CORELLIUM®

Mobile Malware and Threat Research

The Corellium Arm virtualization platform provides cybersecurity threat and research teams with never-before-possible mobile malware and threat research capabilities on virtualized iOS and Android devices. Its high accuracy, Arm-native device models enable static and dynamic mobile app and OS introspection.

It's not an emulator or simulator; it's Arm on Arm virtualization.

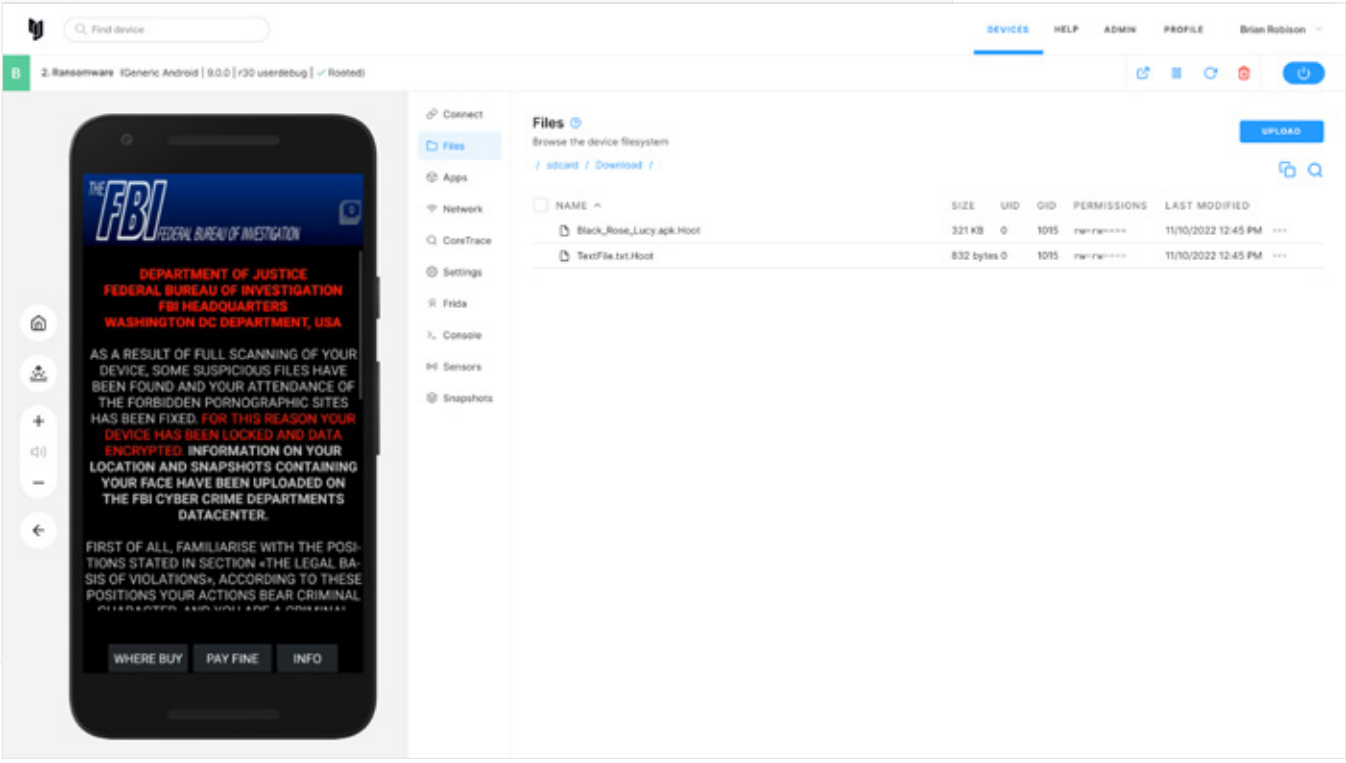
IoC Gathering and Threat Hunting

Augment static mobile malware and threat research with advanced dynamic analysis. Detonate mobile malware or actively engage with smishing and phishing scams directly from a virtual iOS or Android device. Easily change the device's physical location (GPS) to examine location-based threats, and use a local proxy with VPN connectivity to gain network connectivity anywhere in the world.

Mobile Malware Detonation and Sandboxing

Safely detonate mobile malware on sandboxed Corellium virtual devices. For mobile threat hunting, use built-in visualization tools for root access, evidence and IoC analysis, filesystem access, SSL/TLS stripped network monitoring, and mobile app debugging. A comprehensive API and USBFlux technology enables integration with leading development and security research tools such as IDA Pro, Frida, and Burp Suite.

Detonate mobile malware and have direct access to the root filesystem for IoC gathering (Black Rose Lucy ransomware shown)



Solutions Highlights

Malware Detonation
Built-in network monitoring tools let you analyze encrypted C2 and app traffic instantly. CoreTrace gives you access to app syscall tracing during execution.

Threat Hunting
Direct root file system access for iOS and Android devices to gather IoC evidence during and after detonation.

Sandboxing
Sandbox with network-isolated virtual hardware for safer mobile threat analysis and malware detonation.

Virtualization Not Emulation
Arm-native, this is real mobile threats and malware running on virtual devices with the ability to quickly restore device snapshots.

Spin Up Needed Devices
Easily spin up near limitless iOS and Android devices, from past models and releases to the very latest.

Instant Root & Jailbreak
Root any device configuration — including the latest versions of iOS — even when no public jailbreak is available.

Procurement
Eliminate physical device procurement and risks by allocating virtual hardware resources to specific teams, with user and project workspace management tools.

Collaboration
Quickly create and deploy virtual devices across users and teams with one-click device snapshot, restore, and cloning functionality, eliminating physical device limitations.

Control
Simplify onboarding, role-based access (RBAC), and offboarding through centralized administration.

Industries

- Anti-Virus/EDR/XDR Vendors
- Enterprise Threat and Security Research
- Independent Research/3rd Party Testing
- Government

Roles

- Threat Researchers
- Malware Researchers
- Threat Hunters/SoC Teams
- Red & Blue Teams

Technical Capability List

Threat and Malware Research

- Easily spin up near limitless combinations of iOS and Android device, OS, and mobile apps
- Gain device root access, no need to apply additional code or tools
- Conduct research on mobile threats using any iOS version; jailbroken, rooted, or not
- Detonate and monitor mobile malware apps (IPAs and APKs) on sandboxed virtual devices
- Easily intercept C2/malware traffic and strip all SSL/TLS
- Simulate SMS (on iOS) to investigate smishing and phishing attacks
- Browse the device's file system to conduct threat hunting and gather IoCs
- Gain instant access to mobile malware app syscall tracing for dynamic analysis
- Control device sensors, GPS location, and device IDs

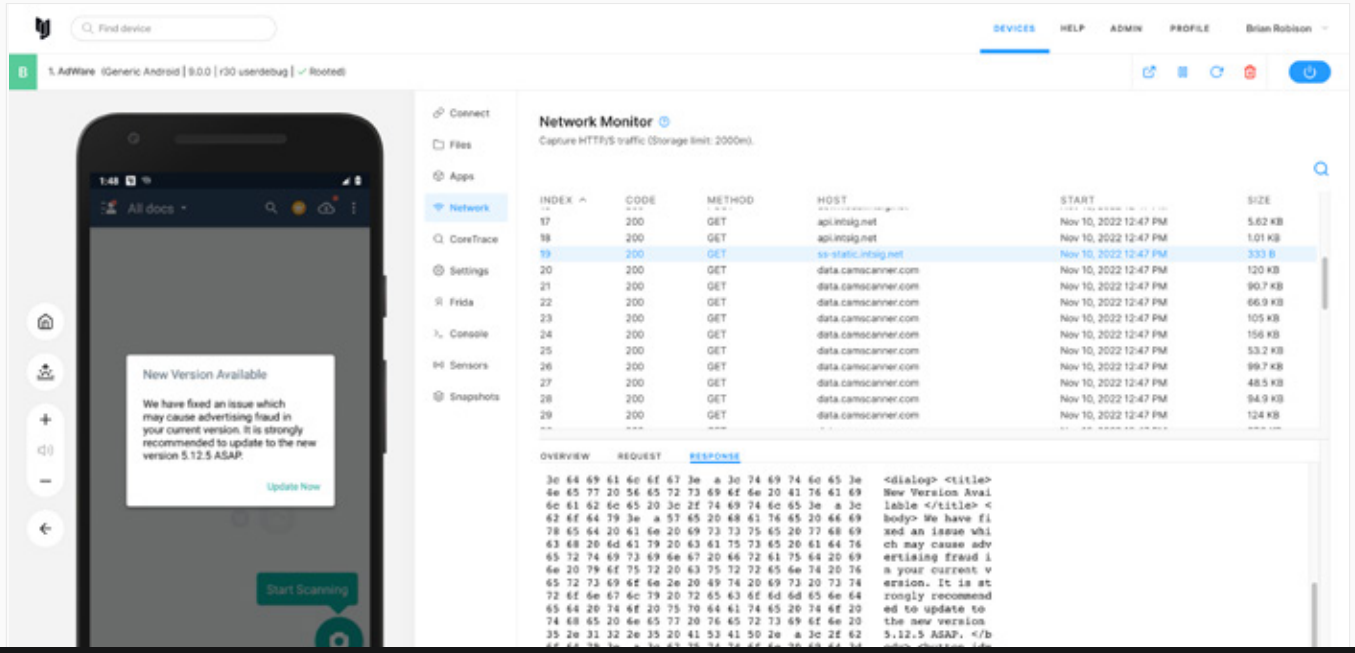
Conduct More Research, Faster

- Single web-based platform for both iOS and Android
- Snapshot and restore virtual devices nearly instantly
- Stop hunting the "used" market for specific devices
- No need to ship physical devices to global team members
- Eliminate time wasted with physical device maintenance

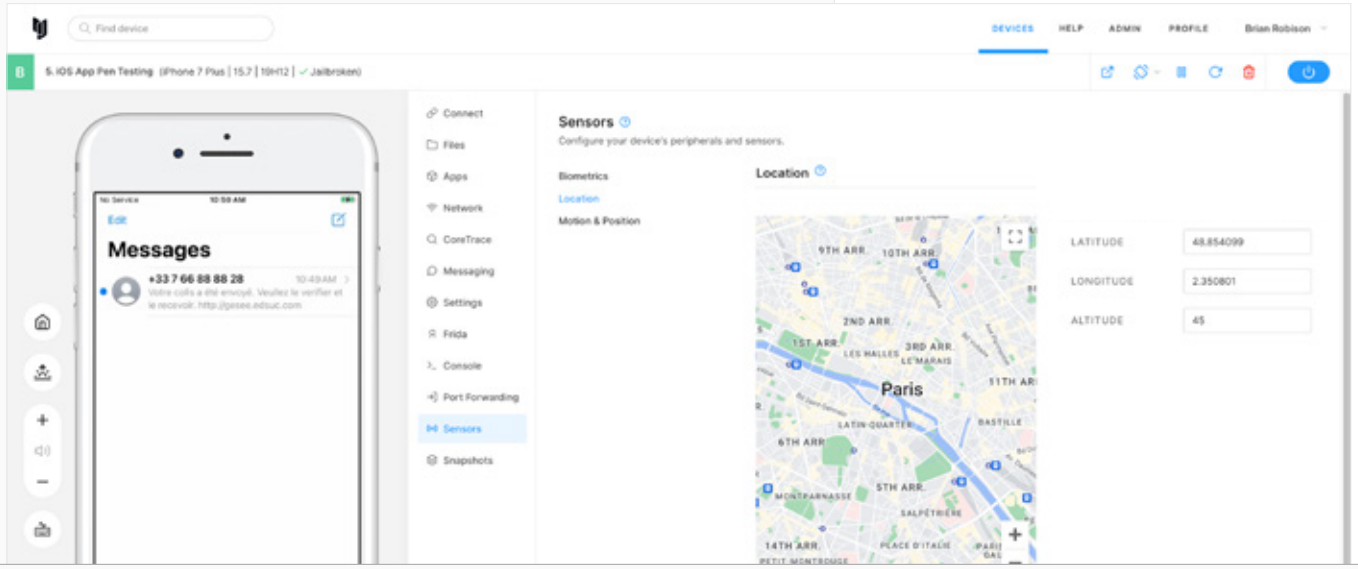
Training & Education

- Mobile threat research training
- Mobile malware research training
- Mobile app demonstration platform
- Teach mobile threat and defensive best practices

Instantly capture unencrypted malware and C2 traffic using built-in Network Monitor (CamScanner adware shown)



Quickly research location-specific smishing and phishing mobile threats without having to ship a physical device



Corellium Virtual Hardware Platform

VIRTUAL DEVICES

Arm-powered phones and IoT devices with endless OS and model combinations.

HYPERVISOR

Corellium Hypervisor for Arm (**CHARM**) is a type 1 hypervisor and the only one of its kind.

ARM SERVER

Virtual models run on Arm, just like real devices, combining native fidelity with on-demand availability.

- **TOOLING**
  Simplified connection of IDE, debugging, network and security tools and comprehensive APIs.
- **CONTROL**
  Configure device buttons, sensors, location, environment, battery, device IDs, ports, cameras and mics.
- **X-RAY VISION**
  Powerful OS, app, file, system call, and console access and control.
- **INTROSPECTION**
  Advanced OS, kernel and boot control and tooling.
- **NETWORK ANALYSIS**
  HTTP/S traffic inspection, tracing, and logging.
- **REPLICATION**
  Snapshot, clone, and restore device states.
- **TEAMING**
  Easy project workspace management and team collaboration.
- **ROOT ACCESS**
  Root or jailbreak devices instantly, no need to add code or apply security vulnerabilities.

CORELLIUM ®