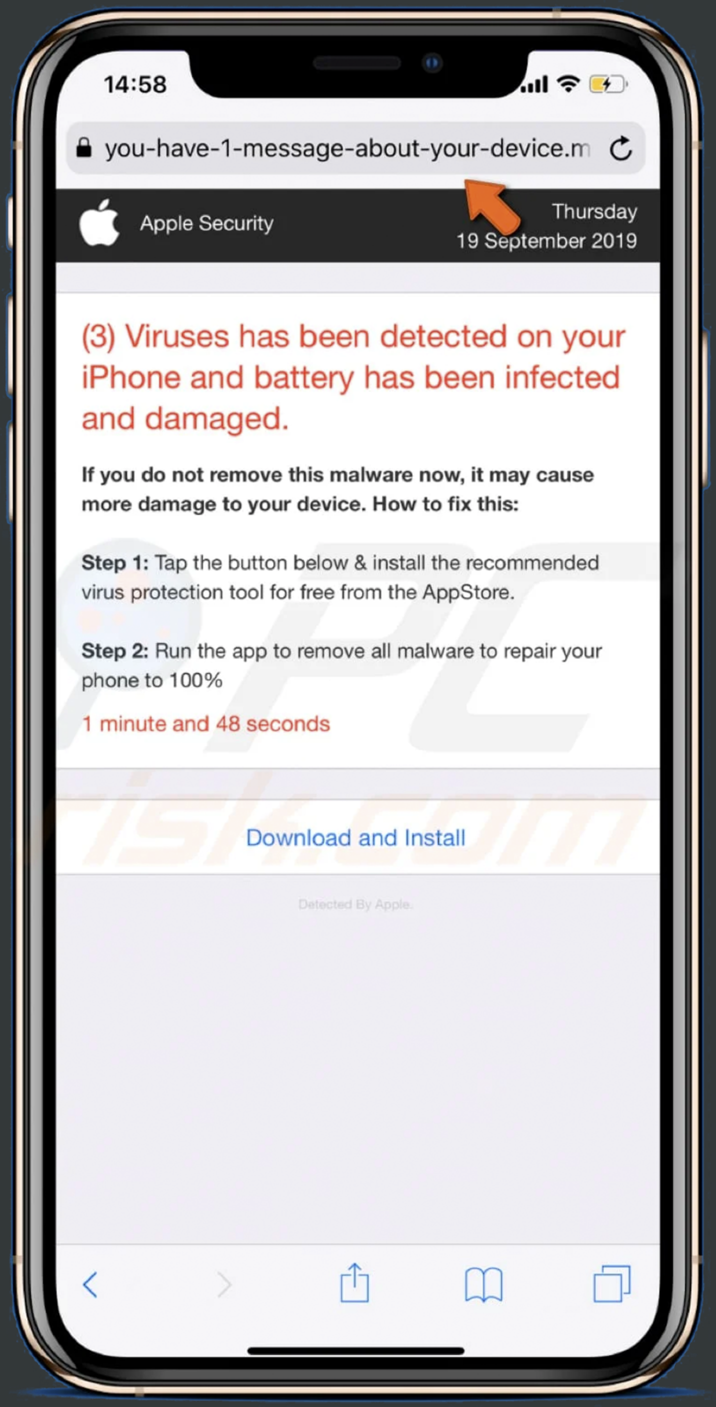
Learn more

Card Number

□ Remember Card

Password

79.4% were built for delivering malware



14:58

you-have-1-message-about-your-device.m

Apple Security

Thursday
19 September 2019

(3) Viruses has been detected on your iPhone and battery has been infected and damaged.

If you do not remove this malware now, it may cause more damage to your device. How to fix this:

Step 1: Tap the button below & install the recommended virus protection tool for free from the AppStore.

Step 2: Run the app to remove all malware to repair your phone to 100%

1 minute and 48 seconds

Download and Install

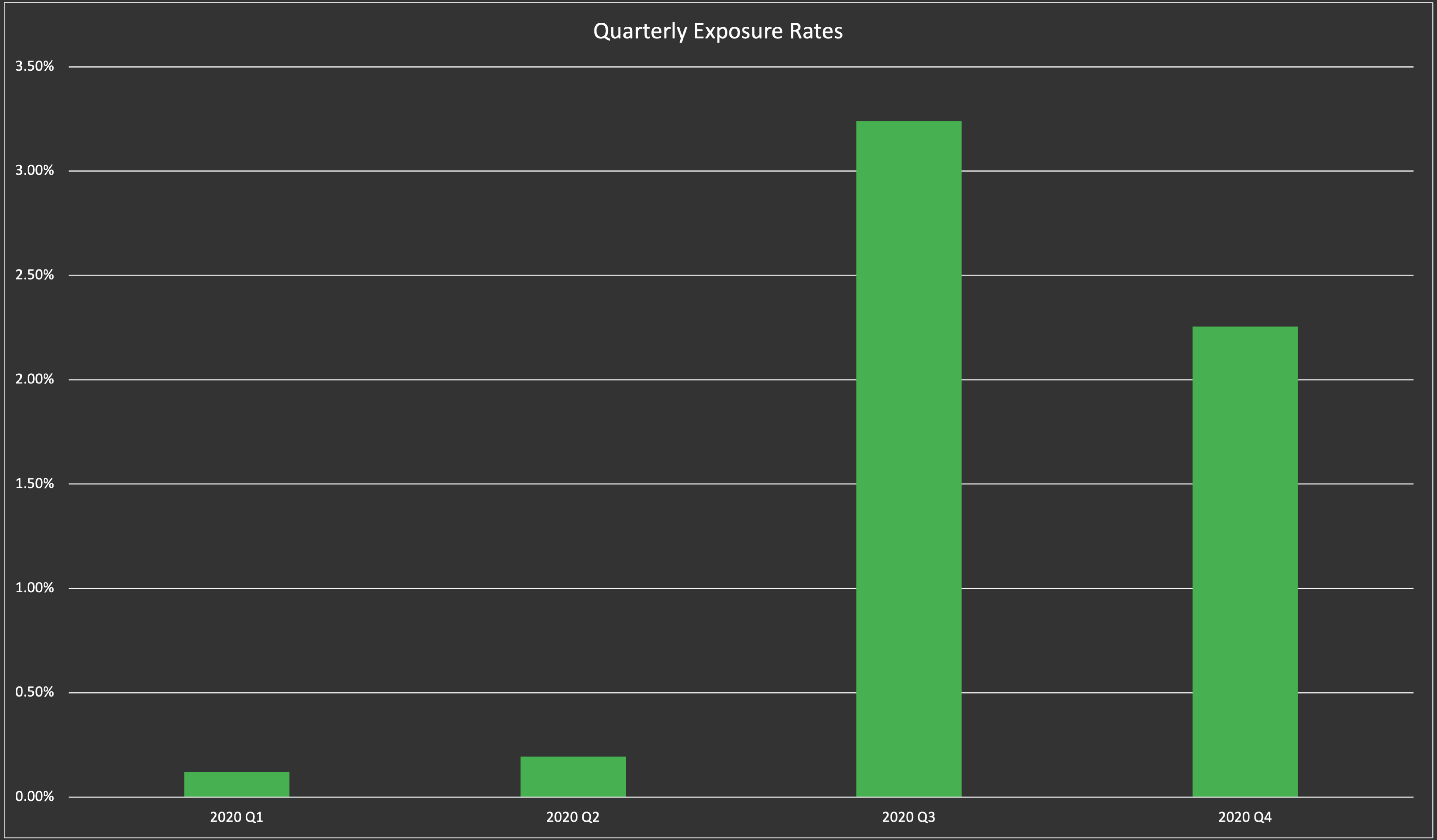
Detected By Apple.

85% of mobile phishing attacks happen in apps outside of email[1]

[1] Verizon Mobile Security Index, February 2020

App threats and risky permissions

Exposure to malicious and risky apps



Three key examples

Chrome for Android

- Triggered when Chrome renders malcrafted HTML content
- Sandbox escape via HTML allows access to Chrome's capabilities without rooting
- MDM will not detect a successful exploit

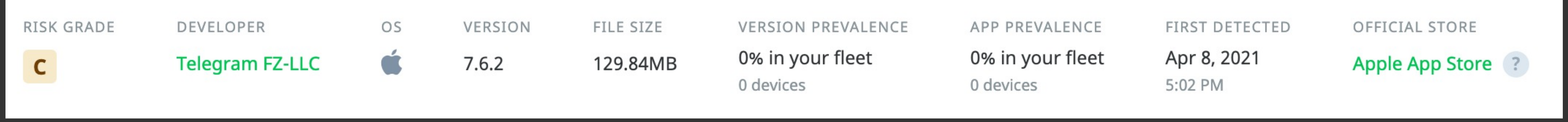
Telegram for iOS

- 13 vulnerabilities were found in one version of Telegram
- A vulnerable library used for emoticons allowed for remote code execution
- Heavy impact to the enterprise because of the app's popularity

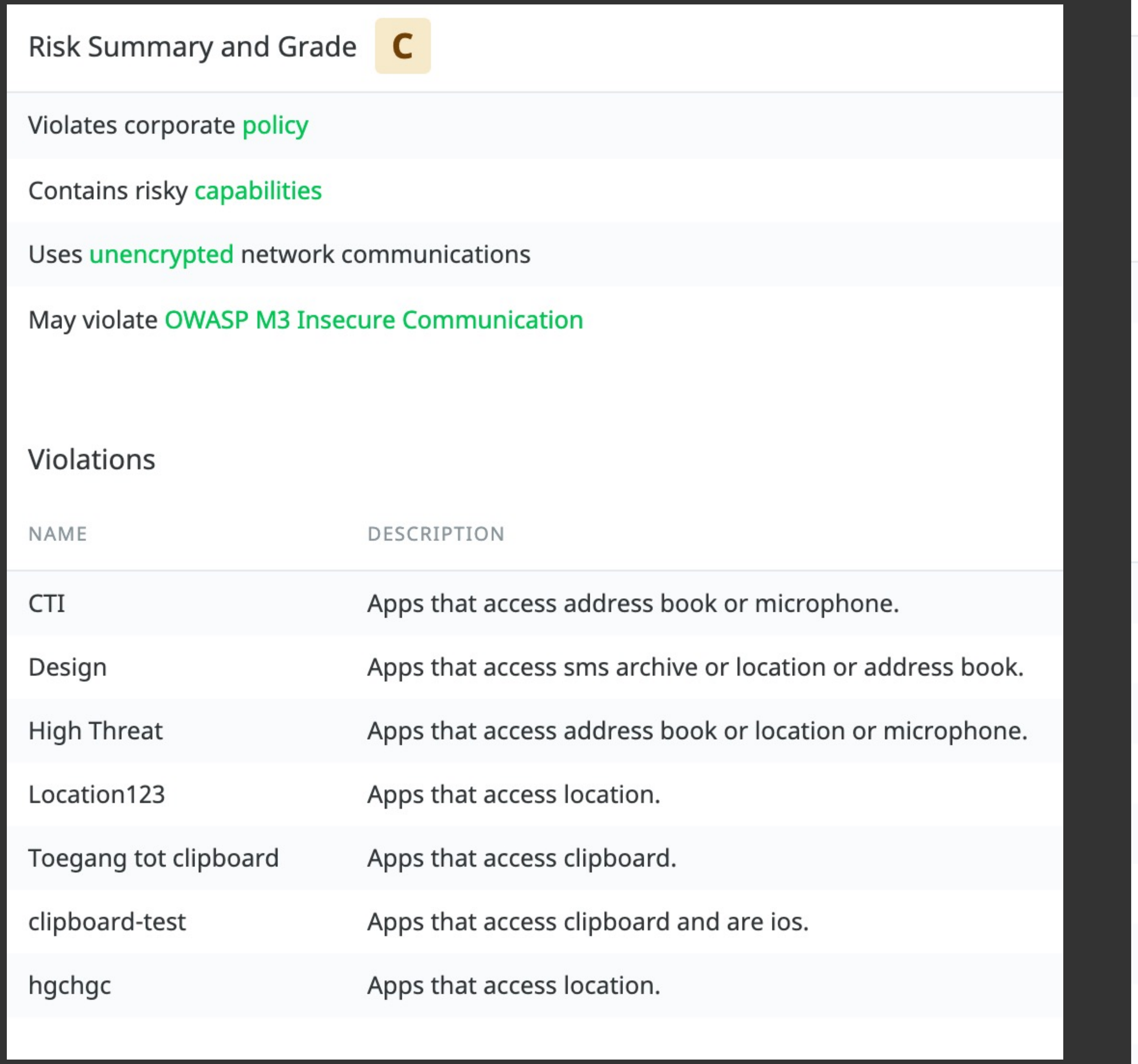
SourMint SDK

- Popular iOS advertising SDK found to have extensive visibility into PII
- Heavy self-obfuscation occurs if the SDK detects any debugging or proxy tools on the device.
- Behavior modification helps it pass through App Store review process

App Analysis: Telegram for iOS



RISK GRADE	DEVELOPER	OS	VERSION	FILE SIZE	VERSION PREVALENCE	APP PREVALENCE	FIRST DETECTED	OFFICIAL STORE
C	Telegram FZ-LLC		7.6.2	129.84MB	0% in your fleet 0 devices	0% in your fleet 0 devices	Apr 8, 2021 5:02 PM	Apple App Store ?



Risk Summary and Grade C

Violates corporate policy

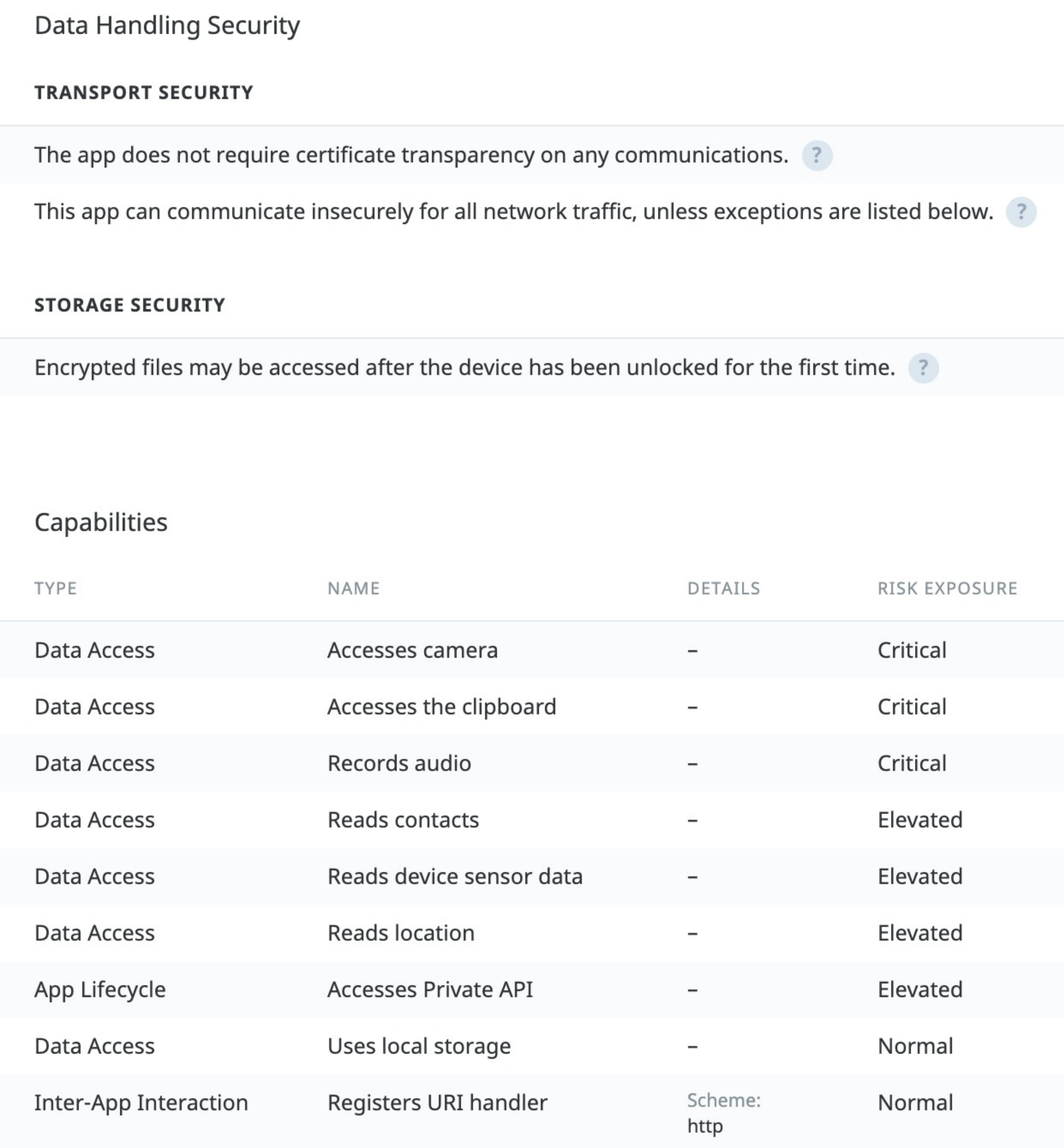
Contains risky capabilities

Uses unencrypted network communications

May violate OWASP M3 Insecure Communication

Violations

NAME	DESCRIPTION
CTI	Apps that access address book or microphone.
Design	Apps that access sms archive or location or address book.
High Threat	Apps that access address book or location or microphone.
Location123	Apps that access location.
Toegang tot clipboard	Apps that access clipboard.
clipboard-test	Apps that access clipboard and are ios.
hgchgc	Apps that access location.



Data Handling Security

TRANSPORT SECURITY

The app does not require certificate transparency on any communications. ?

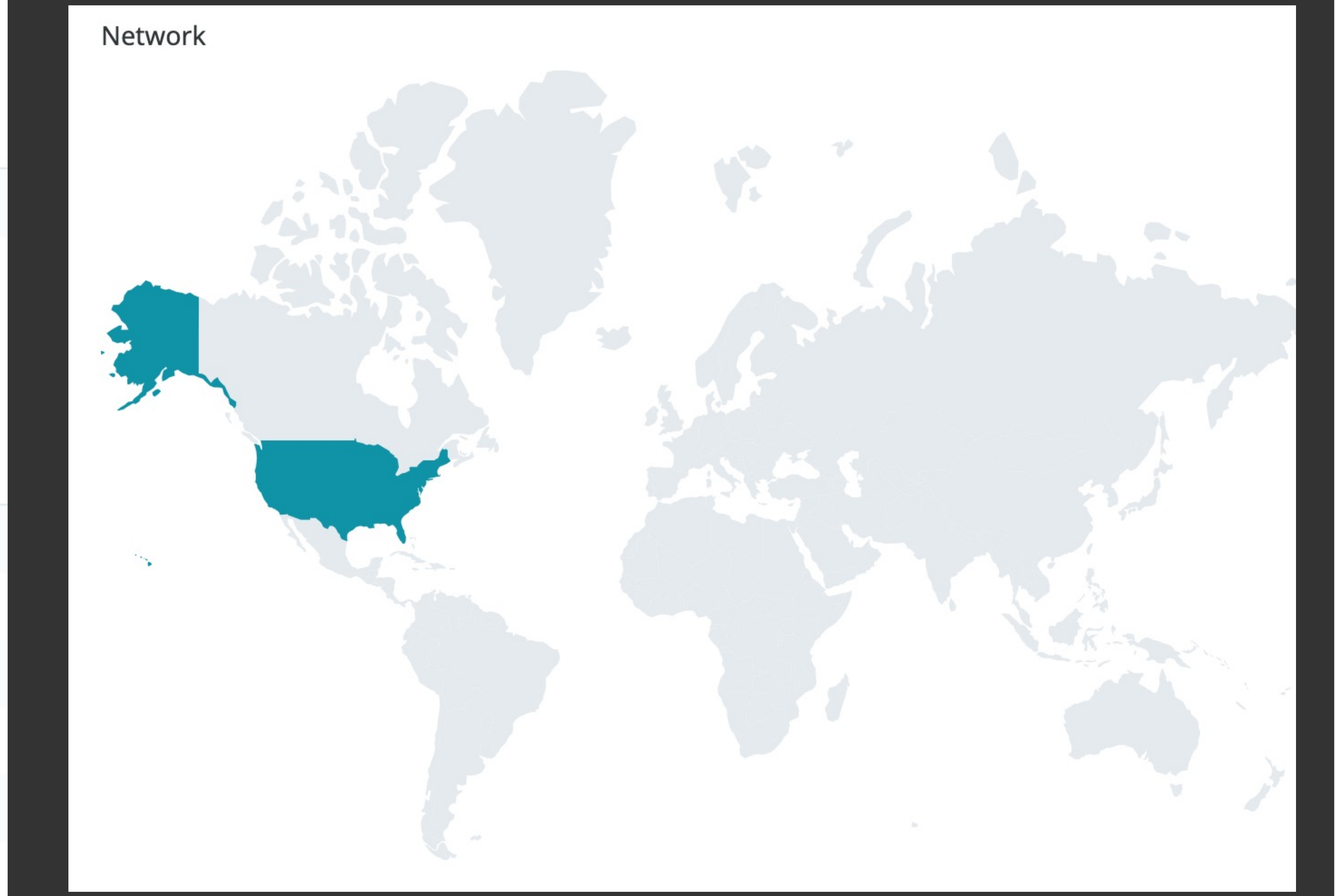
This app can communicate insecurely for all network traffic, unless exceptions are listed below. ?

STORAGE SECURITY

Encrypted files may be accessed after the device has been unlocked for the first time. ?

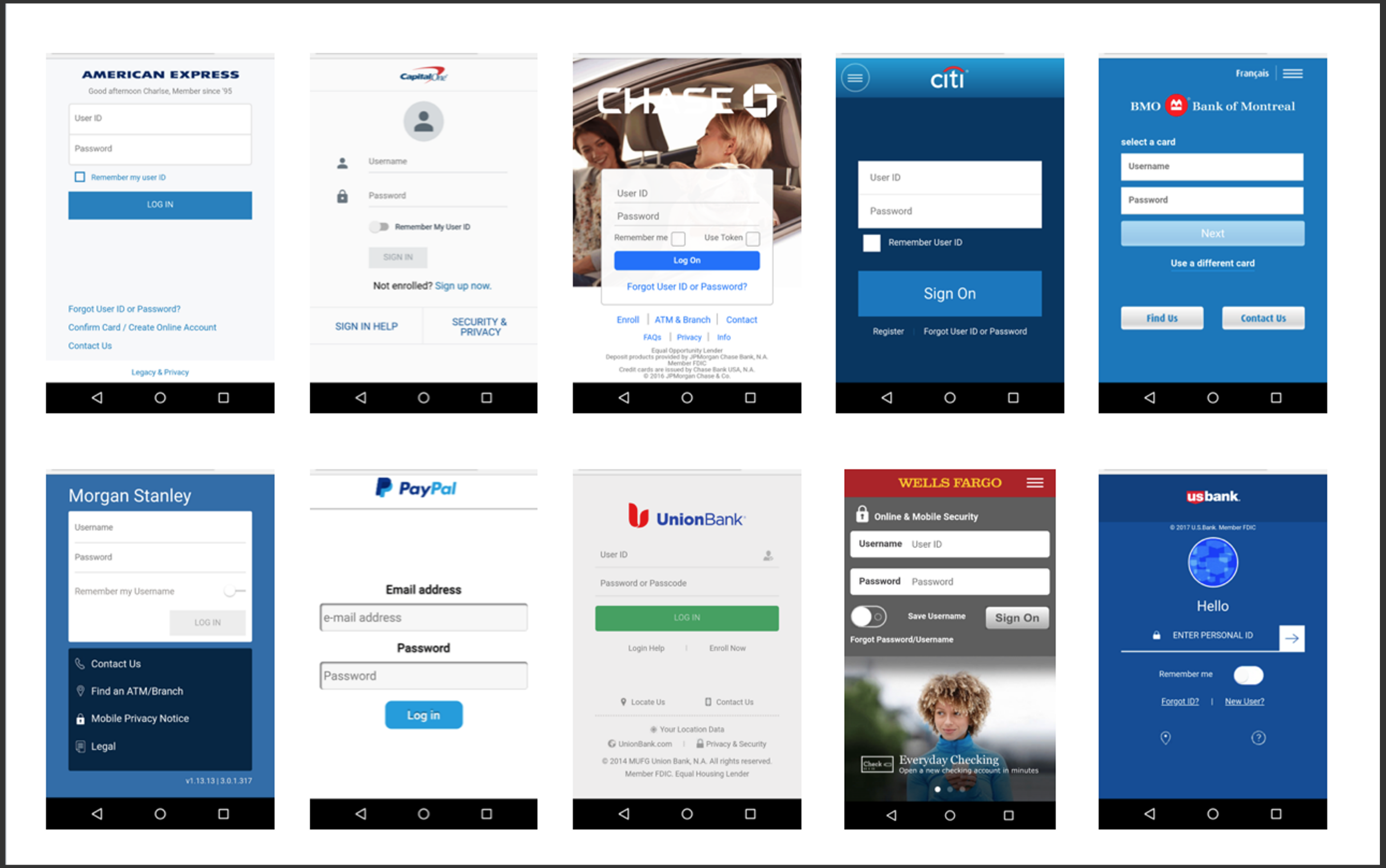
Capabilities

TYPE	NAME	DETAILS	RISK EXPOSURE
Data Access	Accesses camera	–	Critical
Data Access	Accesses the clipboard	–	Critical
Data Access	Records audio	–	Critical
Data Access	Reads contacts	–	Elevated
Data Access	Reads device sensor data	–	Elevated
Data Access	Reads location	–	Elevated
App Lifecycle	Accesses Private API	–	Elevated
Data Access	Uses local storage	–	Normal
Inter-App Interaction	Registers URI handler	Scheme: http	Normal



Network

Bringing it all together: BancamarStealer



- Delivered by SMS and prompts target to download a customized (malicious) app.
- The malware can harvest credentials, implement screen overlays, send the user to other malicious sites, retrieve all SMS, and take control of the device remotely
- Primary use case is trojanizing banking apps, but it’s fully customizable
- Samples have been analyzed that overlay Amazon, Facebook, Skype, Twitter, Uber, and WhatsApp
- First announced by Lookout researchers in 2018. In the last 3 years, the number of observed samples has grown from 7,700 to over 74,000

Where do we go from here?

What life has taught us

Cloud-based security solutions secure your employees where on-prem or on-device solutions fall short.

Secure all devices from endpoint to cloud by implementing mobile security, cloud access security brokerage (CASB), and zero trust network architecture (ZTNA) across devices with one solution.

Use the best data you can. This ensures that your employees are protected from the latest known and unknown threats.

Build access policies based on the risk profile of the device. This includes vulnerable app versions that need to be updated, out of date OSs, risky network connections, and malicious content being present.

Proactively hunt for threats by leveraging app, device, phishing, and network threat data

To learn more

Lookout

THE LOOKOUT SASE SOLUTION

SECURITY FROM ENDPOINT TO CLOUD, ENABLING PRODUCTIVITY FROM ANYWHERE

Your users, apps, and data have left the building

Your apps and data used to reside in data centers, and everyone worked from an office. To gain access, your workforce connected to internal networks using company-issued laptops or desktops. With a security perimeter, you were able to control data flow and protect your organization's data. You also knew what was stored on your endpoints as they were managed by you.

All that changed with cloud technology and remote work. Today, your data goes wherever it is needed. Employees now expect effortless access to whatever they requireneed from anywhere and on any device. To tap into the skyrocketing collaboration, organizations felt they had to relax their security stance as they embraced the cloud. But just because your apps and data left the building, it doesn't mean you're no longer their custodian.

From five corporate locations to five thousand remotes offices

Investing in virtual private networks (VPNs) is how many organizations are supporting their remote workers. While it enables access to on-premise apps from anywhere, it also assumes that every user and device is trustworthy. And because VPN provides whoever is connected unrestricted access to your internal networks, it puts your entire infrastructure at risk.

To promote collaboration while keeping your data secure, you need complete visibility and dynamic access controls. This is where a new framework called secure access service edge (SASE), comes in, delivering protection in the cloud like you still have a perimeter.

Dedicated SASE vendors only provide network-based insight into threats and have limited visibility into the security posture of the endpoint. This means they lack the endpoint capabilities and only have a fraction of what is required to effectively secure an organization from

[Lookout SASE Solution]

Lookout

LOOKOUT MOBILE ENDPOINT SECURITY

PROTECT THE DEVICE THAT GOES EVERYWHERE YOU GO

Don't overlook the device you use the most

Traditional cybersecurity strategies have long been focused on protecting your fixed endpoints such as servers, laptops and desktops from cyberthreats. However, your security requirements have grown organically over time.

The problem is security on mobile devices is often overlooked, creating a gap in your security architecture. While mobile operating systems are considered to be more resilient, cyberattackers increasingly target them because mobile devices are at the intersection of our personal and professional life. These devices have a treasure trove of data and attackers use them as the initial intrusion into your organization.

As you evaluate mobile security solutions to add to your architecture, you face a familiar challenge of choosing between a comprehensive platform or best of breed solution. Because the growth in mobile devices has

BENEFITS

- Cloud-delivered mobile security
- Protects iOS, Android, and Chrome OS
- Endpoint detection and response built by threat researchers
- Optimized lightweight app for processor performance and battery life
- Secures company-owned and employee-owned devices
- Meet compliance requirements while preserving user privacy
- Frictionless deployment on all employee devices
- Scales to mobile fleets of hundreds of thousands of endpoints

[Lookout Mobile Endpoint Security]

Lookout

SECURING ACCESS TO YOUR APPS WITH A ZERO TRUST APPROACH

DYNAMIC ACCESS TO ENTERPRISE APPS AND DATA WITH LOOKOUT ZERO TRUST NETWORK ACCESS

Remote employees expect seamless access to what they need

Cloud-based infrastructure has enabled your employees to be productive from anywhere on any device. This has driven the need for seamless access to corporate data to get their work done.

Traditional security models assume every user and device inside the network can be trusted – but that puts your infrastructure at risk. Once a user is inside your perimeter, they have nearly unrestricted access to everything. This means your data is vulnerable to anyone capable of gaining access to the involved network, system, or applications.

Secure remote access needs to be dynamic

Your workforce is no longer bound by a traditional network perimeter. With more of your data and apps now in the cloud, your employees can stay productive regardless of the network or the device they use.

BENEFITS

- IGranular identity and context-aware access controls
- Consistent security and user experience across onpremise, IaaS and SaaS applications
- Application-centric control limits access only to those who need it
- Application cloaking prevents discovery on the public Internet
- Extends advanced security to legacy applications with identity and access management
- Agentless access from any endpoint device

Second, they don't understand whether the device connecting into the network is free of malware or if the user is who they say they are.

[Lookout ZTNA]

Lookout

SECURING YOUR APPS AND DATA, FROM ENDPOINT TO CLOUD

LOOKOUT CLOUD ACCESS SECURE BROKER PROTECTS YOUR DATA WITH COMPLETE VISIBILITY AND CONTROL

Security challenges introduced by your growing cloud footprint

In the modern work environment, we rely on cloud services to collaborate with colleagues, contractors and partners. It no longer matters where we work or what device we use – we now have easy access to the data we need to be productive.

Amid the skyrocketing collaboration, your data is going where it's needed. Employees work from everywhere, collaborating over networks and devices that you may not have control over. They're also juggling between personal and work cloud apps to keep up with life responsibilities. Collaboration may have skyrocketed, but so have the risks your data is exposed to.

Maintaining visibility and control as you move to the cloud

As your organization collaborates in the cloud, you need to protect your data while also making sure you

BENEFITS

- Simplifies security governance on all cloud and private apps
- Integrates with productivity suites such as Google Workspace and Microsoft 365
- Delivers extensive data discovery capabilities across multi-cloud deployments
- Protects data with advanced classification and Data loss prevention (DLP)
- Secures and controls data shared externally with encryption and rights management
- Detects insider threats with User and entity behavior analytics (UEBA)
- Manages security posture of cloud infrastructure and applications

[Lookout CASB]

Lookout®

Thank you!