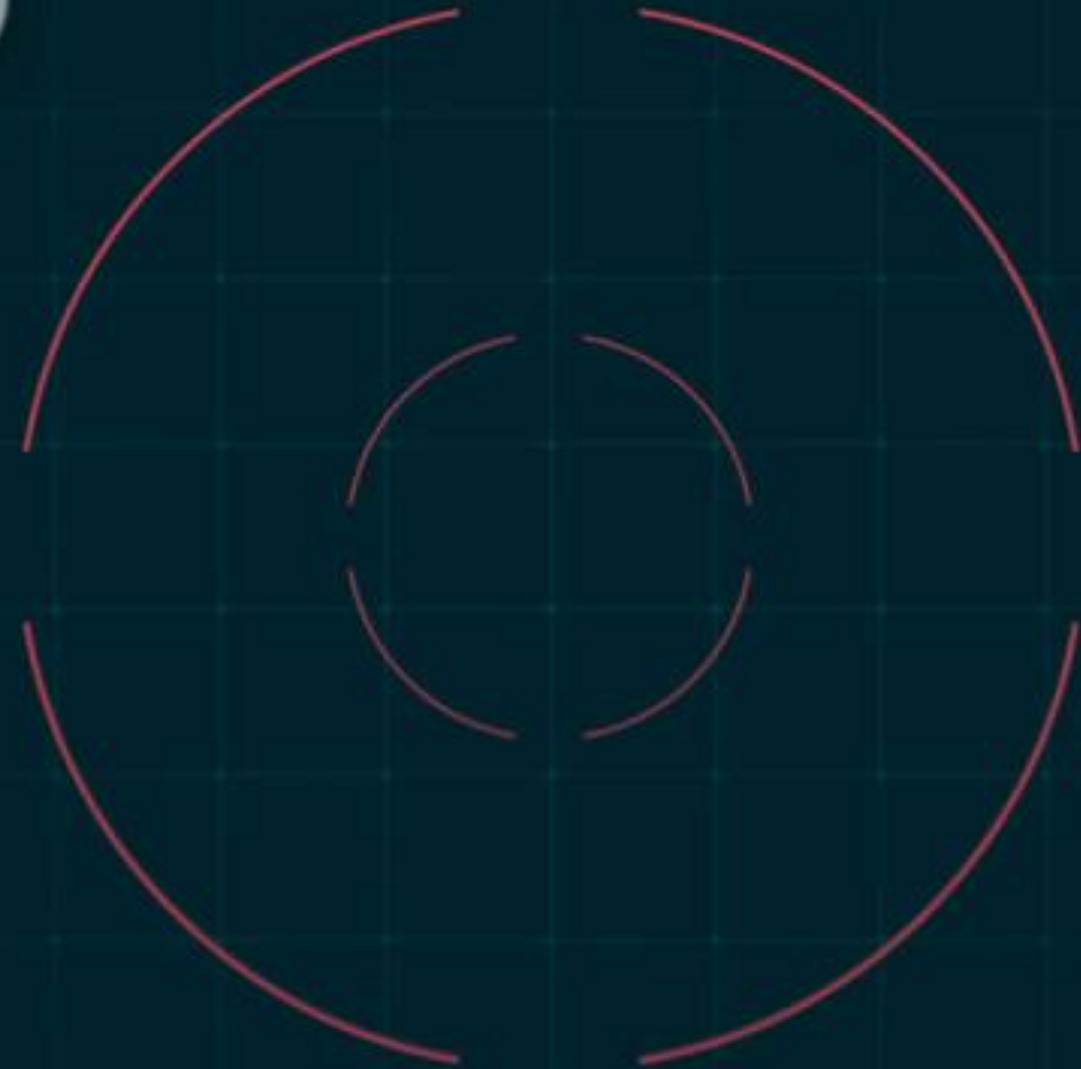


**BUSINESS
AS USUAL
WHERE
IT'S NOT.**



A Quick Intro

S



Common Signs of a Compromised Phone

...and many more



Sudden Reboots



Battery Drain



**Problems Accessing
Mic/Camera**



No Updates

Application / Browser Crashes

Can't power off

Unrecognized Apps

No calls / device logs

Call disconnecting before connecting

Constant switch to 3g/2g networks

Device heating

Keyboard delays

Reboot Loop

Newly created SMS / Outgoing calls

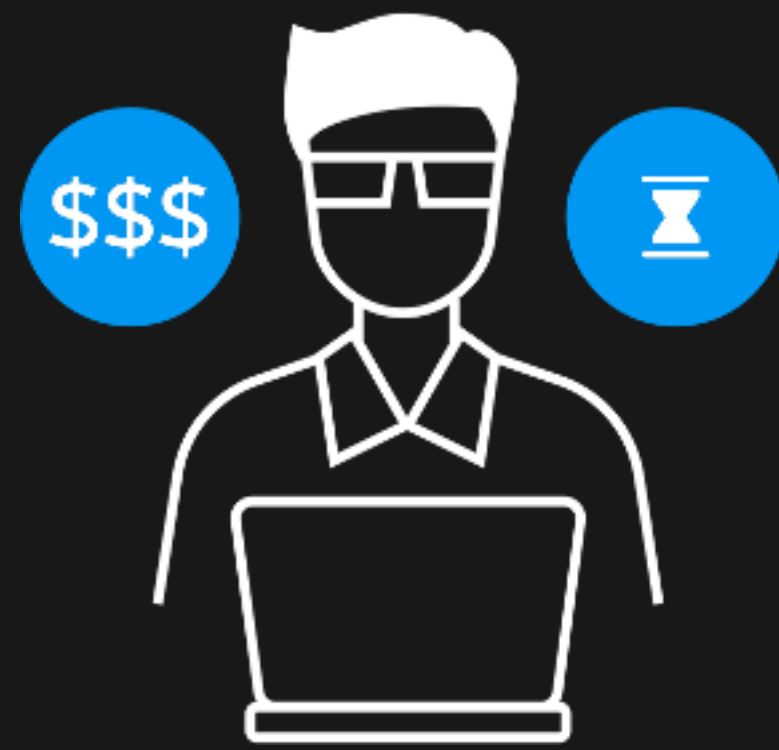
Unrecognized profiles/MDM

Unexpected pincode pop-ups

**SO
HOW DO I KNOW
IF MY DEVICE WAS
ATTACKED?**



Until recently, the closest way to know whether your phone got hacked was



Pay a consultant

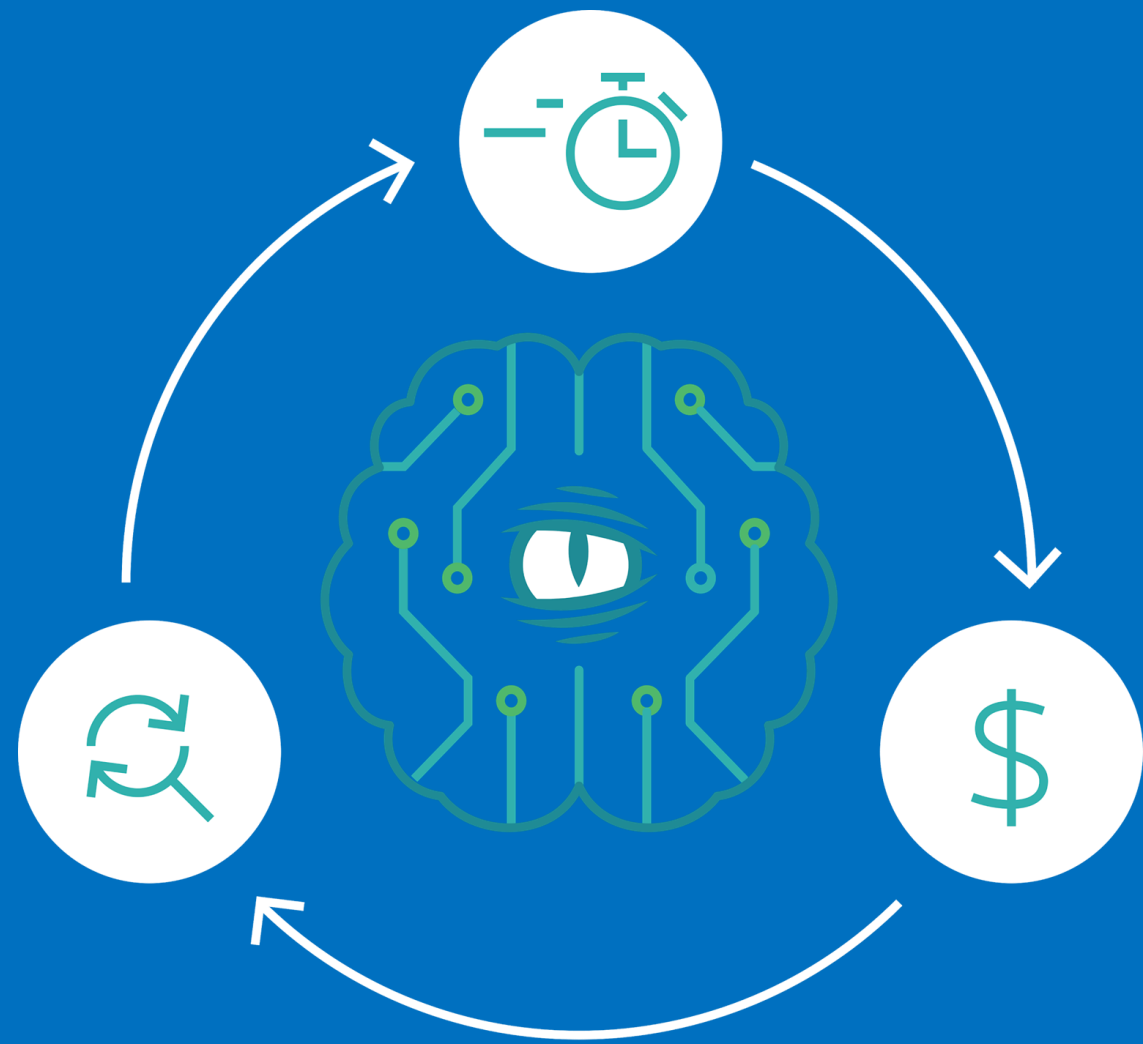
- × Hundreds of dollars / hour
- + Deep Analysis
- × Several months
- × Including PII



Install Anti-Virus/MTD/MDM

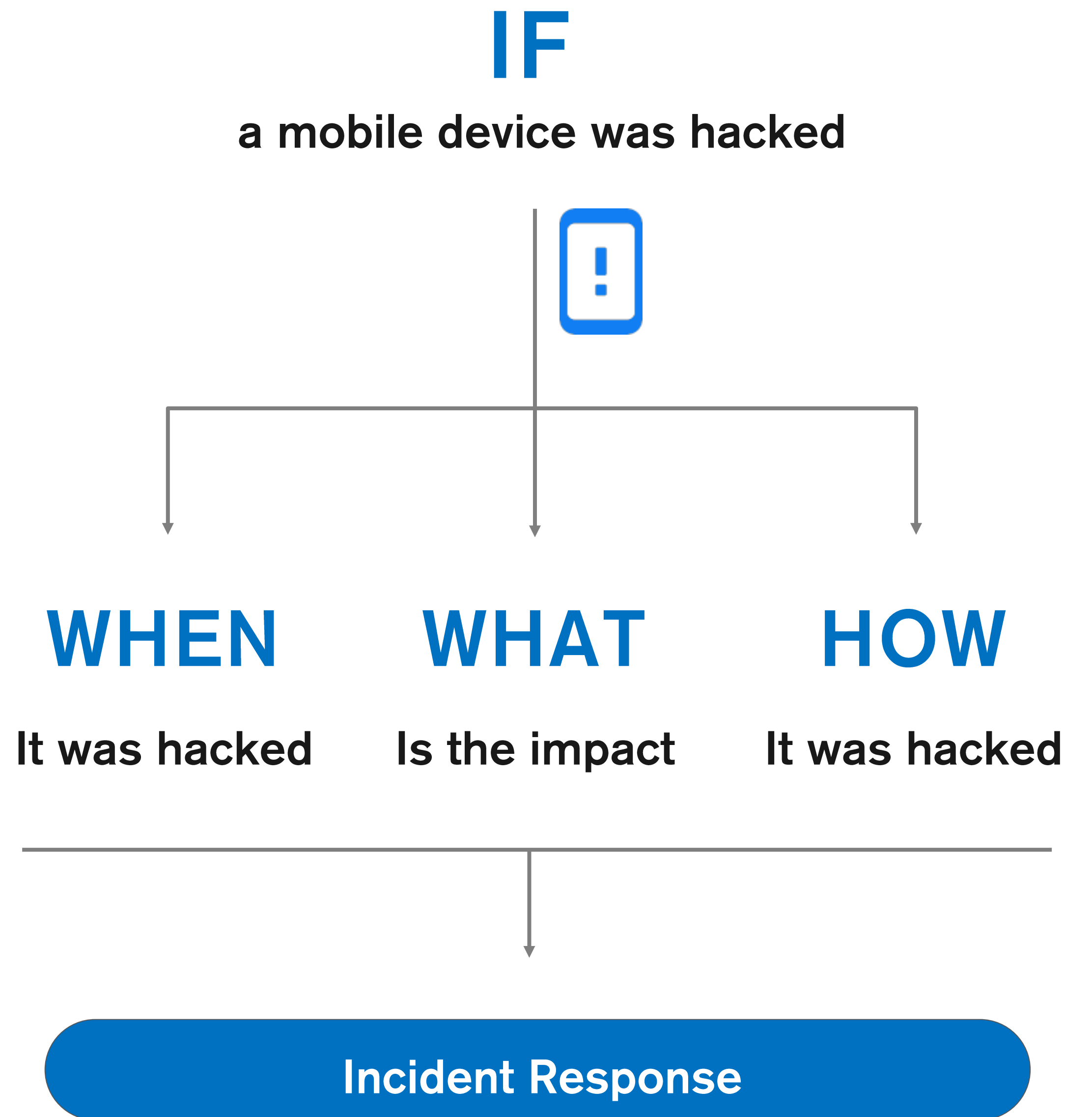
- × Limited access
- + Fast
- × Rely on other tools for a complete investigation

Now - ZecOps Mobile DFIR



Use ZecOps for Mobile to perform deep analysis and get immediate results

- + Deep Analysis
- + Instant Results
- + Agent-less
- + Affordable



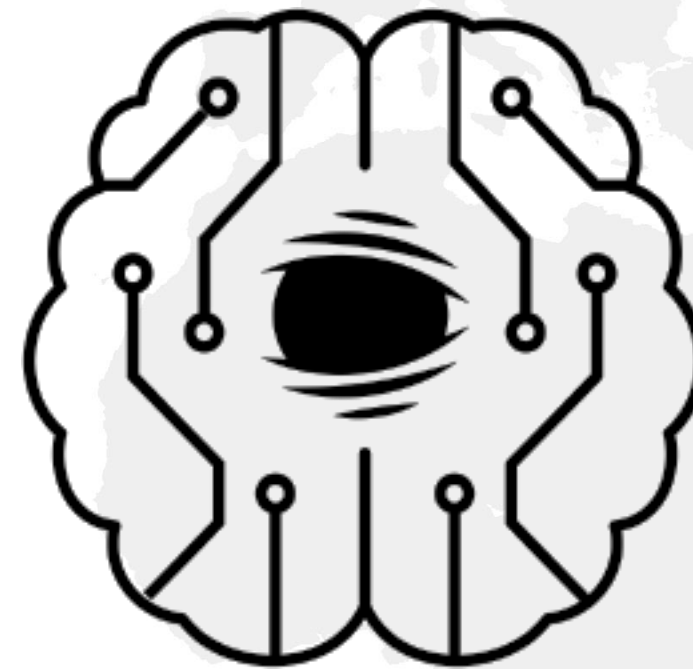
How it works



Mobile Devices

Smartphones / Tablets

*No agent required



Instant Analysis

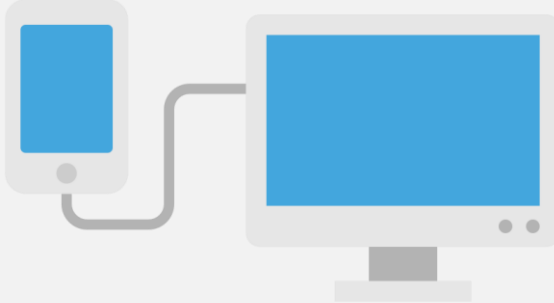
Cloud / On Premises



Incident Response

IF / WHEN / HOW / WHAT

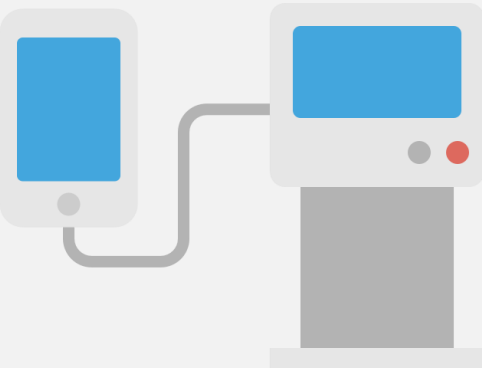
Deployment and Inspection Methods



Computer with application



Computer collector (runs in background)



Kiosk



Ingestion of 3rd party extraction-tools (e.g. Cellebrite/Greyshift/Checkm8)



Collection and Analysis

It only take up to 5 minutes to collect and analyze device logs with Agent-less ZecOps for Mobile

Privacy Friendly



ZecOps does not access PII to perform analysis

We collect for analysis: ✓

Crash logs

Stackshots / spindumps

IPS files

System diagnostics

WiFi manager logs

Processes & threads

Installed Apps

App Store logs

We don't collect: ✗

Passwords

Photos / Videos

Text Messages








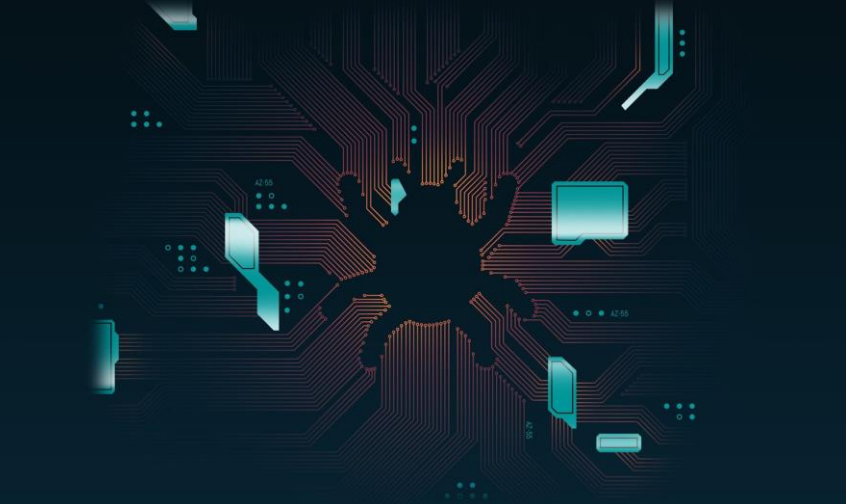
Contacts

Call data
















Browser History

Data in Applications

Sample of Attacks We Discovered

	<p>ATTACK NAME MailDemon</p> <p>VULNERABLE OS iOS 3+</p>	<p>TARGETS World Powers</p> <p>STATUS Patched</p>	<p>IMPACT Remote Compromise</p> <p>MEDIA COVERAGE 100+ Articles in 2020</p> <p>  REUTERS     </p>	
	<p>ATTACK NAME The Al-Jazeera Incidents</p>	<p>TARGETS Journalists</p>	<p>IMPACT Remote and Local Attacks</p>	<p>RESOURCES [link]</p>
	<p>ATTACK NAME Content-filter LPE</p>	<p>TARGETS Fortune 500</p>	<p>IMPACT Local Attacks</p>	<p>RESOURCES [link]</p>

Market Analysis: Cyber Security for Mobile

	ZecOps	Cellebrite / Greyshift	MDM / MTD / AV	Consultant firm
Deployment type	Agent-less	Agent-less	Agent	Agent-less
Advanced Attacks Discovery				
Instant analysis results				
Digital Forensics and Incident Response (DFIR)				
No access to private user-data			Partial	
Data extraction	Partial			

Pricing Model

Phase 1:

- Unlimited checks per year
- \$2,500 per device /per year

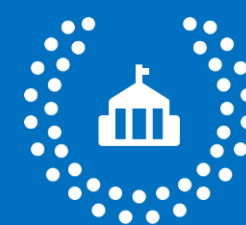
IF



Phase 2:

- Deep Analysis
- Price TBD and per case

“ZecOps for Mobile is the only available tool that provides the capability to extract, deliver, and analyze the mobile device logs for signs of compromise or malicious activity.”



DEPARTMENT OF STATE