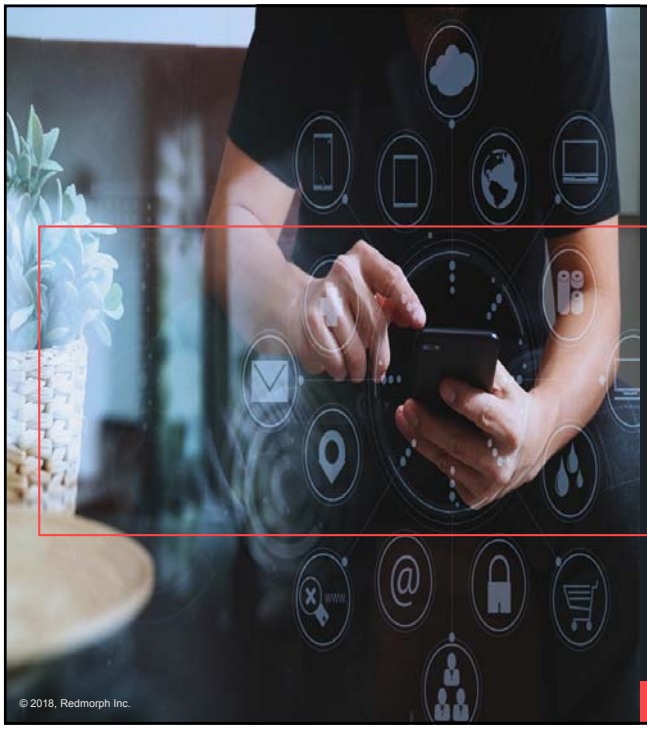


redmorph

Your Data and Social Media

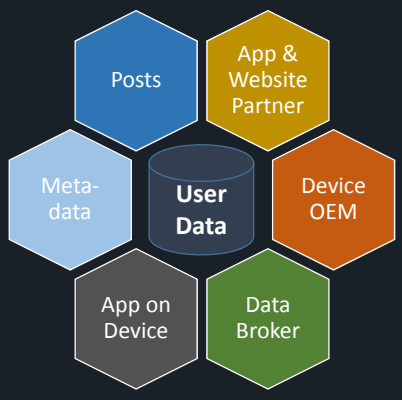
July 17, 2018

What user data is collected and how?

Communications with friends such as messages, photos, videos, etc. linked to your feed or IM

Metadata associated with your posts such as data, time, location, device, etc.

Background data collection by app on device such as other apps used, frequency, location history, call/SMS logs, mic, camera, etc.



Social media “Like” buttons in other websites and apps; Or apps using FB for user authentication

Partnerships with OEM to become a system app with intrusive permissions and tracking and that cannot be uninstalled by user

FB is the largest aggregator of user data and actively purchases or exchanges data with leading data brokers globally

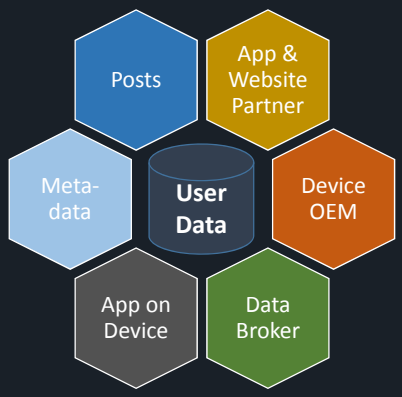
redmorph

How can a user prevent this data collection?

Awareness and discipline on social media app usage

Awareness and discipline on social media app usage

Limiting permissions, preventing overlays and blocking internet access when not in use. App isolation or sandboxing.



Deleting cookies, preventing 3rd parties using network firewall, disabling social media like buttons (Eg. iOS Safari & Firefox browser)

Limiting permissions, preventing overlays and blocking internet access when not in use. App isolation or sandboxing.

Blocking ad-networks, data brokers, etc. behind device, apps & websites prevents data leak and monitoring

redmorph

THE PROBLEM WITH SMARTPHONES

Apps and unknown 3rd parties can access everything or do anything on your device

Most permissions are automatically granted without User consent

LOSS OF PRIVACY

Apps can allow unlimited 3rd parties without your consent

These 3rd parties can monitor and steal your data

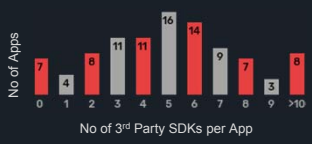
LOSS OF SECURITY

It's difficult for you to identify apps with malicious intent

Malicious app can monitor you, steal your data, or corrupt your files

redmorph

APPS & 3rd PARTY PERMISSIONS



01 Apps requested over 1/3rd more dangerous permissions than required for it to function*

- 69% of Apps do not take explicit user consent during install
- 68% of Apps do not give Users the choice of opting out from providing PII
- 77% of Apps are silent on what happens to User PII

02 93% of Apps have at least one 3rd Party SDK embedded by the developer*

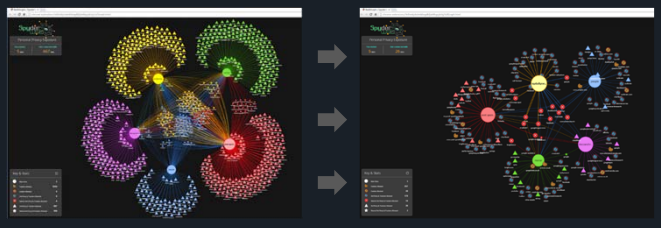
- Advertisers, Analytics, Data Brokers, etc.
- Good vs. bad or unregulated open source SDKs

03 94% of Apps share data with at least one 3rd Party*

- On average, over 50% of network connections belong to 3rd Parties and are not essential to the base function of the App

* Source: Arrka Consulting, 2017 study

redmorph



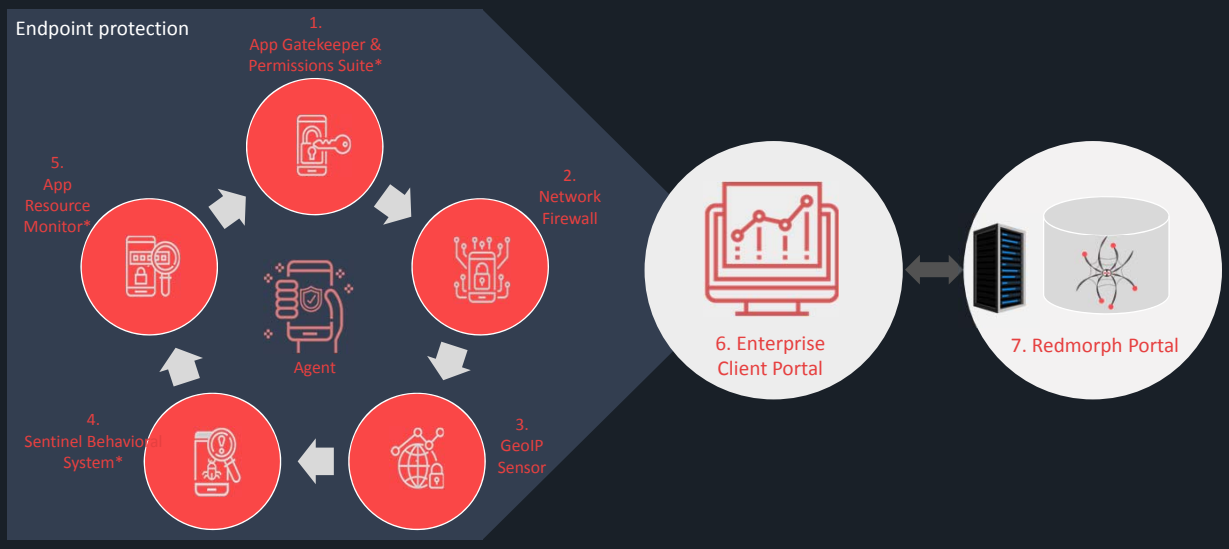
Thank You!

redmorph

Privacy Matters.

Please visit us at redmorph.com or contact us at sales@redmorph.com

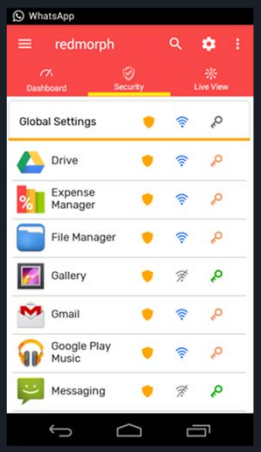
redmorph



redmorph

01. APP GATEKEEPER & PERMISSIONS SUITE

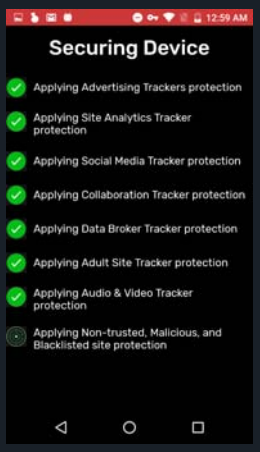
- At install scan ALL apps (OS, OEM, user installed)
  - Get app level profile from Redmorph cloud
  - Quarantine malicious apps and alert user to uninstall
  - Apply app level settings & rules
- Manage the strength of the Redmorph blocking mechanism per App or globally
  - Allow or Block internet to specific Apps
  - Firewall protection levels
  - Sentinel settings
  - System/OEM apps to monitor and control
- Validate all new apps when installed or updated
  - Prevent install of known malicious apps
  - Quarantine unknown apps or apps with dangerous permissions until RM resolution
- Central management of dangerous permissions
  - Alerts for dangerous permissions sets for trusted or untrusted apps



redmorph

02. NETWORK FIREWALL

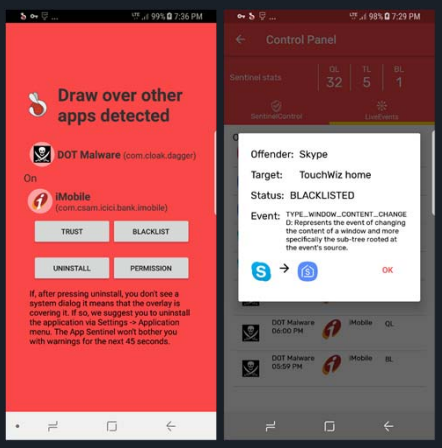
- Enable the monitoring, reporting, and filtering of network traffic on Android devices
  - ► Monitor and block all non-essential incoming and out-going internet connections behind apps, websites, OS and OEM hidden apps
  - ► Real-time proactive monitoring of all device internet traffic
- Over 8 levels of intelligent filters across 3 protection levels
  - ► Customized app level tracker protection: Set level to ensure optimal protection and performance
  - ► Encrypted (SSL) or normal transmissions



redmorph

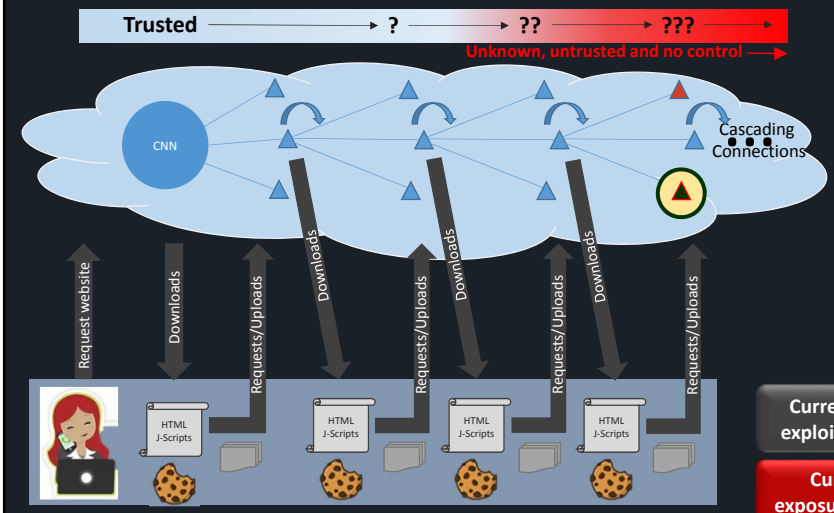
04. SENTINEL BEHAVIOUR SYSTEM

- Behavioral and contextual monitoring in the background
  - ► Monitor app behaviour or intent and to proactively identify and stop potential tracking or malicious activity
- A response to Overlay Attacks or Cloak and Dagger Attacks
- Mitigation of malicious processes on Android Devices
- Application Isolation
  - ► Ensure than when your application is running, no other Process can interfere or collect data in the background
  - ► While any selected application is in the foreground and being used, all other applications will be stopped from operating during that period



redmorph

Understanding background behavior of websites & apps



Privacy Issue
- Unrestricted & intrusive tracking
- Monitoring of online activity
- Gathering of personal info without consent

Security Issue
- Malicious activity such as loading of Malware, Trojan, Phishing, Virus, etc.
- Theft of confidential information or worse

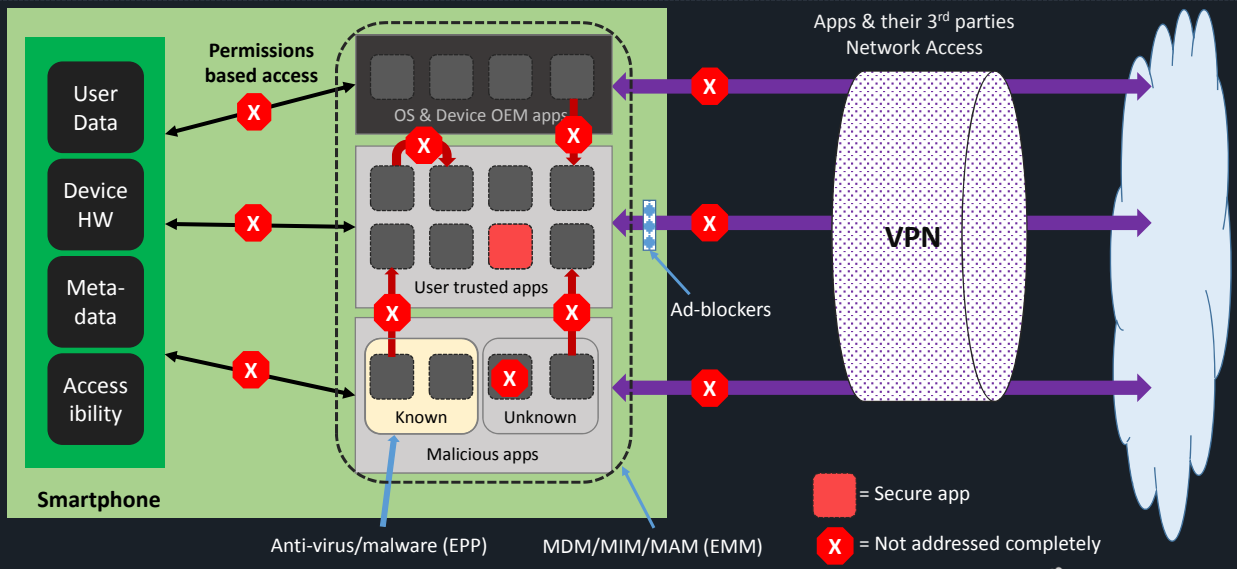
Suboptimal Performance
- Slow page loads & app performance
- Excess data & battery consumption

Current web architecture allows for bad actors to exploit unsuspecting websites/apps and their users

Current tools do not adequately address this exposure to security threat and potential IP/PII leaks

redmorph

THE ECOSYSTEM & CYBERSECURITY TOOLS



redmorph