

Advanced Persistent Threats Go Mobile

chapter 4

إسراء عبد الباسط صوان

يقين عبدالفتاح زربية

فرح الامين الارباح

In this chapter :

- The Changing Face of Hackers
- Targeting the Victim
- The ABCs of APTs
- The Lifecycle of a Modern Attack
- The Central Role of Malware
- APTs and Mobile Security

The Changing Face of Hackers

01

The Changing Face of Hackers

- Has far more resources available to facilitate an attack.
- Has greater technical depth and focus.
- Is supported by an organization or nation-state.
- Operates as part of a team rather than as an individual.
- Is well funded.



Why does this matter?



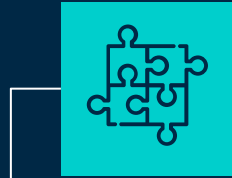
Targeting the Victim

02

The ABCs of APT's

03

Key characteristics of an APT



01

Advanced



02

Persistent



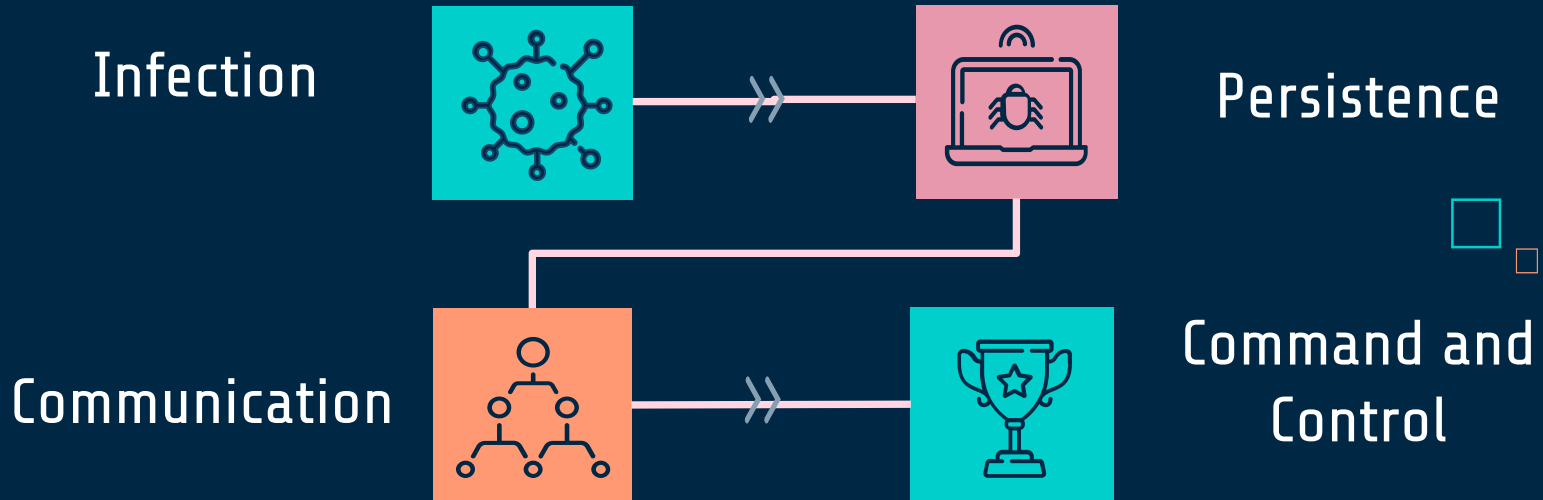
03

Threat

The Lifecycle of a Modern Attack

04

The Lifecycle include :





Infection

Infection

- تبدأ هذه المرحلة باستغلال المخترق لثغرة أمنية في برنامج او نظام تشغيل أو عن طريق استغلال الجوانب الإجتماعية.
- تساعد تطبيقات التواصل الاجتماعي المهاجمين في جمع الضحايا من خلال ارفاق رابط ضار مع عنوان يجذب المستخدمين وبمجرد النقر على الرابط يتم اختراق اجهزتهم.
- بمجرد أن يستغل المهاجمون أحد التطبيقات بنجاح ، يمكنهم اتخاذ عدد من الإجراءات بعد ذلك. أحد أكثر الإجراءات شيوعًا هو إنشاء `access shell` ، توفر للمهاجم واجهة سطر أوامر ، احد الامثلة عن استغلال Shell على الأجهزة المحمولة هو `Webview exploit` .

Ways that **Malware** use to avoid security controls :

Avoid signature-based detection



Blocking of attack transmissions over the encrypted channel

The background is a dark blue field filled with numerous small squares of varying sizes and colors, including teal, orange, and pink, scattered across the entire area.

02



Persistence

Some of the **tools** used by malware :

it is a piece of malware
that hides in the upper
functions of the operating
system.

rootkits

bootkits

It is a type of malicious
infection which targets
the Master Boot Record
located on the physical
motherboard of the
computer.

they enable an attacker to
bypass normal
authentication procedures
to gain access to a
compromised system.

Backdoors

The background is a dark blue field filled with numerous small squares of varying sizes and colors, including teal, orange, and pink, scattered across the entire area.

03



Communication

Attack Traffic Blocking

Techniques :

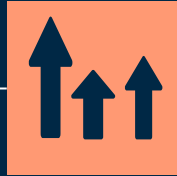


01

Encryption

with SSL, SSH (Secure Shell), or some other custom application.

بهذه الطريقة يمكن للمهاجمين التحرك عبر قطاعات الشبكة والأجهزة بسهولة وبخفية.



02

Port evasion

التهرب من المنافذ باستخدام أجهزة إخفاء هوية الشبكة.



03

Generate very little traffic

توليد حركات مرور بكميات قليلة جداً.



04

DNS fast fluxing

هذه الطريقة تمكن المهاجمين من ربط عدة عناوين IP باسم domain واحد وتغيير عناوين IP هذه بسرعة، حتى لا يتم كشفهم.

The background is a dark blue gradient. It is decorated with numerous small squares of various sizes and colors, including teal, orange, pink, and white. Some squares are solid, while others are outlines. They are scattered across the entire frame, with a higher density in the upper corners.

04



Command and Control

The Central Role of Malware

05

The modern threat shell game



APTs and Mobile Security

06



APTs and Mobile Security



Real-world mobile malware: **Dplug**

07

Real-world mobile malware: Dplug

Dplug

Dplug uses SMS to hijack the device's unique identifiers, subscribe to premium services and hide this behavior from the user by blocking the premium service notifications



THANKS

