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.



loC Gathering and Threat Hunting

0

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)

Q. Find device		DEVICES HELP ADMIN PROFILE Brian Robison -
B 2. Ransemware (Generic Android 9.0.0 r30 userdebug ~ Rooted)		et 🖩 C 😫 🕓
<image/> <image/>	Connect Files Files Browne the device flesystem / stored / Connected / Apps Network Network Connected NAME ^ Brack,Bose,Lucy apk Hoot Brack,Bose,Lucy apk Hoot	EZE UID GIO PERMISSIONS LAST MODIFIED 237 H8 0 1015 rearrance 1010/2022 12:45 PM *** 832 bytes 0 1015 rearrance 1010/2022 12:45 PM ***

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.

Q 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 guickly restore device snapshots.

C 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.

응+ Procurement

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

은 Collaboration

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

計 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

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

Ð Я 8

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)

						C	0 0
	& Connect	Network I	Monitor 🙂				
• —	C) Files	Capture HTTP	VS traffic (Storag	ge limit: 2000m).			
148 2 9	© Apps						
🖆 All docs - 🔍 🖨 🐼 T	T Network	INDEX A	CODE	METHOD	HOST	START	SIZE.
		17	200	GET	api.intsig.net	Nov 10, 2022 12:47 PM	5.62 KB
	Q. CoreTrace	18	200	GET	apiLintsig.net	Nov 10, 2022 12:47 PM	1.01 KB
		19	200	GET	ss-static intsig net	Nov 10, 2022 12:47 PM	333 B
	Settings	20	200	GET	data.camacanner.com	Nov 10, 2022 12:47 PM	120 KB
		21	200	GET	data.camscanner.com	Nov 10, 2022 12:47 PM	90.7 KB
	S Frida	22	200	GET	data camscanner.com	Nov 10, 2022 12:47 PM	66.9 KB
		23	200	GET	data.camscanner.com	Nov 10, 2022 12:47 PM	105 KB
	>, Console	24	200	GET	data.camocanner.com	Nov 10, 2022 12:47 PM	156 KB
		25	200	GET	data.camecanner.com	Nov 10, 2022 12:47 PM	53.2 KB
New Version Available	PF Sensors	26	200	GET	data.camscanner.com	Nov 10, 2022 12:47 PM	99.7 KB
		27	200	GET	data camscanner.com	Nov 10, 2022 12:47 PM	48.5 KB
We have fixed an issue which	U Snapshots	28	200	GET	data.camacanner.com	Nov 10, 2022 12:47 PM	94.9 KB
may cause advertising fraud in		29	200	GET	data.camscanner.com	Nov 10, 2022 12:47 PM	124 KB
your current vension, it is strongly recommended to update to the new vention 5.12.5.45.8P		OVERVEN		****			
Locate New		30 64 69	61 6c 6f 63	3e a 3c 74 69	74 6c 65 Je <dialog> <title< td=""><td></td><td></td></title<></dialog>		
		60 65 77	20 56 65 72	73 69 61 60 20	41 76 61 69 New Version Ava:	1	
0.101		62 61 64	19 3e a 51	65 20 68 61 76	65 20 66 69 body> We have fi	1	
the second se		78 65 64	20 61 60 20	69 73 73 75 65	20 77 68 69 xed an issue wh:	1	
		63 68 20	6d 61 79 20	63 61 75 73 65	20 61 64 76 ch may cause ad	Y	
		65 72 74	69 73 69 68	67 20 66 72 61	75 64 20 67 ertising freud :	h.	
		65 72 73	69 6f 6e 2e	20 49 74 20 69	73 20 73 74 ersion. It is st	T	
Start Scanning		72 6f 6e	67 6c 79 20	72 65 63 6£ 6d	6d 65 6e 64 rongly recommend	d	

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

OS App Pen Testing: (Phone 7 Plus 15.7 10+112 Jailbroken)</th <th></th> <th></th> <th></th> <th></th> <th></th> <th>C.</th> <th>Ø -</th> <th></th> <th>o.</th> <th>9</th> <th></th>						C.	Ø -		o.	9	
Invite V Data V Data V Data V	 ✓ Connect ✓ Files ④ Apps ✓ Network ◯ ConsTrace Ø Messaging Ø Settings ※ Frida >. Console •) Port Forwarding № Sensions @ Snapshots 	Sensors ③ Configure your device's peripher Biometrics Location Motion & Position	abs and sensors.	STER AR	LATY LONN	TUDE		48. 2.3 45	154099		

Corellium Virtual Hardware Platform



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.



© 2023 Corellium, Inc. All rights reserved. iPhone® is a registered trademark of Apple, Inc. iOS® is a registered trademark of Cisco Systems, Inc. Android[™] is a registered trademark of Google, LLC. All other trademarks are the property of their respective owners.