



THE PROBLEM

Companies are at risk from apps on employees' phones that are capable of leaking company or customer's private data.

- Private data is taken from all 2 billion global smart-phone users, largely without user knowledge
- "To prevent data leakage enterprises will spend \$76.9 billion this year growing to \$101 billion by 2018" – Gartner
- "Cyber attacks cost businesses \$400 billion per year" – Lloyds of London

THE SOLUTION



Mobile Intelligence Dashboard

Search for User, App, Etc.

Advanced

Data Taken Today



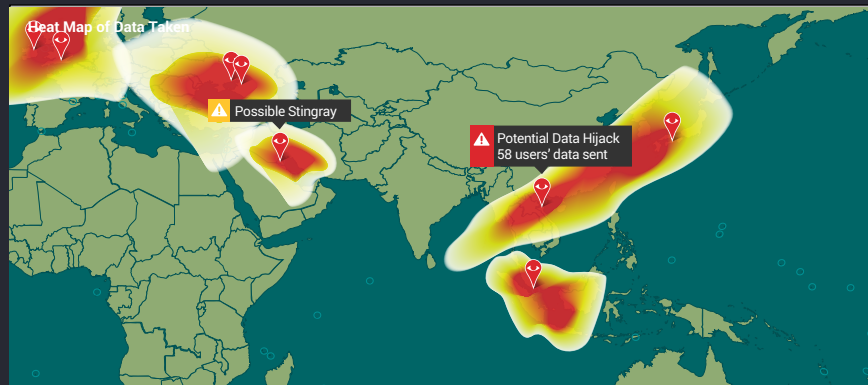
Data Taken 10.4 Gb
Data Sent 807 Mb

Emerging Issues
Dashboard
Reports
Saved Reports
Create Custom Report

Top Intelligence

- ▶ All Mobile Apps
- At-Risk Users
- App Authors
- Banned Apps
- Vulnerabilities
- Data Destinations
- Other Devices
- Phone Towers

Edit Dashboard



Alerts

- ⚠ Potential Data Hijack
58 users' data sent
- ⚠ Possible Stingray – False cell tower
- ⚠ Potential Illicit Camera Use

Most At-Risk Users

1. Darren Warrekind
2. Valentina Morokoff
3. Parul Singh
4. Jay Edwardson
5. Jason Epstein
6. Nicole Peterson
7. Vera Tennyson
8. Thomas Beadersley
9. Washington Victor
10. J. Lincoln Rich

Top Destinations

1. Beijing
2. Donetsk
3. Dublin
4. San Jose
5. London

[See All](#)

Riskiest App Authors

1. Capio caecus
2. Valetudo
3. Persto consectetuer
4. Commodo
5. Pertineo ut
6. Capio caecus
7. Valetudo
8. Persto consectetuer
9. Commodo
10. Pertineo ut

[See All](#)

App Installation Denied

1. LEO Privacy Guard
2. Valetudo Flashlight App
3. Happy Kittens
4. Go Launcher Pro
5. SwiftKey Keyboard

Intelligence

Sed humo scisco eros importunus, opto te te eros eros.
2:15 PM, 3/3/16

Ex interdico in abbas facilisis duis jus proprius aliquip ille.
2:15 PM, 3/3/16

Luptatum capto, tincidunt augue illum ut commoveo
2:15 PM, 3/3/16

Iriure molior regula quibus et facilisi.
2:15 PM, 3/3/16

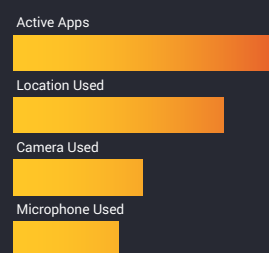
Vulputate mauris ut neque jus consequat turpis capto.
2:15 PM, 3/3/16

Nostrud uxor uxor ex in abbas dolus.
2:15 PM, 3/3/16

Today's Most Active Apps

1. Capio caecus
2. Valetudo
3. Persto consectetuer
4. Commodo
5. Pertineo ut
6. Eligo causa
7. Vero in interdico
8. Tum premo in
9. Reprobo at
10. Ludus tation sed

Status



SOLUTIONS FOR THE ENTERPRISE

The Privacy Sentry Mobile Threat Intelligence Platform enables companies to monitor, analyze and take control of leaky applications which may exfiltrate personal or private information of the employee, company, or the company's customers.

- Monitor app behavior on employee phones via SpyAware Privacy Guard Enterprise
- Mobile Threat Intelligence Database combines real time data from SpyAware Privacy Guard Enterprise, along with



data from Privacy Sentry's own Deep Analysis Platform to provide detailed, up-to-date privacy threat information

- Mobile Threat Intelligence Dashboard's simple tools provides actionable intelligence from the Mobile Threat Intelligence Database

- Integrate Mobile Threat Data with Enterprise SIM (Security Information Management) and MDM (Mobile Device Management) Solutions
- Licensed on a per seat subscription model or as SAAS service

SOLUTIONS FOR THE CONSUMER

The free SpyAware Privacy Guard mobile app provides consumers with Real time monitoring and data exfiltration protection, monitoring the leakage of all smart phone data: what's being taken and where it's going.

- Monitor device for apps that are misusing their permissions to take private data or your location
- Stay up-to-date & be notified when high-threat apps are detected on your device

The screenshot shows the 'Threat Report' screen of the SpyAware app. At the top, the status bar shows various icons and the time 1:13 PM. The app header is red with a shield icon and the text 'Threat Report'. Below the header, a Facebook icon is followed by the text 'Facebook took your data'. A table shows 'Vulnerabilities' as 13 risky permissions and 'Amount of Data Taken' as 5.6 MB sent and 21.6 MB received. Below this is a map titled 'Data Was Sent to 104 Destinations' with several red location pins. At the bottom, there are two sections: 'Took Your Location' showing '0 times' and '0% in background', and 'Notifications' showing 'OFF / ON'. A red 'Take Action' button is at the bottom left, and social media icons for Facebook and Twitter are at the bottom right.

DOWNLOAD THE SPYWARE ANDROID APP



iPhone App COMING SOON