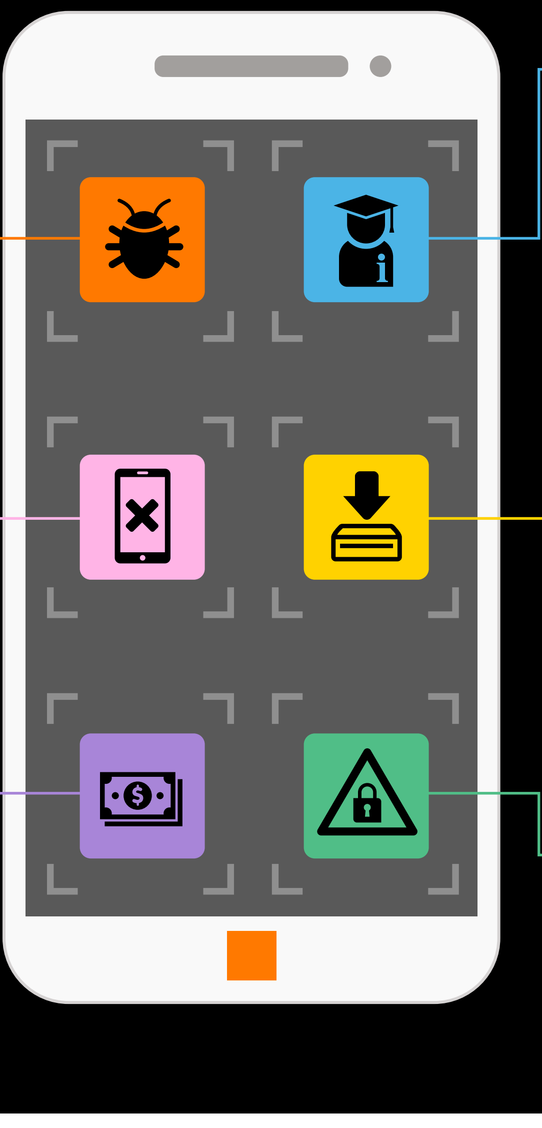
Security

Plugging the mobile security gap

Securing the mobile enterprise

Could mobile devices be the weakest link in today's enterprise? According to a 2017 survey of IT professional, 20 percent of companies have experienced a mobile security breach[1].



3% of mobile devices in the average Global 2000 enterprise are infected by malware[2]

54 mobile malware attacks per business on average per year[3]

$26.4m economic risk of mobile data breach[4]

65% of security experts doubt their organizations can prevent a device breach[5]

1.6m malicious installation packages were detected in the third quarter of 2017[6]

253% increase of ransomware on mobile devices in 1H 2017[7]

Enterprise secrets at risk

Attacks on mobile devices are evolving quickly. Attackers can exploit mobile devices to steal confidential data from the enterprise.

Hackers can eavesdrop by taking over the device's microphone and camera

A single device compromised with malware like GhostCtrl can spy on closed-door meetings by using the microphone and camera

Criminals can steal enterprise data by accessing emails, texts and call logs

Discovering a breach takes an average of 99 days globally[8]. Once detected, the damage has already been done

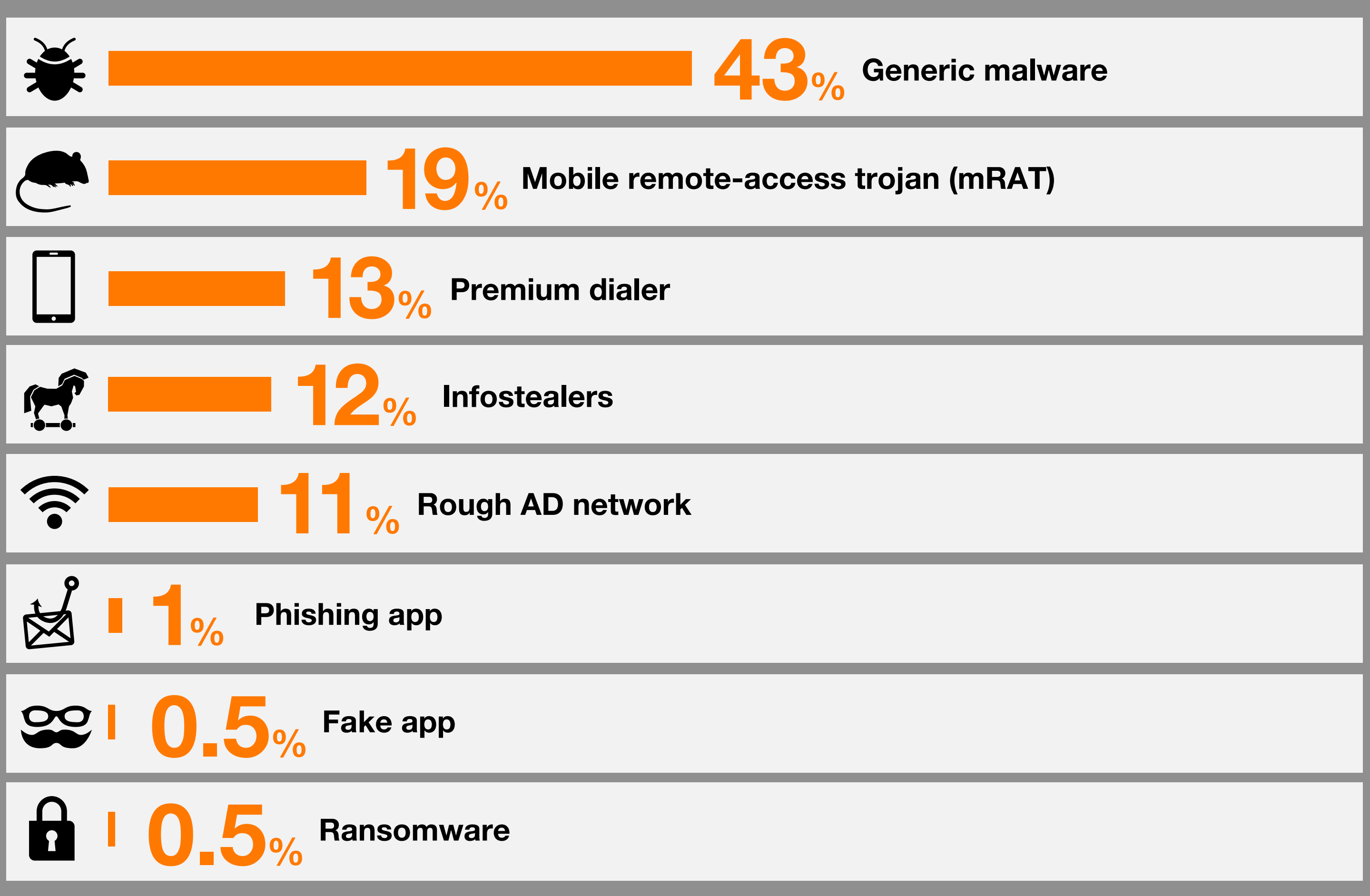
Crooks can compromise secure containers to extract application data

User activity outside of the enterprise perimeter can be compromised allowing hackers to steal passwords and access secure areas

Many infection vectors

Mobile malware takes many different forms, and you need to protect yourself against all of them not to fall victim to attack.

Mobile threats detected by Checkpoint[9]:



Identify your weaknesses

Mobile attacks on enterprises come from three main areas: malware-infected apps, network attacks and device vulnerabilities.

DressCode

2m users downloaded it. Allows the attacker to get access to private communications or files[10]

Apps can be riddled with malware and expose the device to attack.

Man-in-the-middle

89% of users experienced at least one MITM attack over Wi-Fi, which directs devices towards malicious sites[11]

Network attacks, such as wireless interception or captive portals trick devices to compromise them.

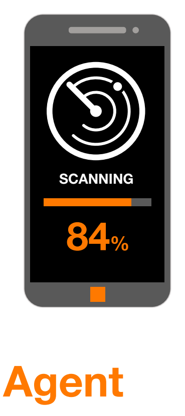
Rooted or jailbroken device

75% enterprises tested had at least one connected to their corporate network[12]

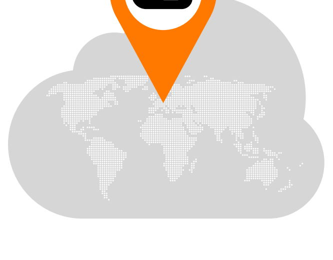
Unpatched devices are vulnerable to attack, particularly if they are rooted or jailbroken.

Manning the defenses

Despite these threats many organizations are still unprepared. Mobile Threat Protection (MTP) is the key to protecting your mobile estate.

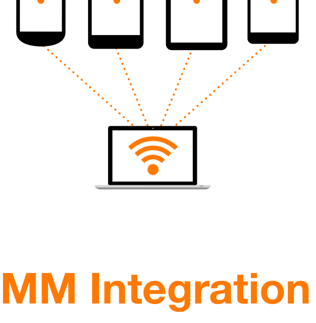


Agent
Run in the background, low consumption, CPU/battery



Cloud platform
Cloud platform, global knowledge base, European location

Admin portal
Deep visibility of the threat, dashboard and configuration



EMM Integration
Visibility and total fleet control to proactively remove threats

To find out more about MTP from Orange Business Services visit:
https://www.orange-business.com/en/products/mobile-threat-protection

orange™ Business Services

Sources: 1. Checkpoint: Five Mobile Security Myths Debunked. 2. The Ponemon Institute: The Economic Risk of Confidential Data on Mobile Devices in the Workplace, 2016. 3. Checkpoint: Mobile Cyberattacks Impact Every Business. 4. The Ponemon Institute: The Economic Risk of Confidential Data on Mobile Devices in the Workplace, 2016. 5. Checkpoint: Mobile Cyberattacks Impact Every Business. 6. Kaspersky Lab. 7. Kaspersky Lab. 8. Mandiant M-Trends 2017. 9. Checkpoint 2016 Security Report. 10. Miercom Industry Assessment 2017. 11. Checkpoint: Mobile Cyberattacks Impact Every Business. 12. Checkpoint: Mobile Cyberattacks Impact Every Business