RSACONFERENCE2013

CORPORATE ESPIONAGE VIA MOBILE COMPROMISE

Andrew Hoog
viaForensics

Session ID: END-F41

Session Classification: Intermediate

In 1955, the KGB designed the ultimate espionage device, though impossible to build with technology of the era…

… it is now pervasive

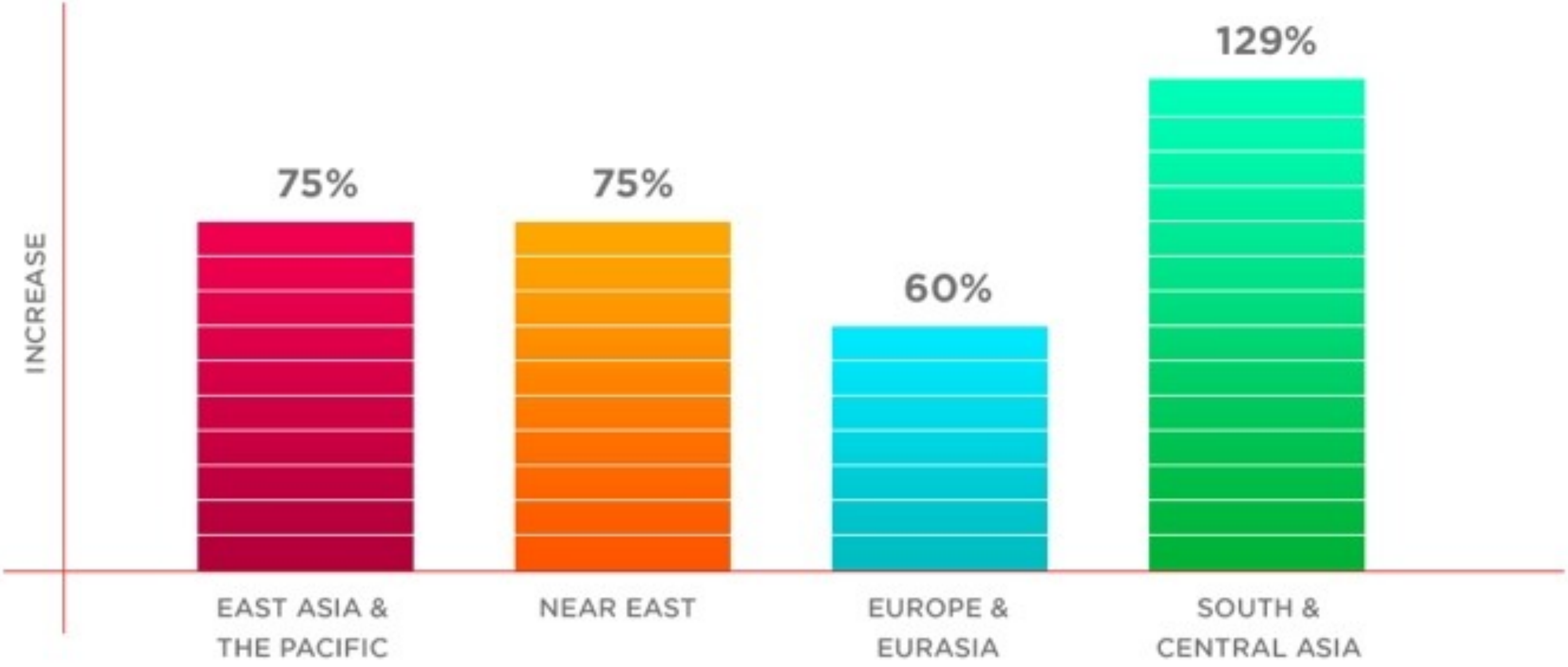
- Flexible means to gather intelligence
- Remotely accessible and updateable
- Possesses sophisticated sensors
- Goes anywhere, does not attract attention
- And targets readily carry it with them

Corporate Espionage

- Threat of sensitive data, processes, relationships to influence competitive advantage
- Increasingly perpetrated via cyber

DSS on targeting of U.S.

- Targeting of U.S. technologies is **constant** and **unwavering**
- 75% increase overall from FY10



FBI Counterintelligence

- “economic espionage losses to the American economy total more that $13 billion”

BYOD: Breaking Your Own Defenses?

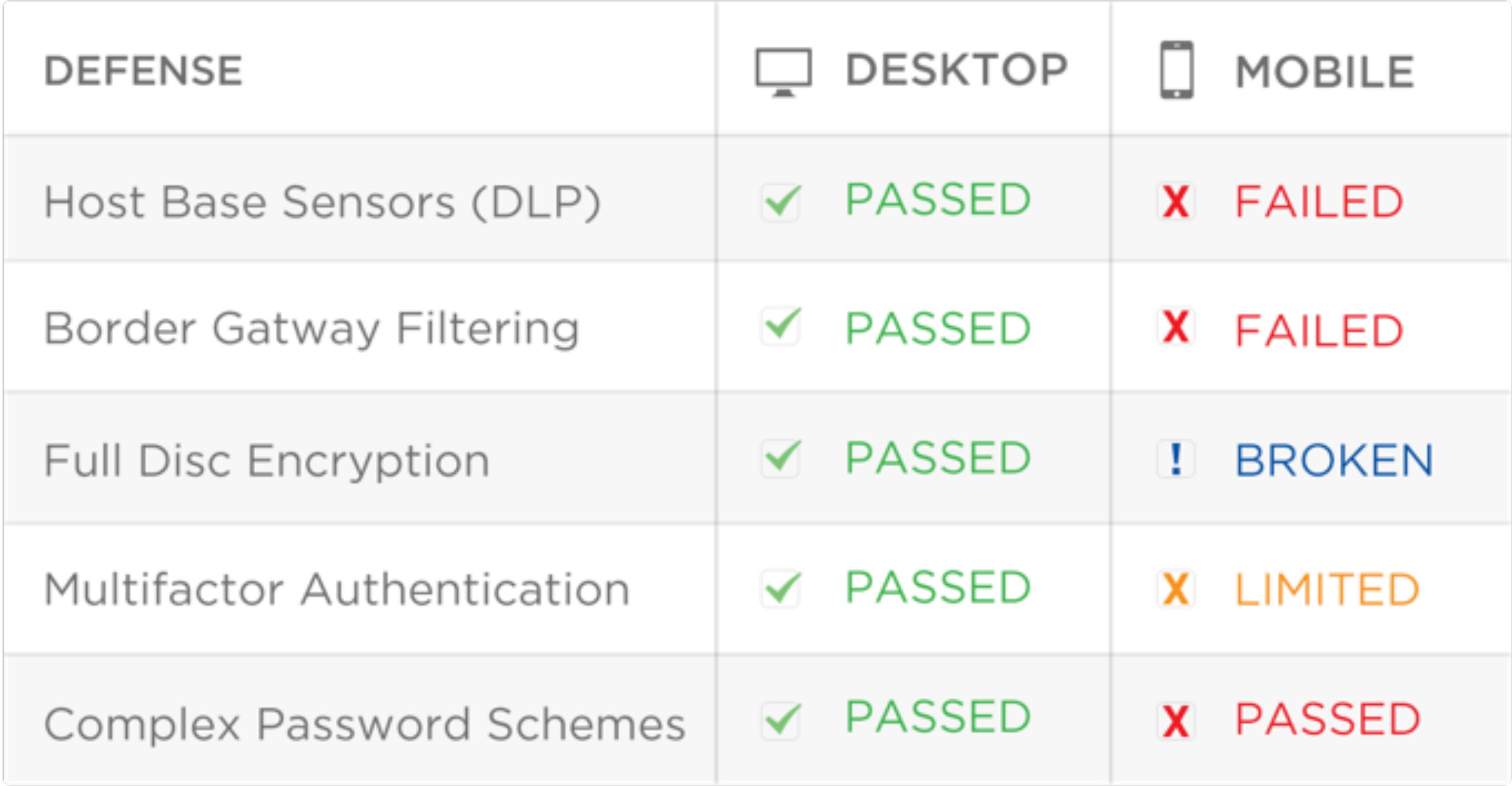
Enter mobile

- Operates on both sides of the firewall
- Stores sensitive corporate and person data
- Mostly outside the control of IT/Security (BYOD)
- Runs loads of untested code, of unknown origin

Attacker Perspective

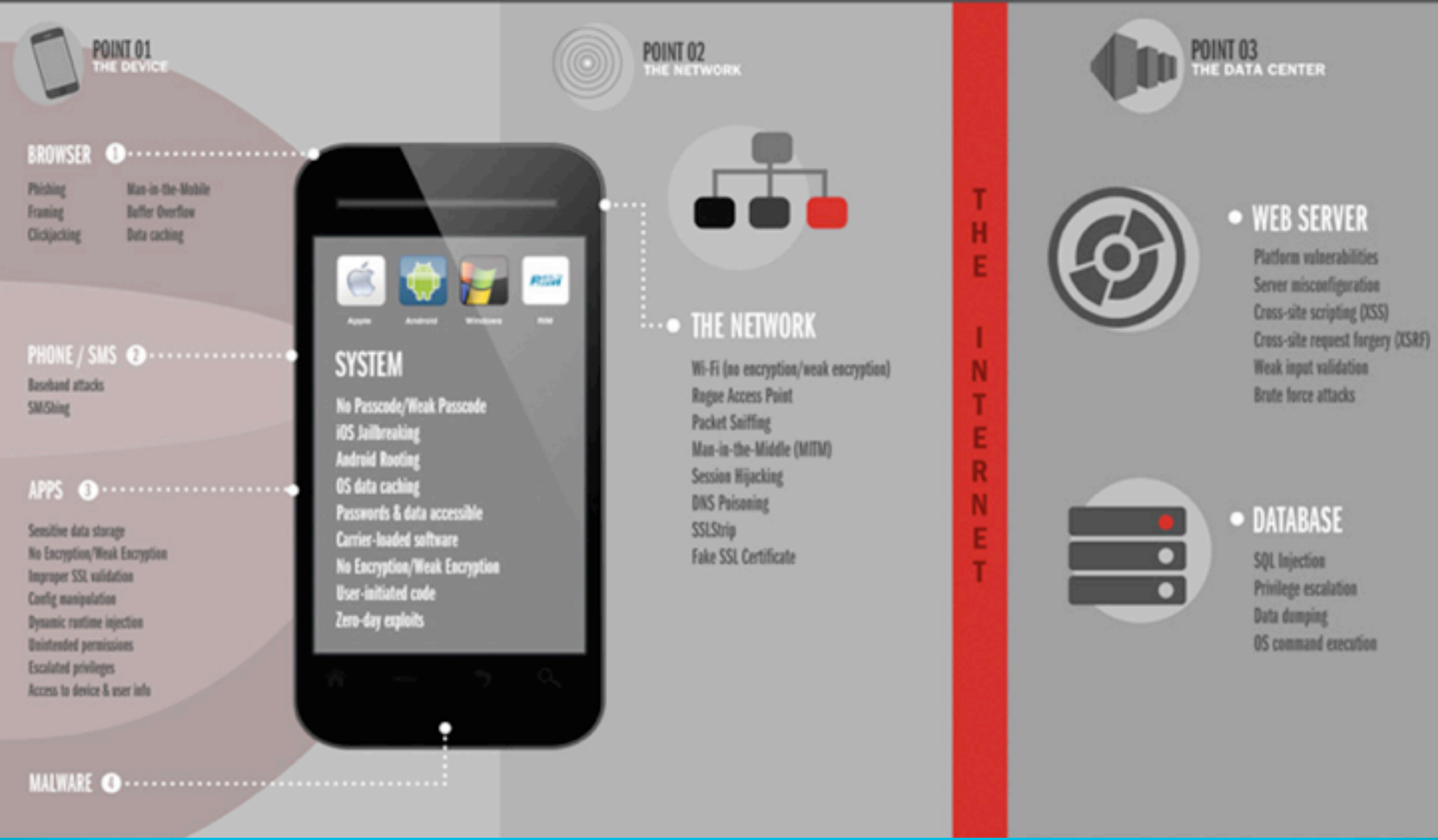
- Convenient channel to distribute attacks (app store)
- Data rich, diverse channels for data exfil
- Limited virus scan/malware detection
- New technologies outpacing traditional security controls
- Re-programmable hardware

Corporate Defenses vs. Mobile



DEFENSE	DESKTOP	MOBILE
Host Base Sensors (DLP)	✓ PASSED	X FAILED
Border Gatway Filtering	✓ PASSED	X FAILED
Full Disc Encryption	✓ PASSED	! BROKEN
Multifactor Authentication	✓ PASSED	X LIMITED
Complex Password Schemes	✓ PASSED	X PASSED

ANATOMY OF A MOBILE ATTACK



POINT 01
THE DEVICE

BROWSER 1

- Phishing
- Framing
- Clickjacking
- Man-in-the-Mobile
- Buffer Overflow
- Data caching

PHONE / SMS 2

- Baseband attacks
- SMiShing

APPS 3

- Sensitive data storage
- No Encryption/Weak Encryption
- Improper SSL validation
- Config manipulation
- Dynamic runtime injection
- Unintended permissions
- Escalated privileges
- Access to device & user info

MALWARE 4

SYSTEM

- No Passcode/Weak Passcode
- iOS Jailbreaking
- Android Rooting
- OS data caching
- Passwords & data accessible
- Carrier-loaded software
- No Encryption/Weak Encryption
- User-initiated code
- Zero-day exploits

POINT 02
THE NETWORK

THE NETWORK

- Wi-Fi (no encryption/weak encryption)
- Rogue Access Point
- Packet Sniffing
- Man-in-the-Middle (MITM)
- Session Hijacking
- DNS Poisoning
- SSLStrip
- Fake SSL Certificate

POINT 03
THE DATA CENTER

WEB SERVER

- Platform vulnerabilities
- Server misconfiguration
- Cross-site scripting (XSS)
- Cross-site request forgery (XSRF)
- Weak input validation
- Brute force attacks

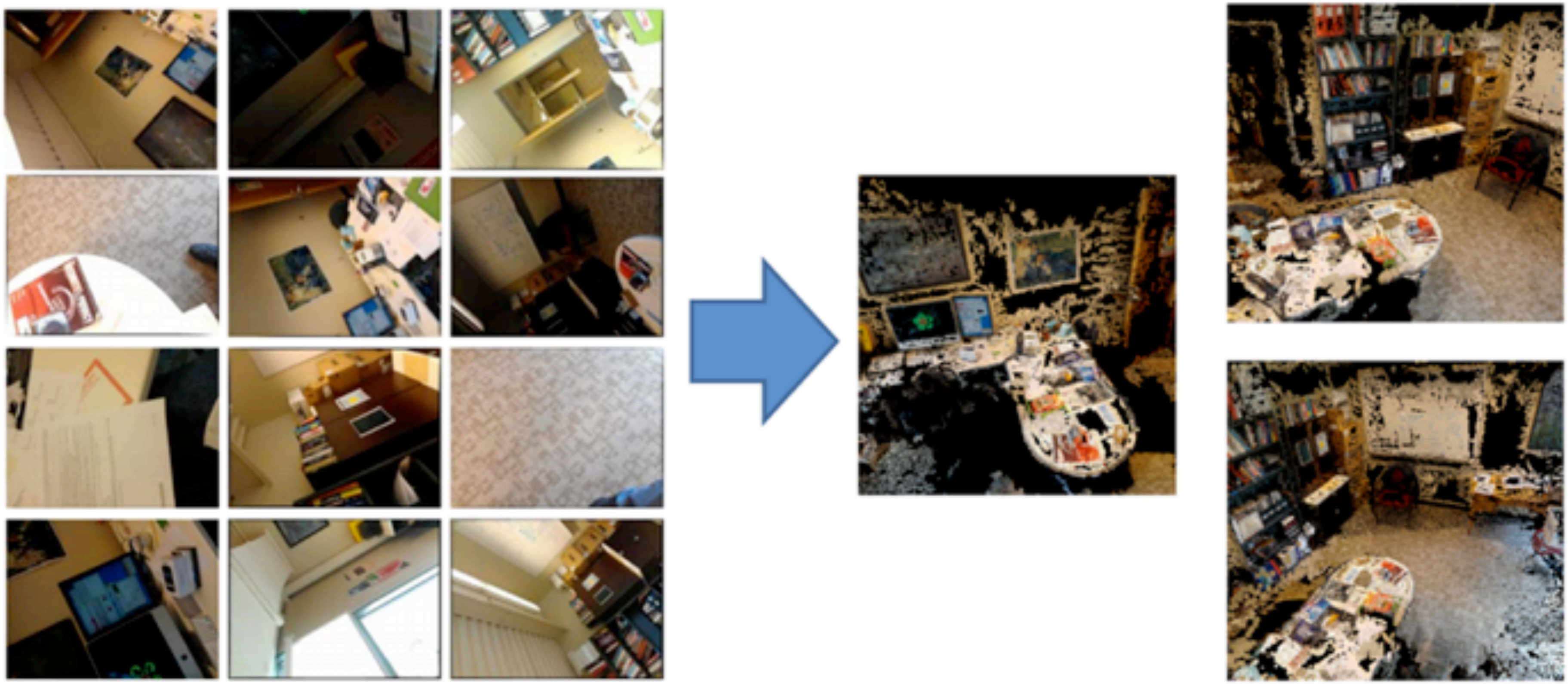
DATABASE

- SQL Injection
- Privilege escalation
- Data dumping
- OS command execution

Bypassing traditional defenses

Circumvent traditional corporate security controls

Hijack the camera



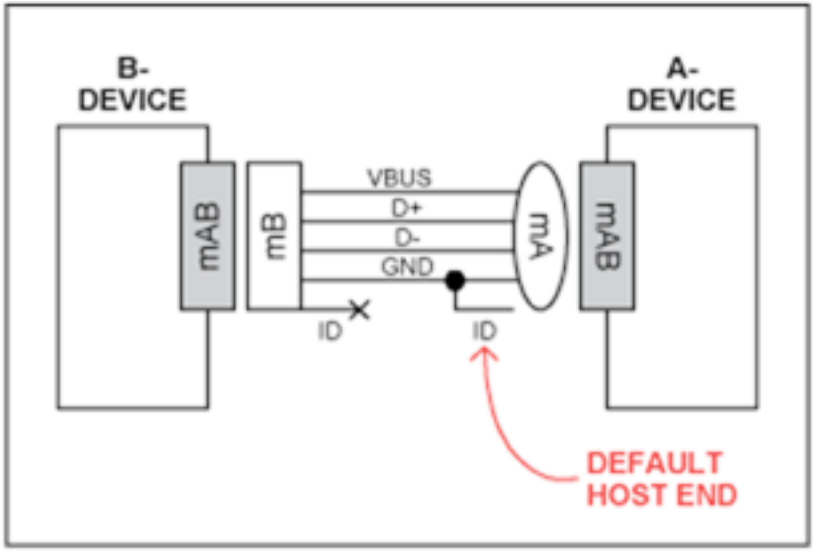
PlaceRaider “visual malware”
R. Templeman et al

Mobile Compromise via HID

- Exploit reprogrammable USB hardware of a mobile device to morph on command
- Circumvents all traditional defenses
- Gives attacker hands on keyboard
- Exploit and expand easily

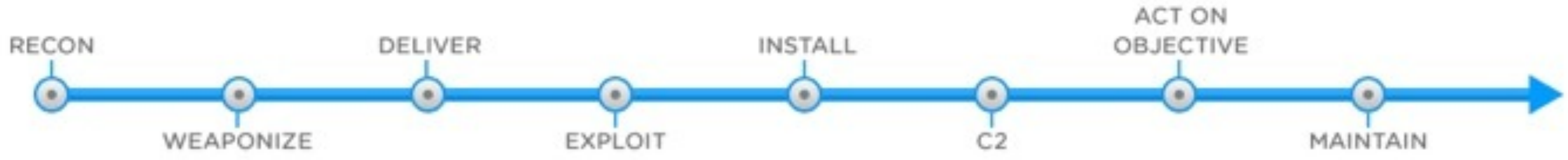
Reprogrammable HW

- Host Negotiation Protocol: OTG dual-role device can operate either as a host or peripheral.
- Used to provide features such as ADB, Mass Storage, MTP, tether, docking station on Android
- USB OTG + Linux Gadgete framework = Arbitrary USB device

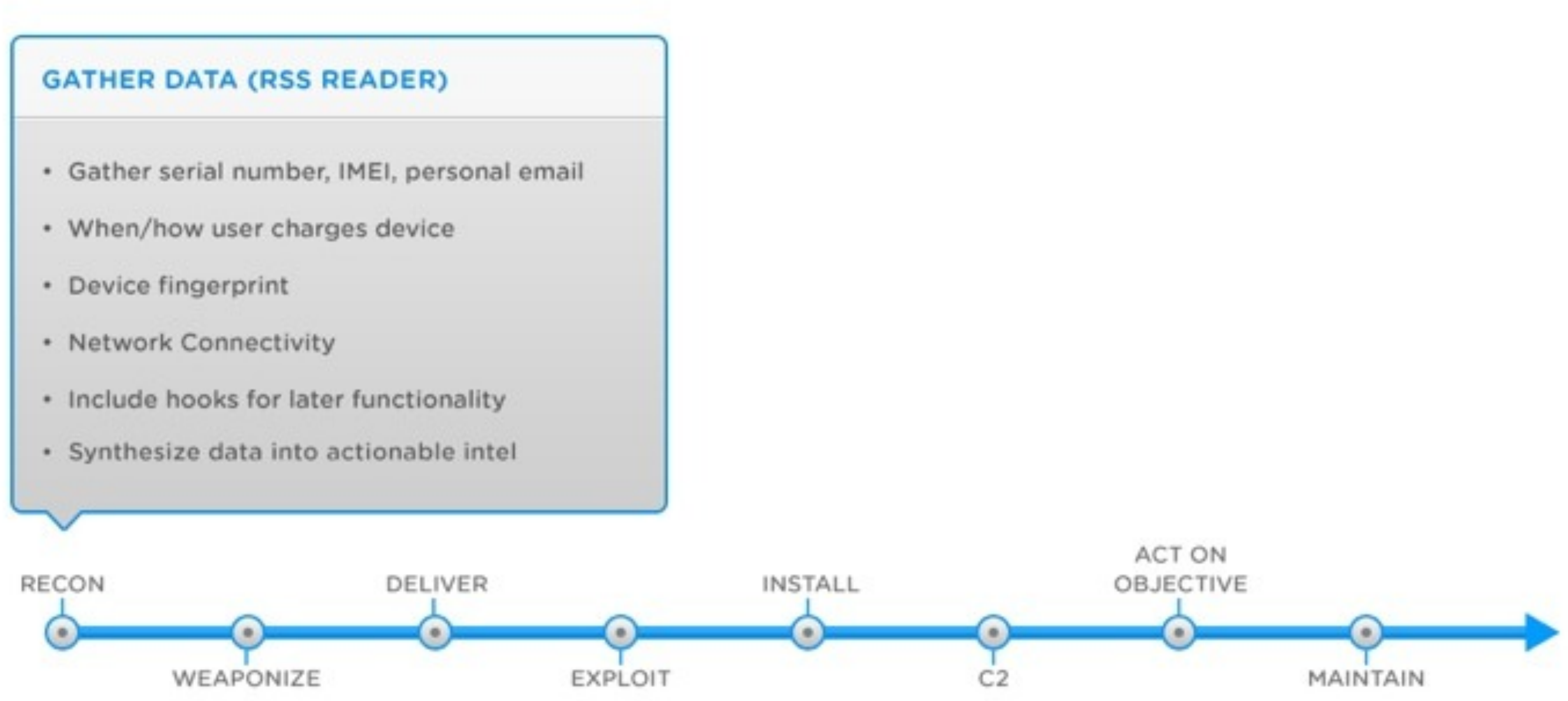


Mobile Kill Chain

- Similar to traditional kill-chain
  - More complex because of mobility
- Must account for interaction with other systems and modalities
  - home vs. work
  - VPN vs. not
  - multi-factor authentication



Mobile Kill Chain



GATHER DATA (RSS READER)

- Gather serial number, IMEI, personal email
- When/how user charges device
- Device fingerprint
- Network Connectivity
- Include hooks for later functionality
- Synthesize data into actionable intel

RECON

WEAPONIZE

DELIVER

EXPLOIT

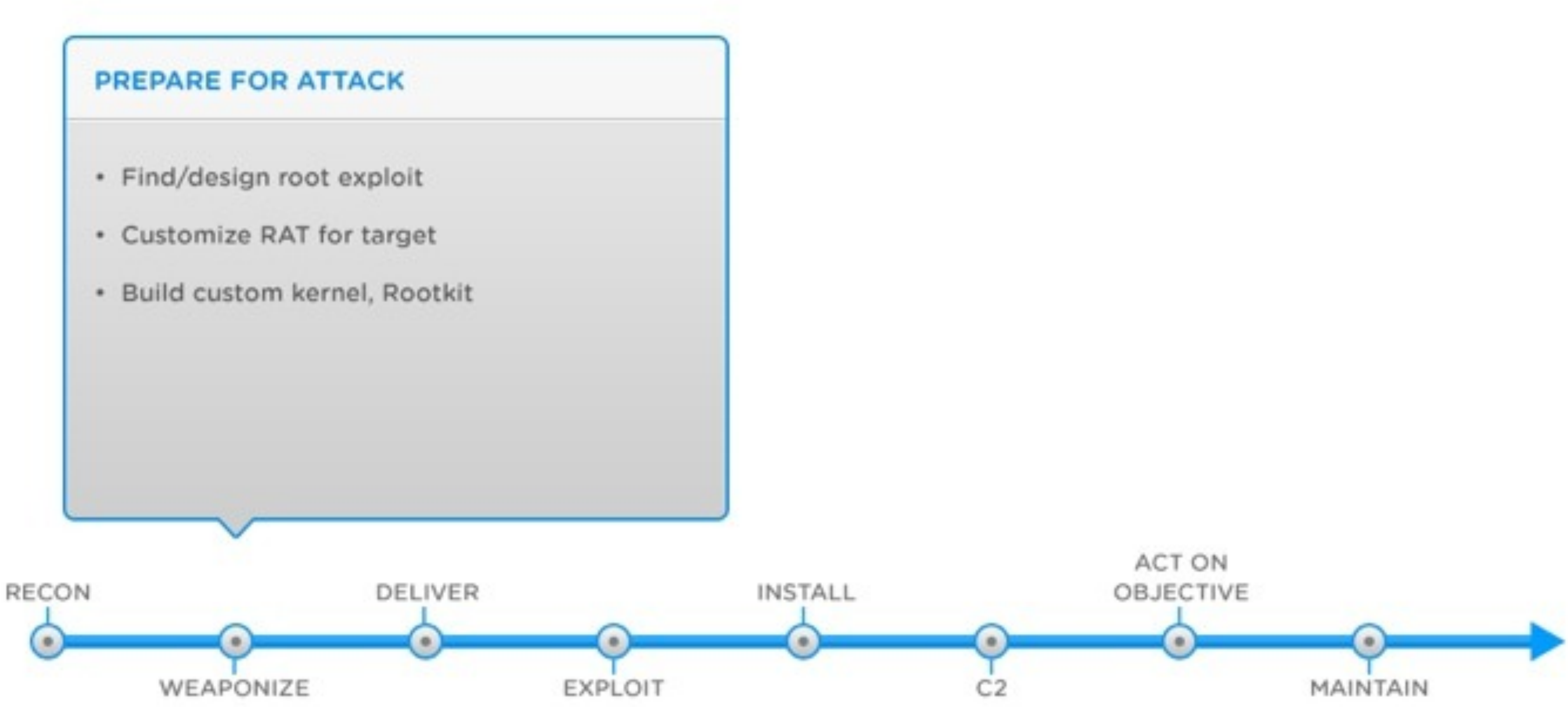
INSTALL

C2

ACT ON OBJECTIVE

MAINTAIN

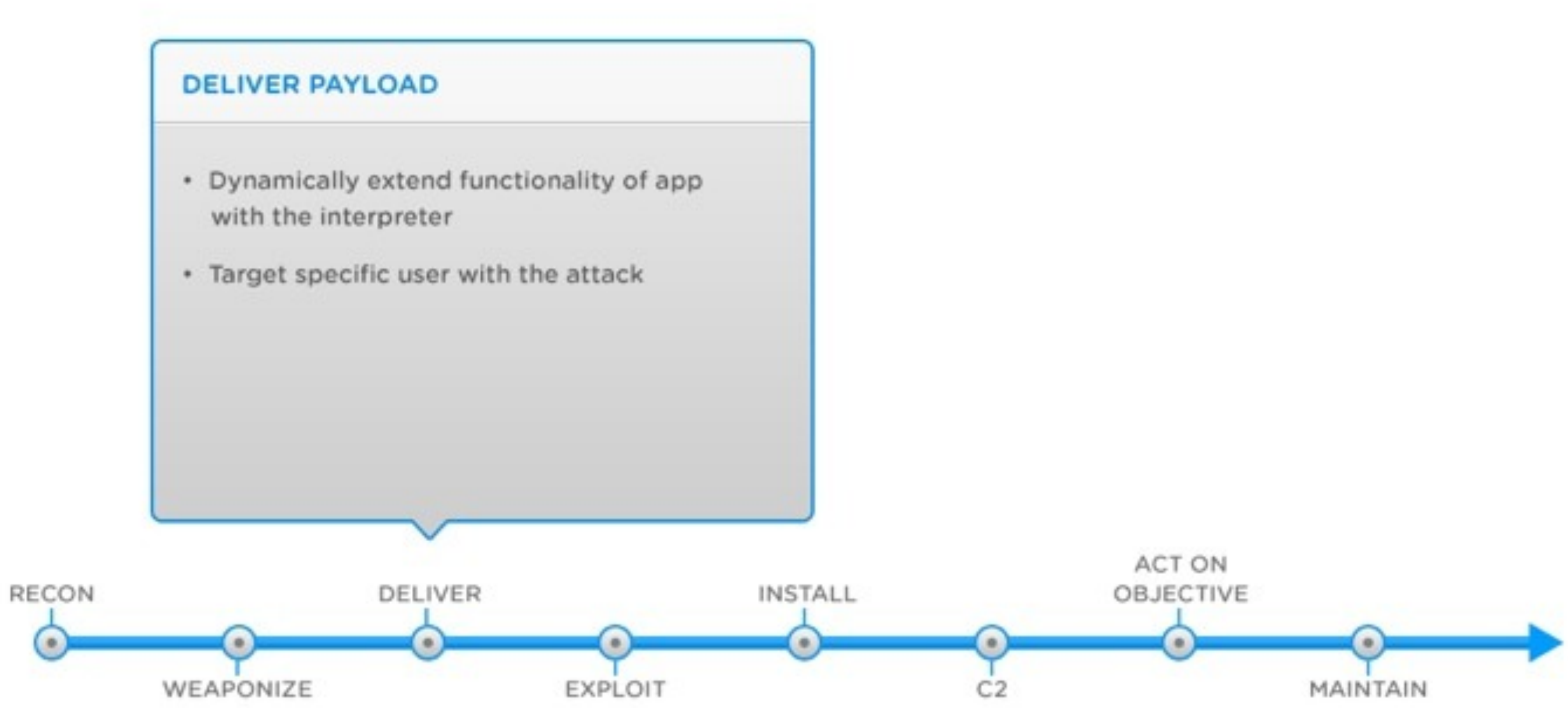
Mobile Kill Chain



PREPARE FOR ATTACK

- Find/design root exploit
- Customize RAT for target
- Build custom kernel, Rootkit

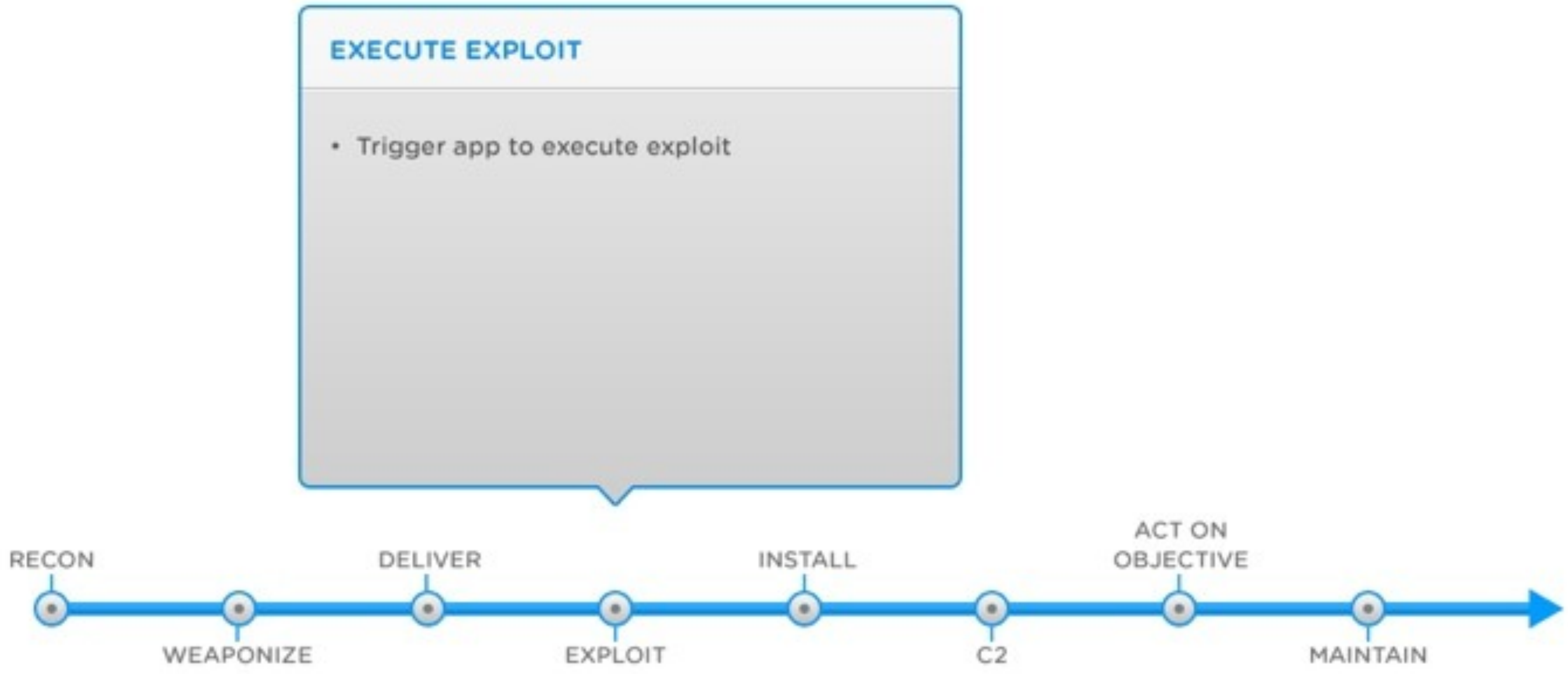
Mobile Kill Chain



DELIVER PAYLOAD

- Dynamically extend functionality of app with the interpreter
- Target specific user with the attack

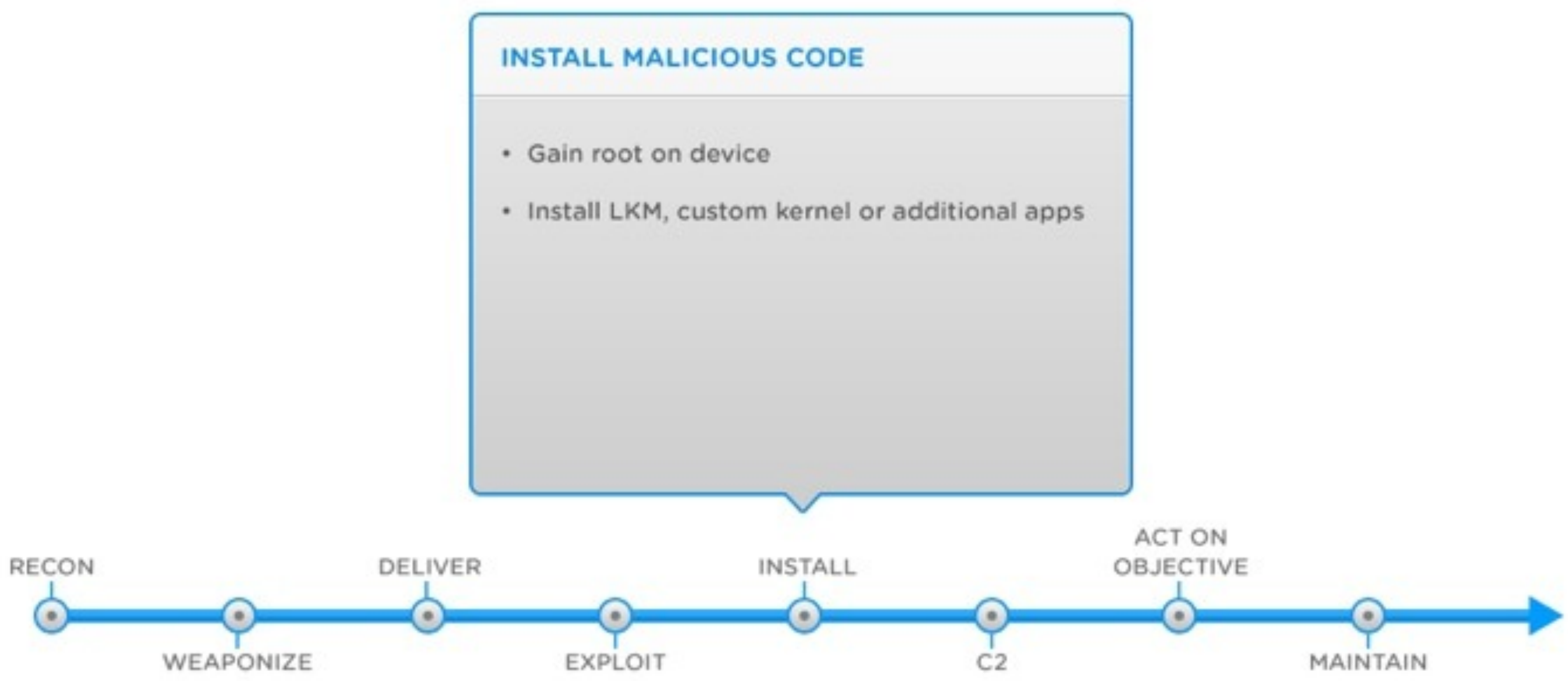
Mobile Kill Chain



EXECUTE EXPLOIT

- Trigger app to execute exploit

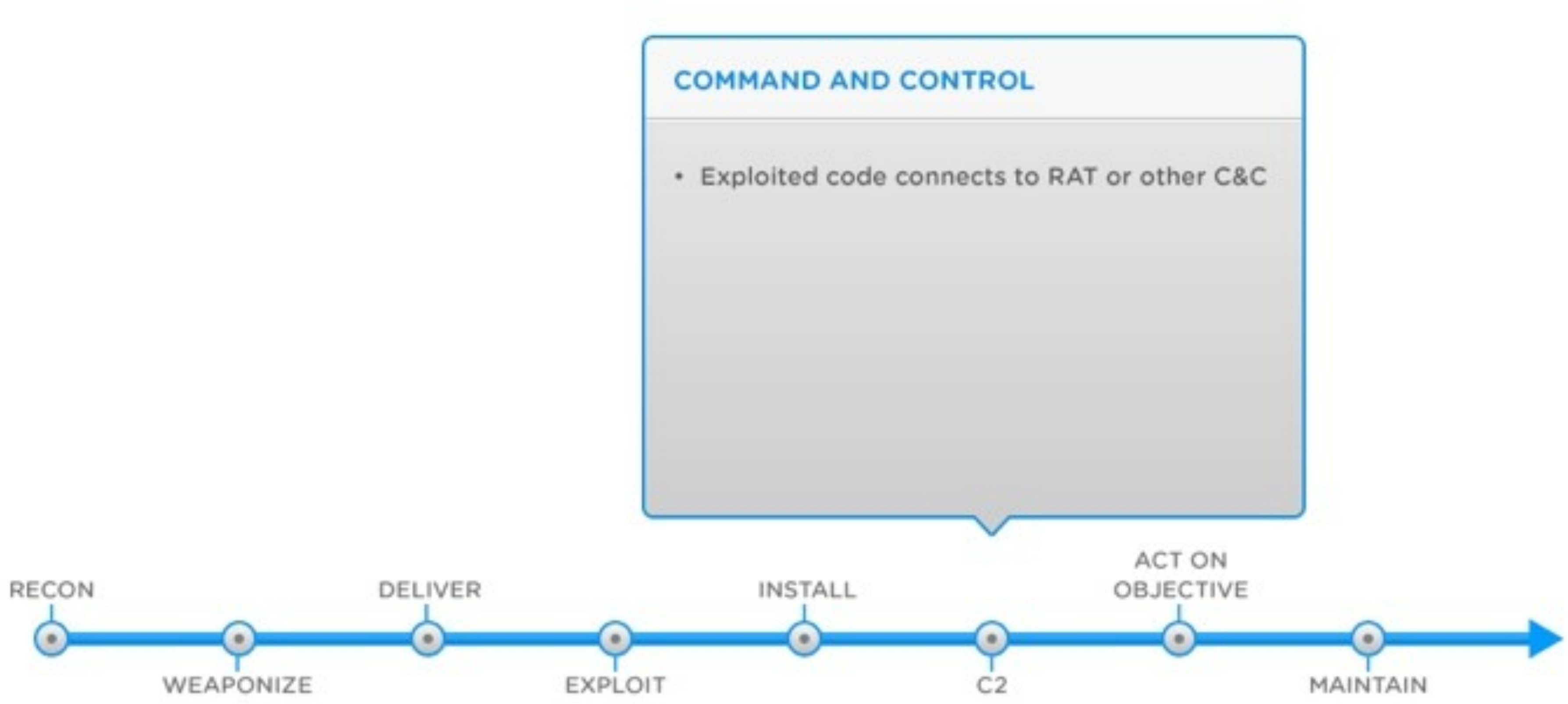
Mobile Kill Chain



INSTALL MALICIOUS CODE

- Gain root on device
- Install LKM, custom kernel or additional apps

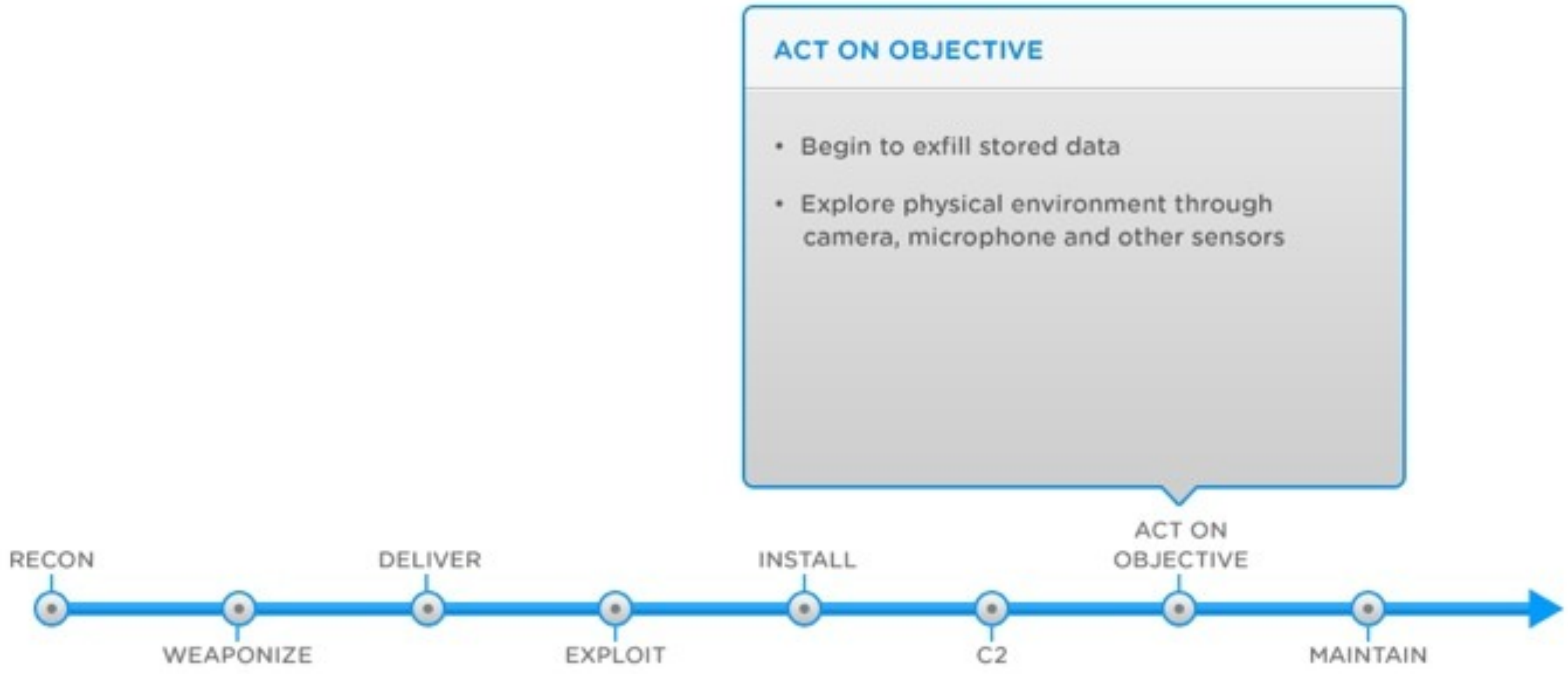
Mobile Kill Chain



COMMAND AND CONTROL

- Exploited code connects to RAT or other C&C

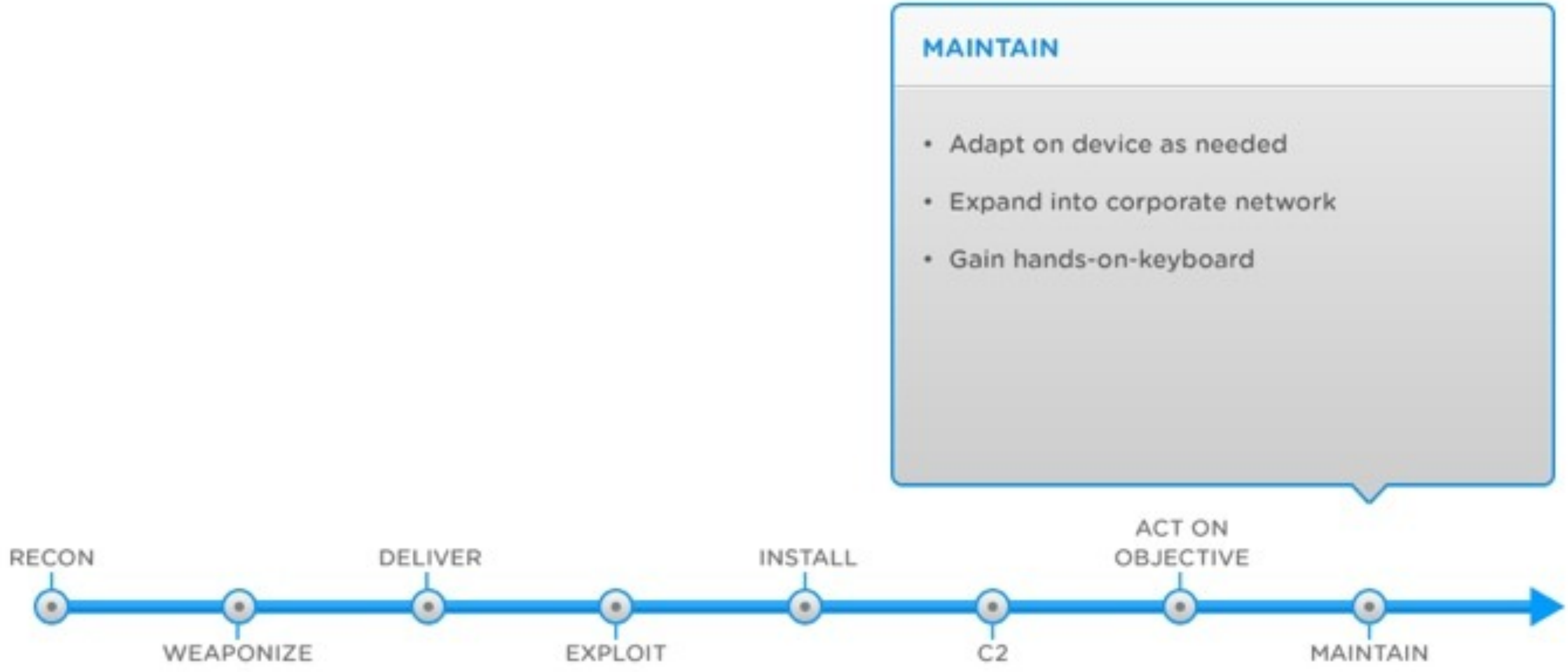
Mobile Kill Chain



ACT ON OBJECTIVE

- Begin to exfill stored data
- Explore physical environment through camera, microphone and other sensors

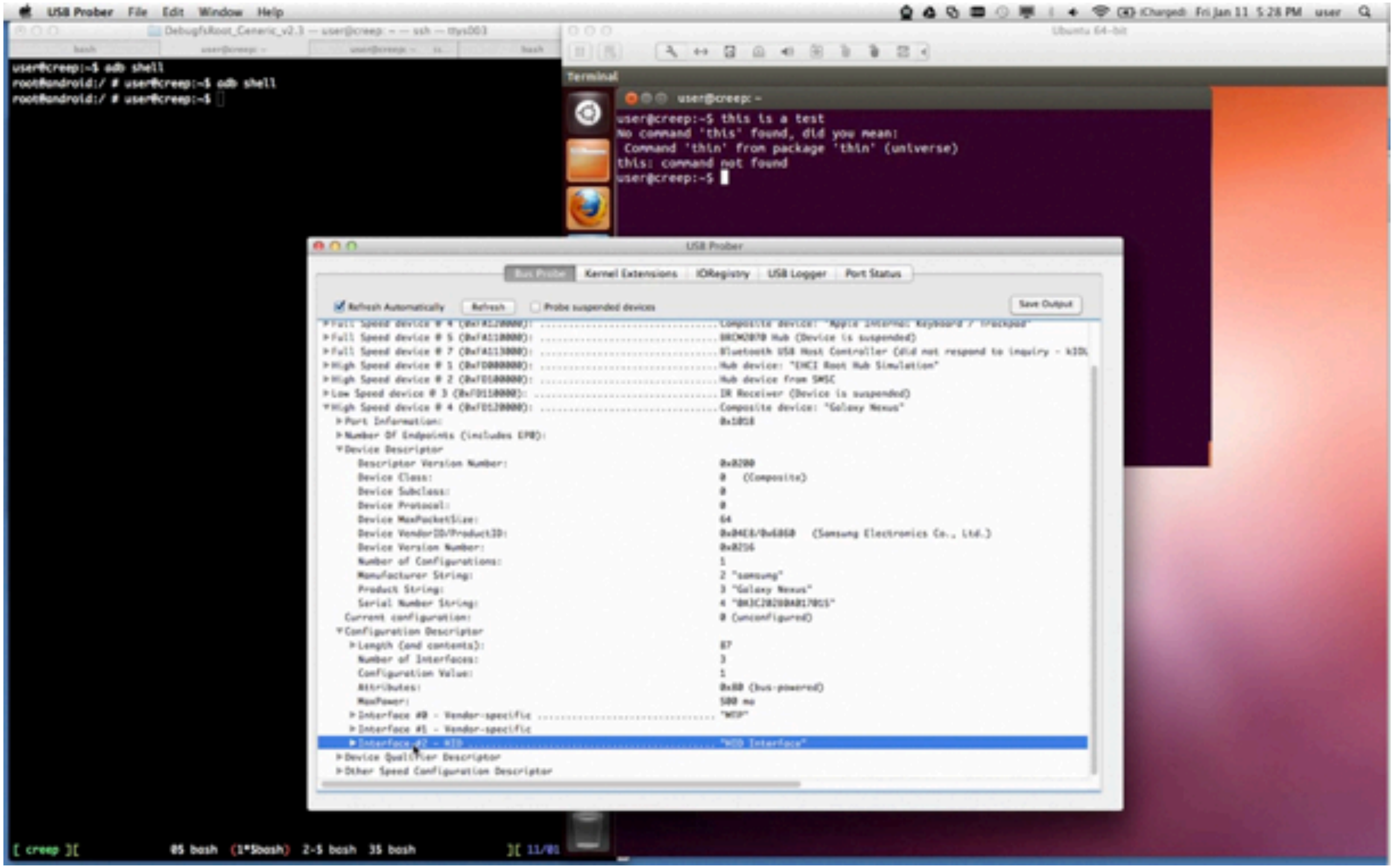
Mobile Kill Chain



MAINTAIN

- Adapt on device as needed
- Expand into corporate network
- Gain hands-on-keyboard

Mobile Compromise via HID



```
user@creep:~$ adb shell
root@android:/ # user@creep:~$ adb shell
root@android:/ # user@creep:~$
```

```
[ creep ][      0$ bash  (1*$bash)  2-$ bash  3$ bash        ][ 11/01
```

```
user@creep:~$ this is a test
No command 'this' found, did you mean:
 Command 'thin' from package 'thin' (universe)
this: command not found
user@creep:~$
```

☑ Refresh Automatically   □ Probe suspended devices

```
▸Full Speed device # 4 (0xFA120000): ..............................Composite device: "Apple Internal Keyboard / Trackpad"
▸Full Speed device # 5 (0xFA110000): ..............................BRCM2070 Hub (Device is suspended)
▸Full Speed device # 7 (0xFA113000): ..............................Bluetooth USB Host Controller (did not respond to inquiry - kIOU
▸High Speed device # 1 (0xFD000000): ..............................Hub device: "EHCI Root Hub Simulation"
▸High Speed device # 2 (0xFD100000): ..............................Hub device from SMSC
▸Low Speed device # 3 (0xFD110000): ...............................IR Receiver (Device is suspended)
▾High Speed device # 4 (0xFD120000): ..............................Composite device: "Galaxy Nexus"
  ▸Port Information:                                               0x1018
  ▸Number Of Endpoints (includes EP0):
  ▾Device Descriptor
     Descriptor Version Number:                                    0x0200
     Device Class:                                                 0   (Composite)
     Device Subclass:                                              0
     Device Protocol:                                              0
     Device MaxPacketSize:                                         64
     Device VendorID/ProductID:                                    0x04E8/0x6860   (Samsung Electronics Co., Ltd.)
     Device Version Number:                                        0x0216
     Number of Configurations:                                     1
     Manufacturer String:                                          2 "samsung"
     Product String:                                               3 "Galaxy Nexus"
     Serial Number String:                                         4 "0A3C2020A017015"
    Current configuration:                                         0 (unconfigured)
  ▾Configuration Descriptor
    ▸Length (and contents):                                        87
     Number of Interfaces:                                         3
     Configuration Value:                                          1
     Attributes:                                                   0x80 (bus-powered)
     MaxPower:                                                     500 ma
    ▸Interface #0 - Vendor-specific ...............................  "MTP"
    ▸Interface #1 - Vendor-specific
    ▸Interface #2 - HID ...........................................  "HID Interface"
  ▸Device Qualifier Descriptor
  ▸Other Speed Configuration Descriptor
```

Recommendations

- Proactive monitoring of mobile devices and app
- Improve DLP software to detect new keyboards
- Develop mobile kill chain
- Treat mobile an attack platform
- Incorporate mobile broadly into defensive posture

Questions Please!

@viaforensics

☎ 312-878-1100

✉ ahoog@viaforensics.com