Check Point
SOFTWARE TECHNOLOGIES LTD

SECURITY
BEYOND THE PERIMETER

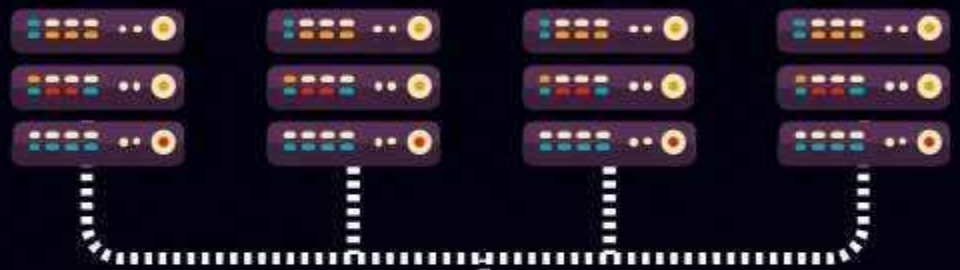
Protecting devices, Securing data

AGENDA

1. Outside your Perimeter
2. New Realities need New Protections
   - Smartphones & Tablets
   - Laptops
   - Cloud Applications
3. Importance of Zero-Day threat prevention
4. Consolidated Threat Intelligence

OUTSIDE YOUR PERIMETER

Your IT architecture has evolved – Your security must evolve as well



Business Yesterday

Business Today

Check Point
SOFTWARE TECHNOLOGIES LTD

BEYOND YOUR PERIMETER ...

Securing the perimeter was simple and highly effective.

Attackers have shifted their focus to easier targets.

Check Point
SOFTWARE TECHNOLOGIES LTD

BEYOND YOUR PERIMETER IS AN ATTACKER'S PARADISE

- Less security outside the perimeter
- Mixture of "personal" and "business" on the same device
- Employees act more carefree when not in the office
- Hackers find it easier to exploit these weaknesses

Common attack vectors used by attackers

Surfaces

LAPTOPS

E-Mail

File Share

Malicious Network

Man in the Middle

Web

Phishing

Account Take Over

SMARTPHONES & TABLETS

E-Mail

File Share

Malicious Network

Man in the Middle

Web

Phishing

Malicious Application

Account Take Over

CLOUD APPLICATIONS

E-Mail

File Share

Phishing

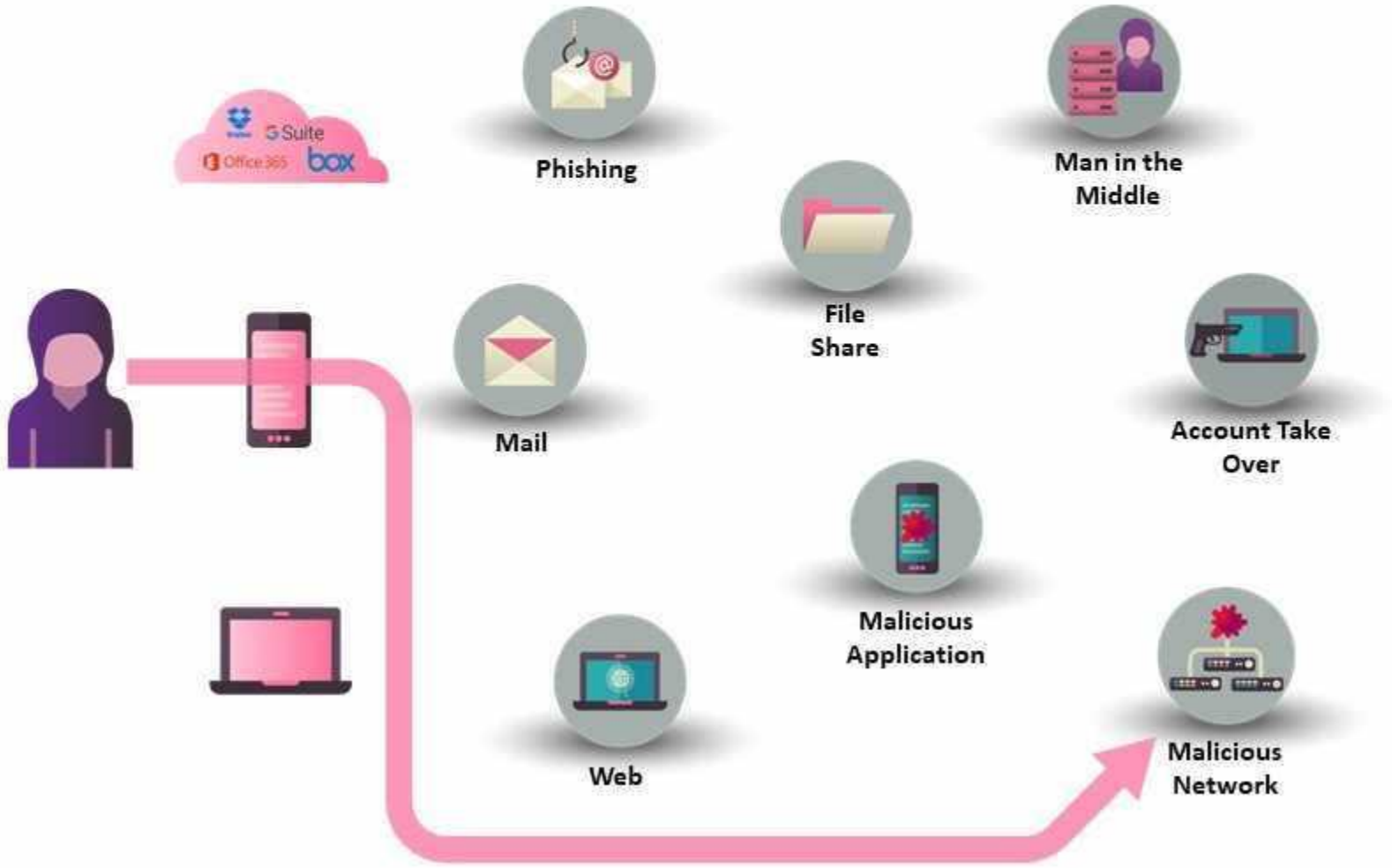
Malicious Application

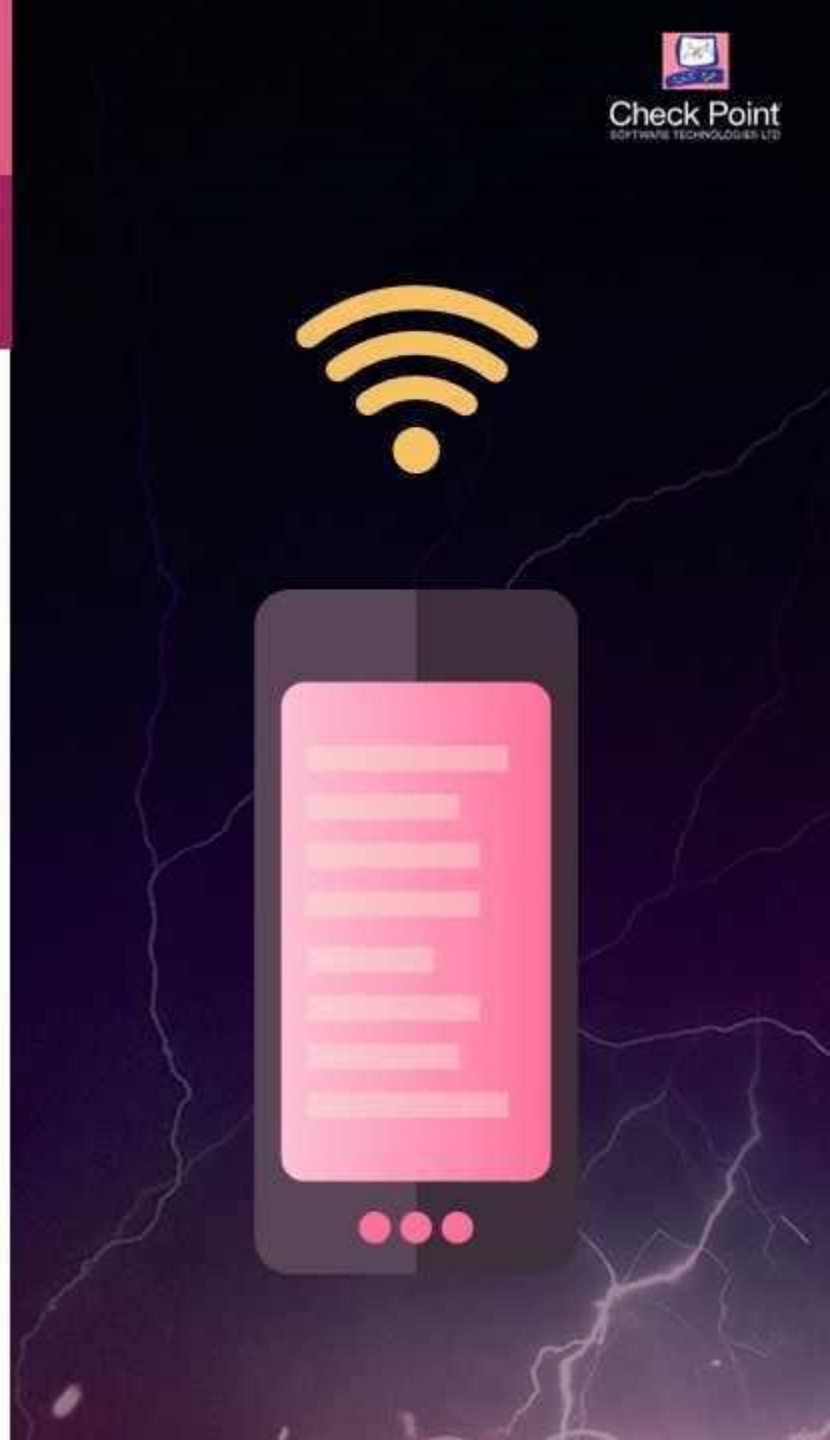
Account Take Over

TARGETED MOBILE ATTACK

Step1: Set the trap

Victim connects to a “friendly” hotspot; Or..

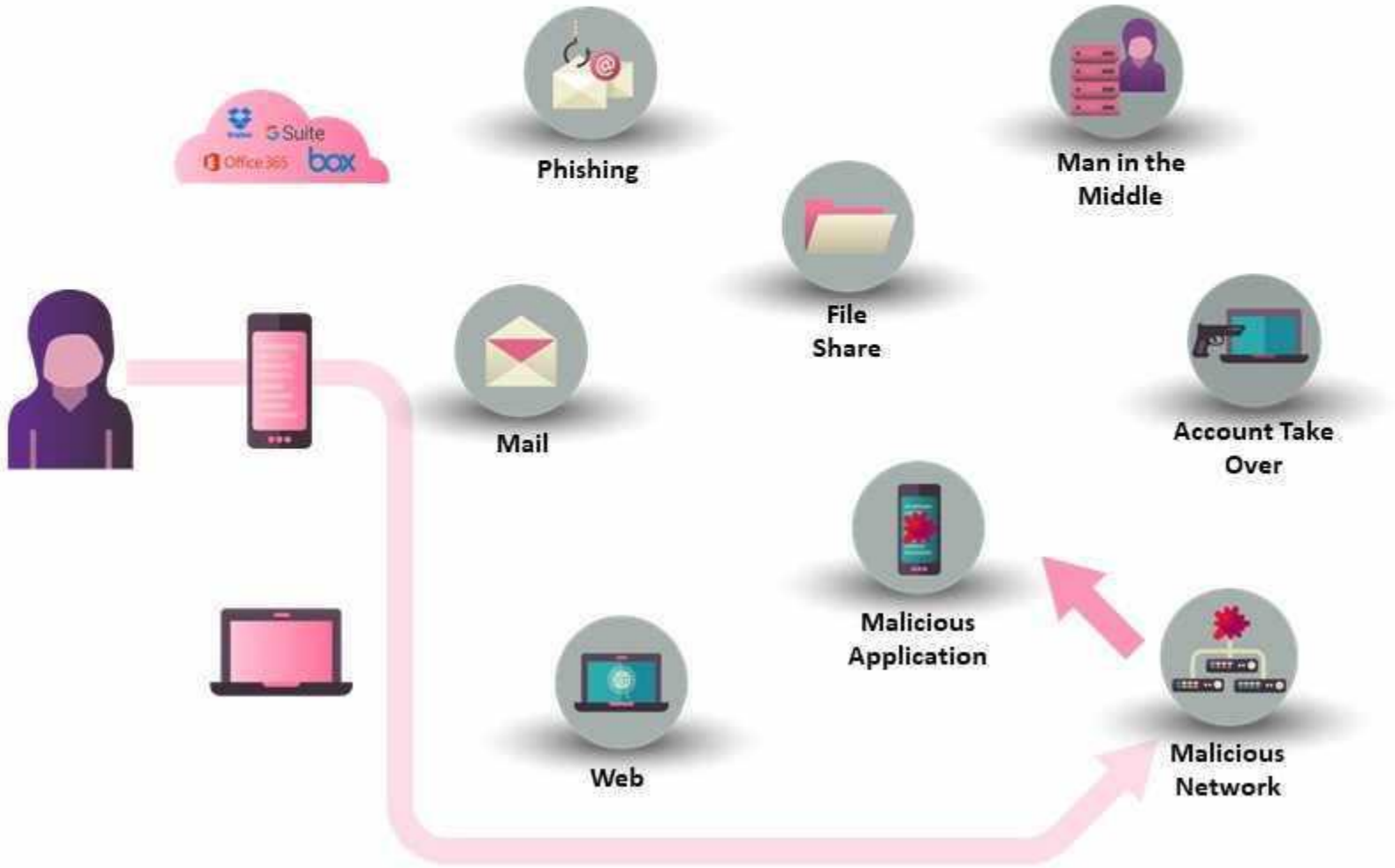




TARGETED MOBILE ATTACK

Step2: Infect your device and/or tap your network

Victim is tricked to download a “legitimate” app in order to take control over the phone



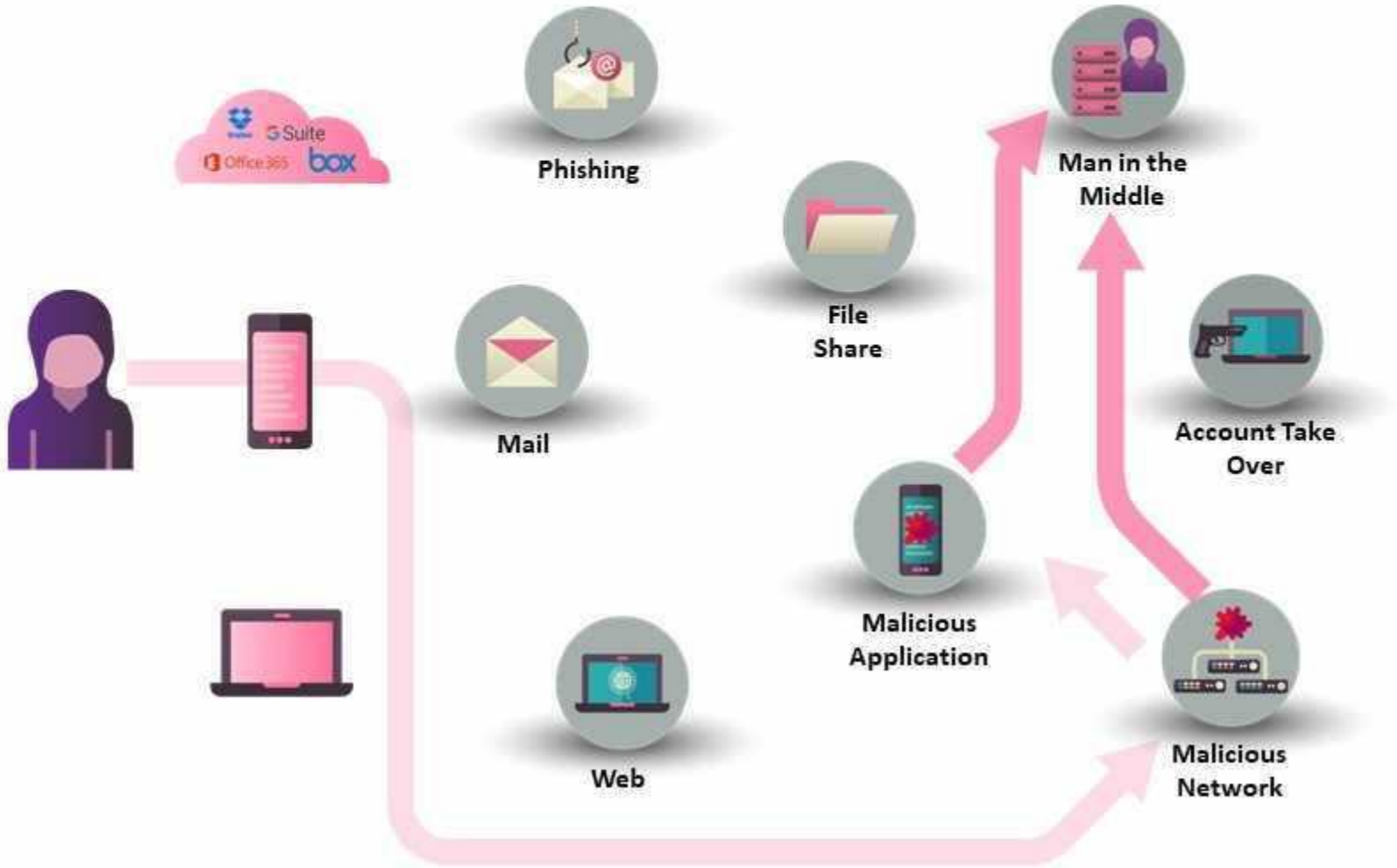
Check Point

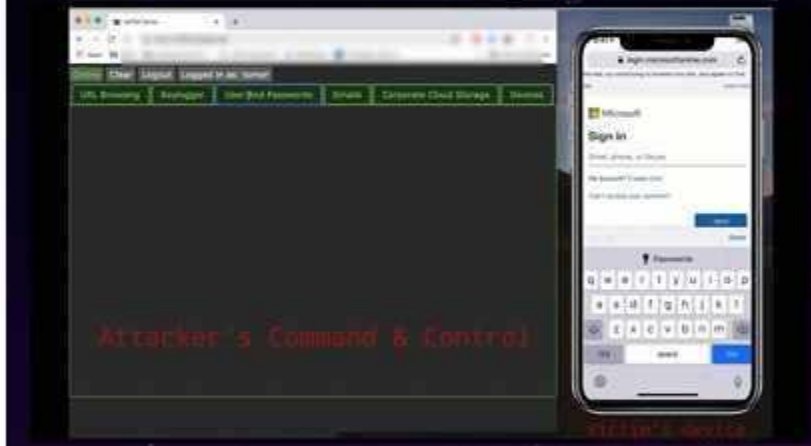
Click to Enlarge

TARGETED MOBILE ATTACK

Step 3: Collect Data

Attacker gets full remote control over the device, steals passwords, mail, identify the location and use the recorder and camera per need



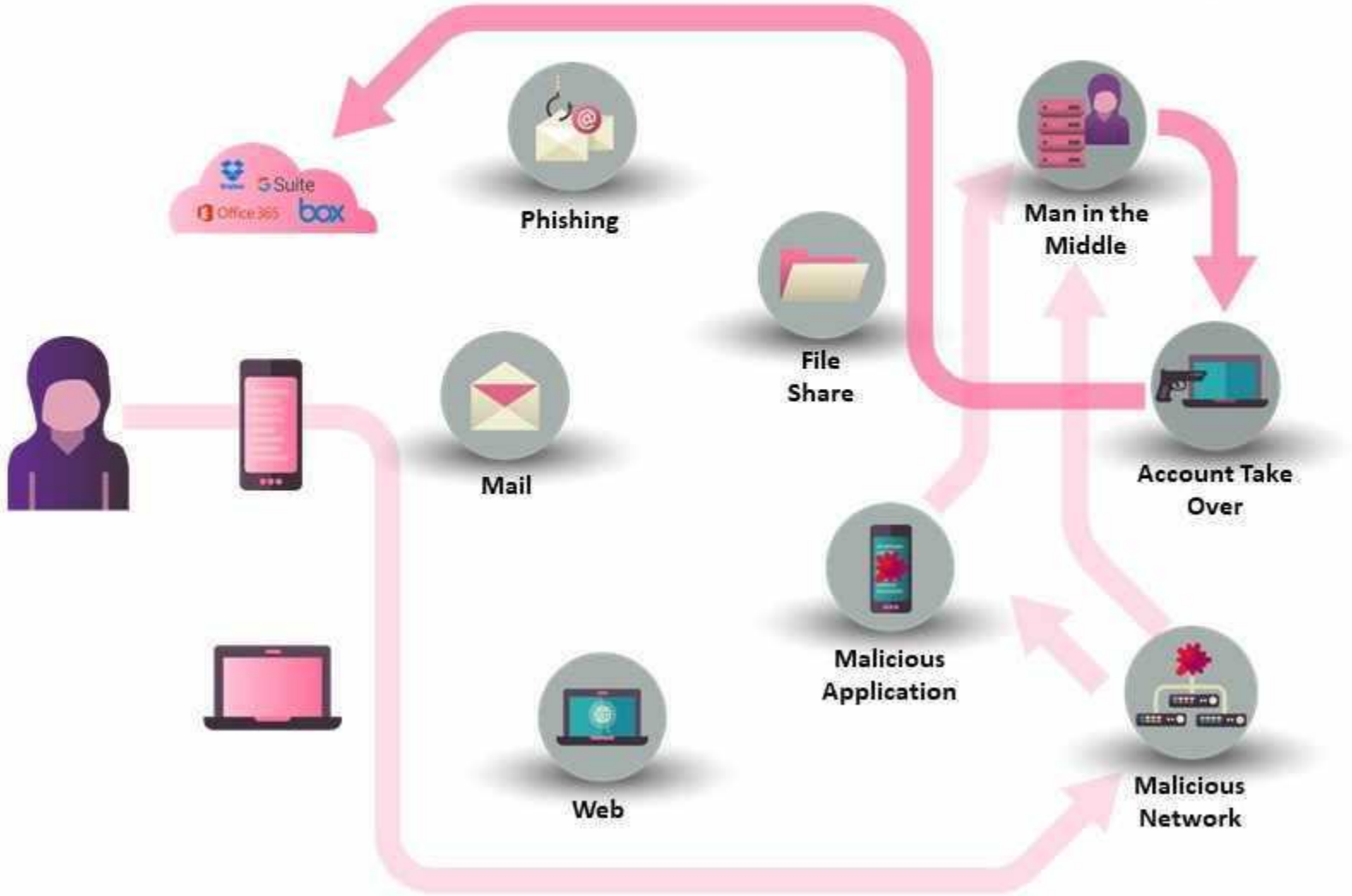


Click to Enlarge

TARGETED MOBILE ATTACK

Step 4: Create devastating damage

Attacker takes over your accounts, he has unlimited opportunities, steal private and corporate data, access your cloud apps



MULTI-VECTOR ATTACK

Step 1: Phishing scam for Account Takeover

Phishing mail requesting to update your O365 credentials

Mon 2/26/2018 10:43 AM

MO

Microsoft Office [redacted]

Password Expiration

To reply@noreply.com

'MICROSOFT OFFICE 365

Good Afternoon,

We sent this E-mail to notify you that your Password is about to expire,
Immediately your password expires, your E-mail would be locked.

To continue using your mailbox as usual, Click here

Email sent using Optus Webmail

Web

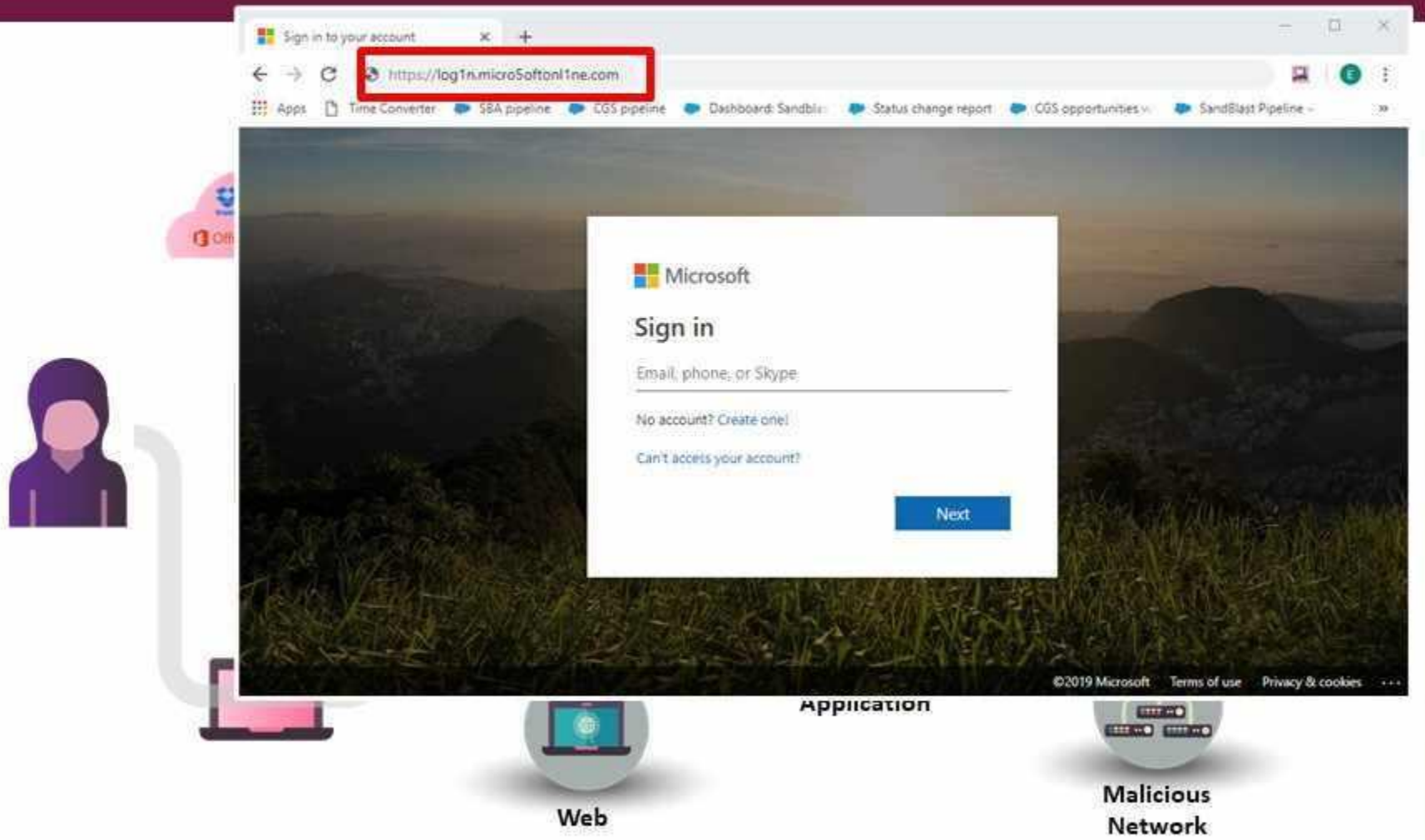
Malicious Network

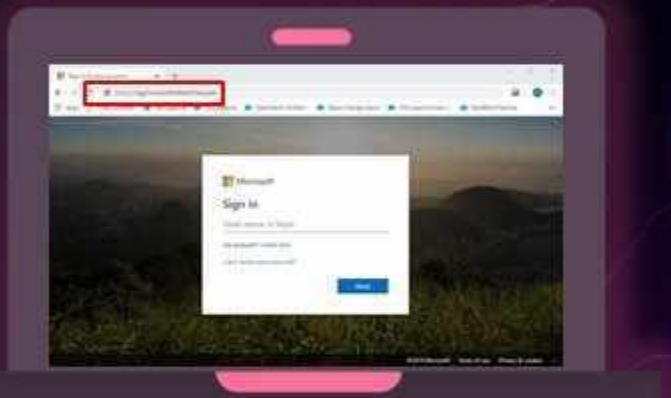
Click to Enlarge

MULTI-VECTOR ATTACK

Step 1: Phishing scam for Account Takeover

Clicking the link leads to a malicious phishing web site



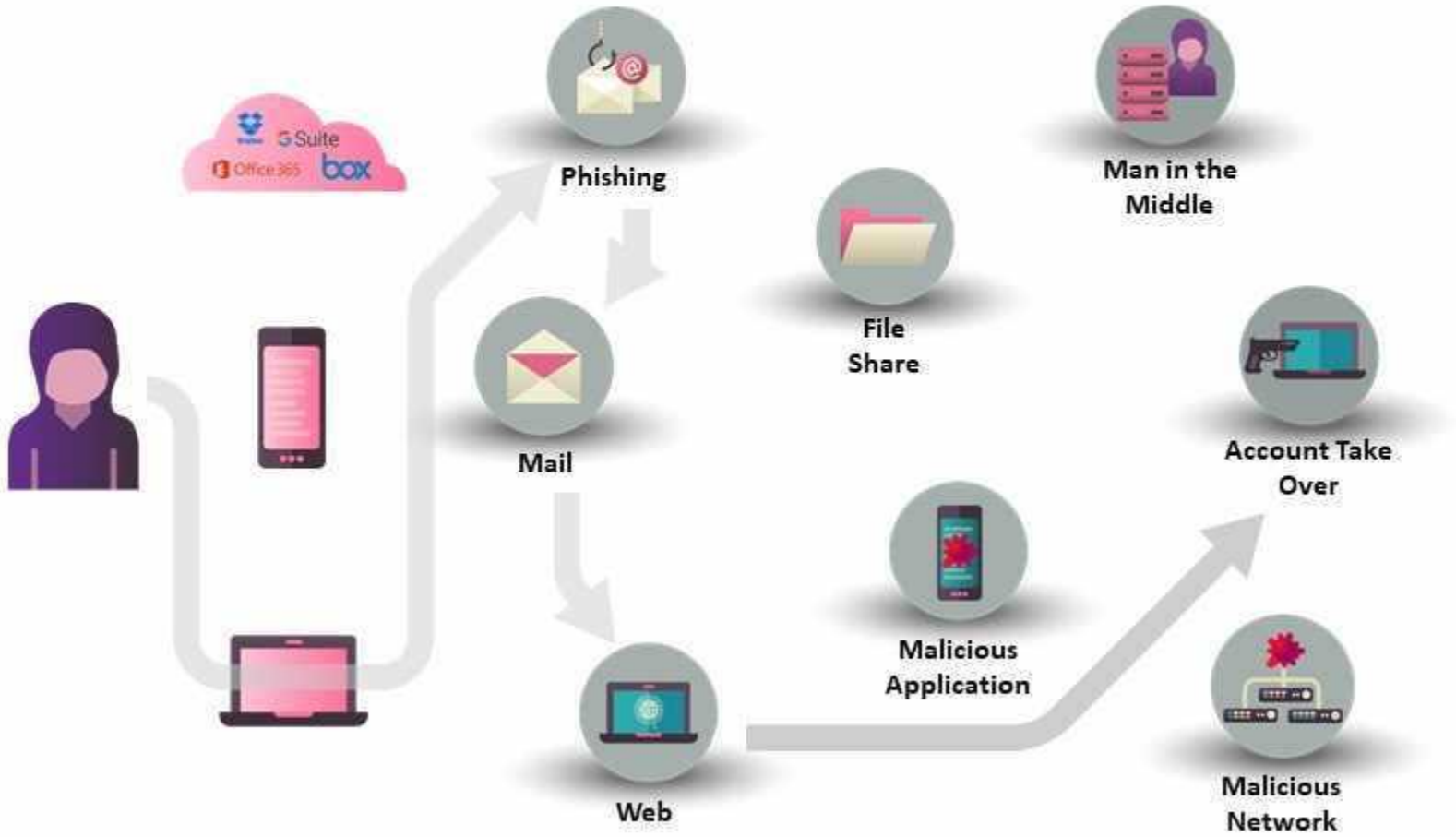


Click to Enlarge

MULTI-VECTOR ATTACK

Step 1: Phishing scam for Account Takeover

Victim is tricked to use his credential and account take over succeeded



MULTI-VECTOR ATTACK

Step 2: Shifting to a whaling attack

Attacker uses the stolen account and send wire transfer request for the CFO, usin

Urgent - Message (HTML)

FILE MESSAGE

Richard Brown
Faster Payment

Hi Frank,

Hope your day is going on well, I need you to send out a same day UK to UK faster payment immediately, Kindly email me the required details you will need to send out the payment.
I will appreciate a swift email response.

Kind regards,
Richard

Click to Enlarge

MULTI-VECTOR ATTACK

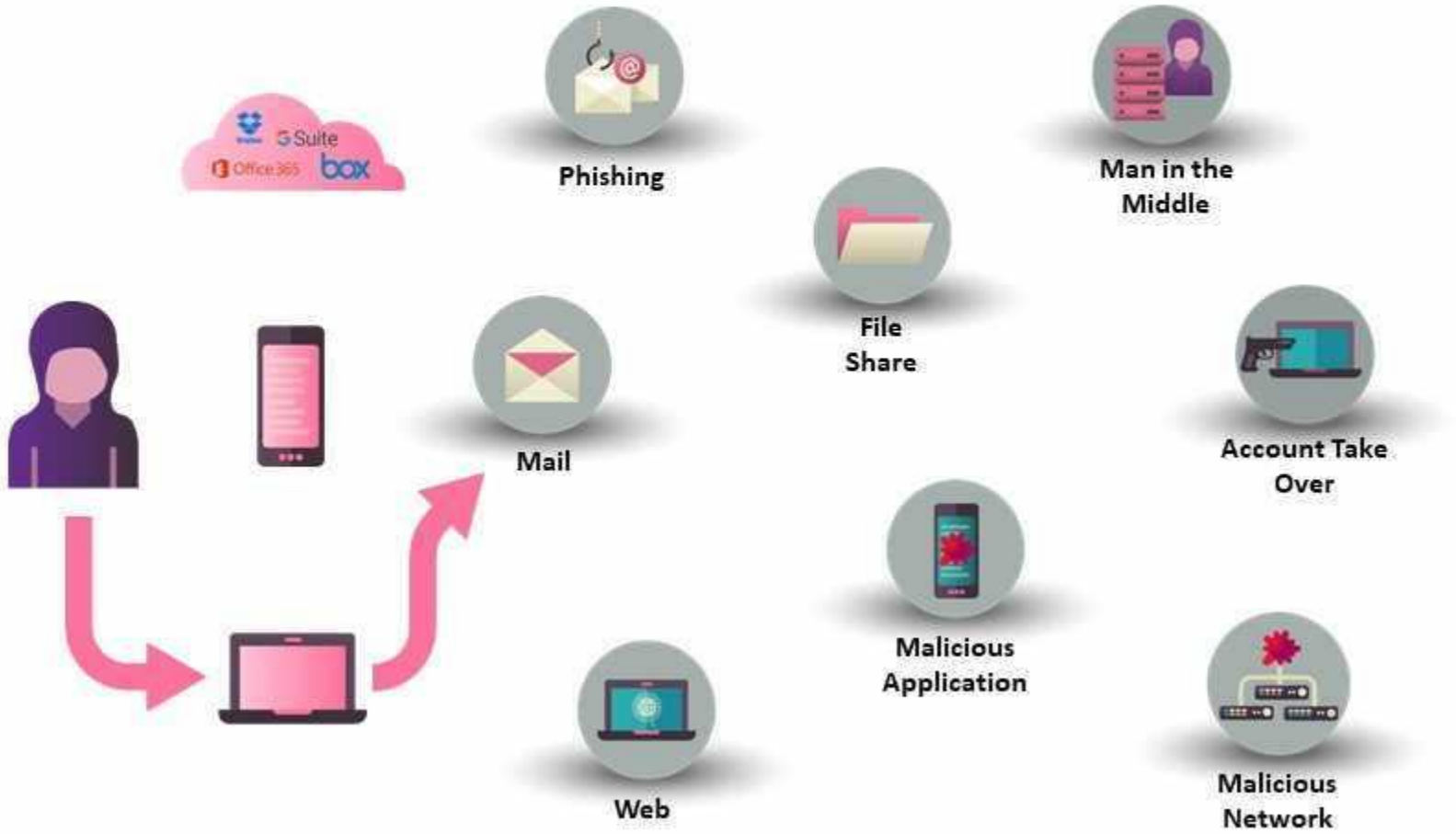
Step 2: Shifting to a whaling attack

Wire transfer completed

Click to Enlarge

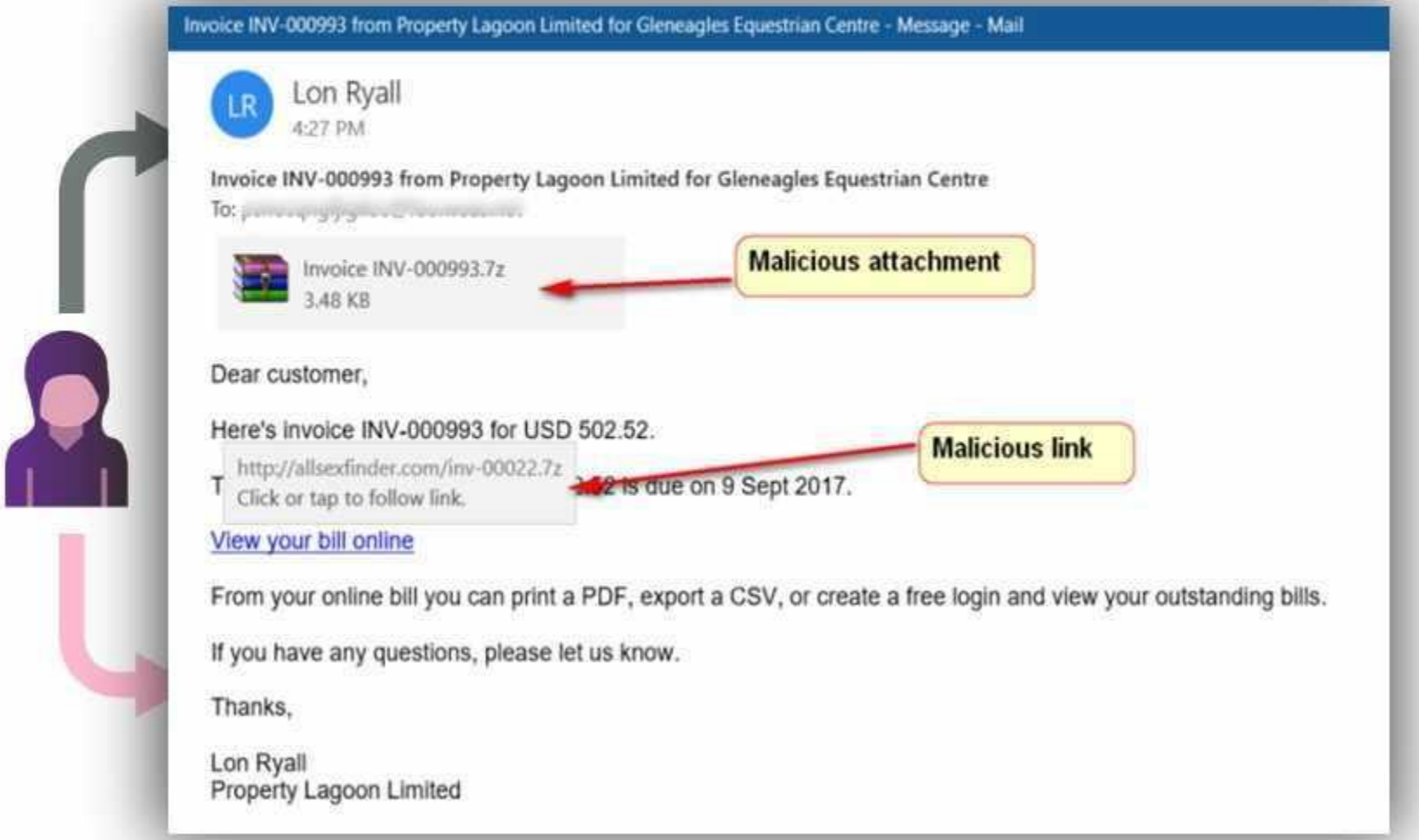
MULTI-VECTOR ATTACK
Step 3: Data Theft

Attacker decides to continue and drives a data theft targeted attack



MULTI-VECTOR ATTACK
Step 3: Data Theft

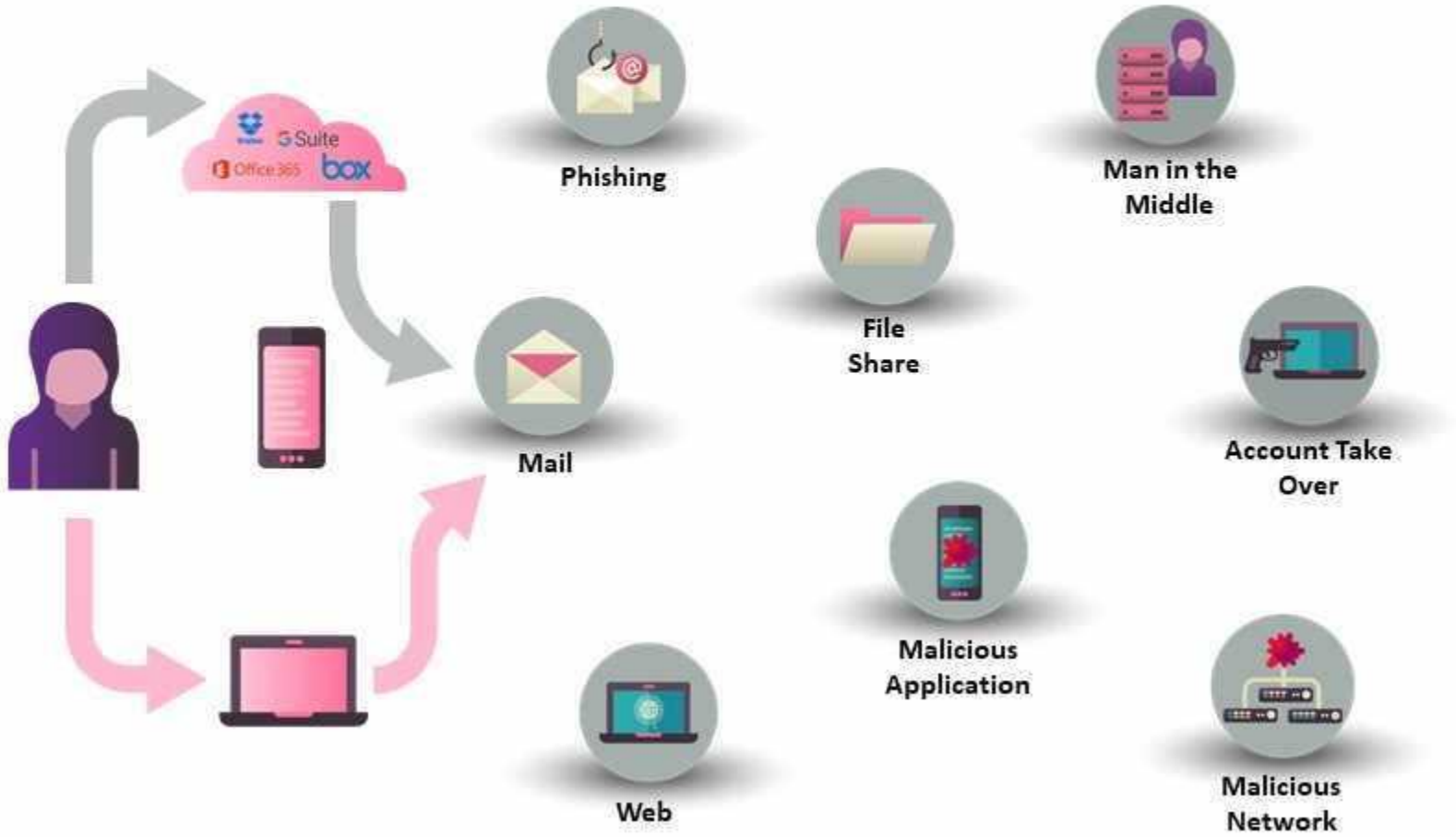
Using the stolen account he sends an “innocent” mail, embedded with a malicious attachment or link



Click to Enlarge

MULTI-VECTOR ATTACK
Step 3: Data Theft

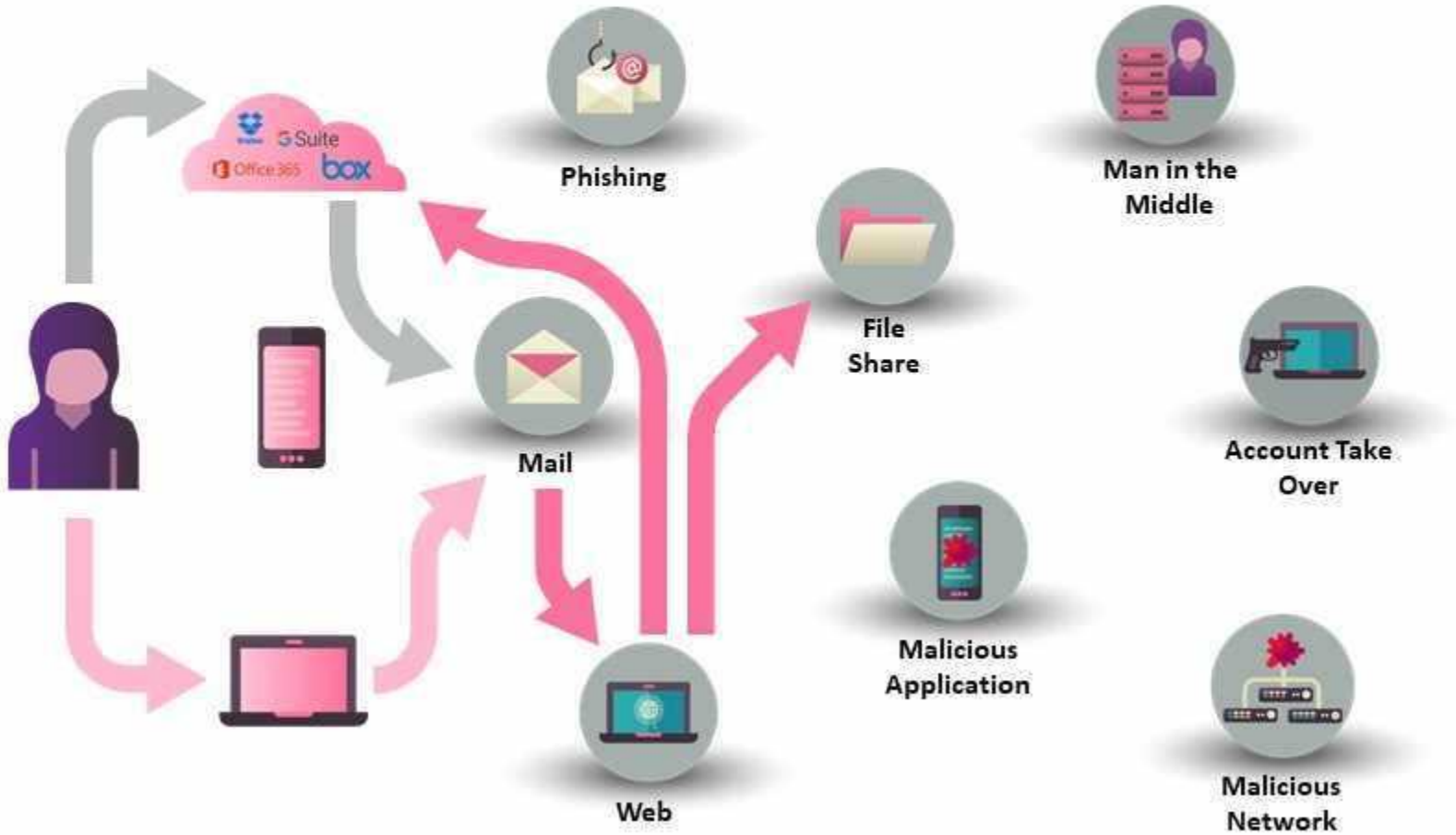
Victim's laptop is being infected by malicious malware and the attack accelerates



MULTI-VECTOR ATTACK

Step 3: Data Theft

The malware uses file shares to infect more laptops via lateral movement



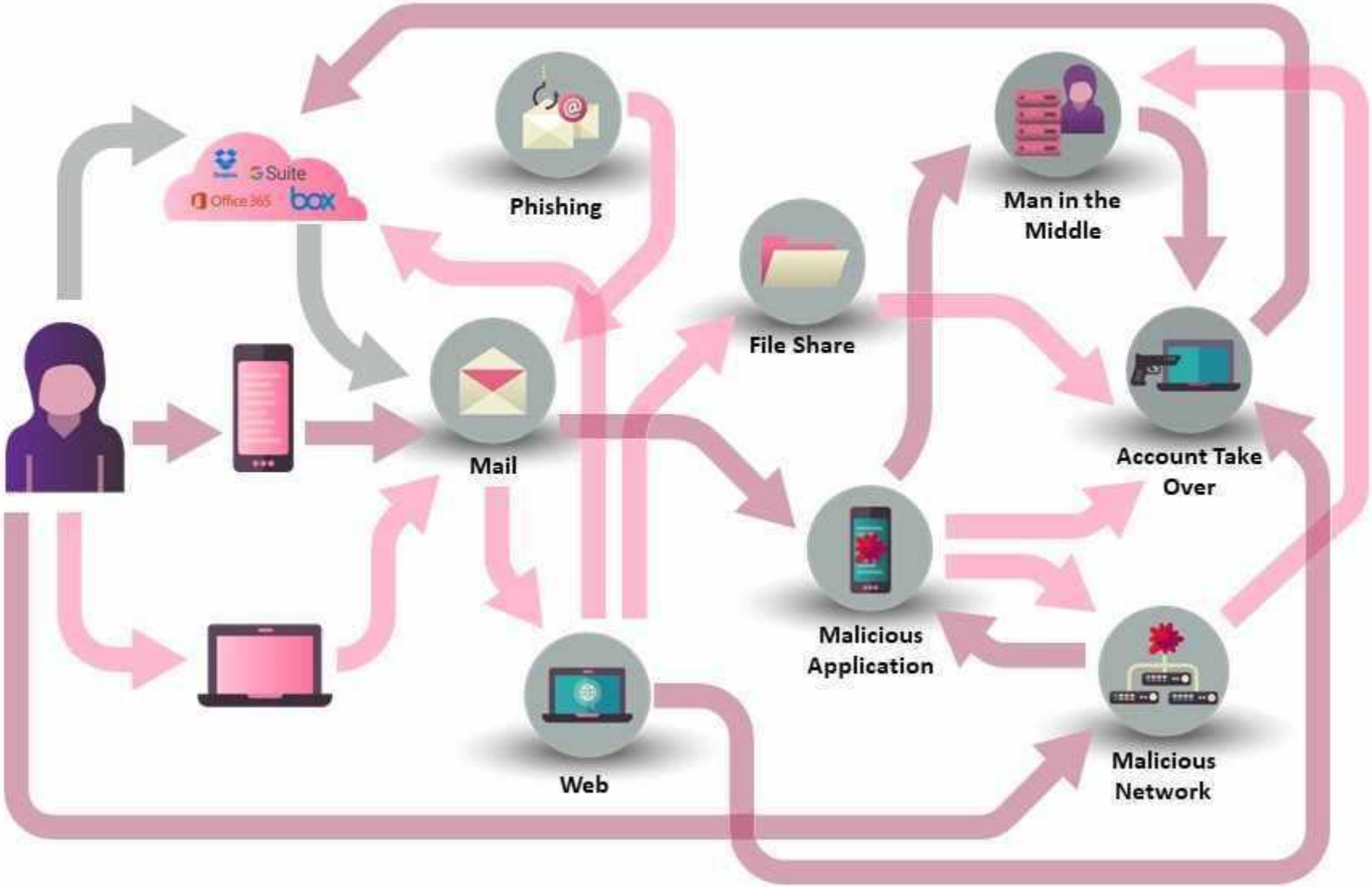
MULTI-VECTOR ATTACK

Step 3: Data Theft

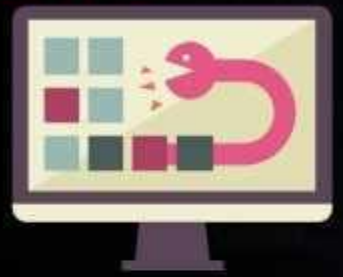
Attacker accomplished his attack, stealing more accounts, taps smartphones, laptops, collecting data or injecting additional malware

CONNECTING THE DOTS

Unlimited paths to take control of your assets



Traditional Protections are insufficient



Signatures and Reputation do not protect against zero-day attacks

- **Zero-day Viruses** - Only **45%** of malware attacks can be detected by AV* (source: theguardian.com)
- **Zero-day URLS** – Recently established Phishing URLs have no reputation
- **Zero-day malicious mobile applications**

Polymorphic attacks designed to avoid and evade 1st Gen sandboxes

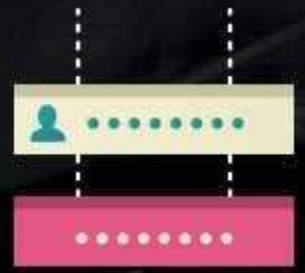
Traditional Protections are insufficient

Smartphones & Tablets Operating System security – vast majority are out of date

- 78% of devices are running on older O/S with known vulnerabilities

Increased prevalence of Application malware

- Google Play's app vetting is insufficient; malware also found in AppStore



Attacks use credential theft to drive phishing and whaling attacks

- Employees quick to click and download
- 81% of breaches involve weak or stolen credentials

A Modern Security Paradigm is Needed

- Advanced detection engines that continuously learn and evolve
  - (Dynamic Analysis, Evasion resistant, Machine learning, AI, Big Data)
- Take security decisions in real-time
  - Blocks Zero-day Viruses
  - Blocks malicious URLs with no reputation
  - Blocks malicious apps with no reputation