Advanced Persistent Threats Go Mobile

chapter 4

يقين عبدالفتاح زريبة

إسراء عبد الباسط صوان

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?

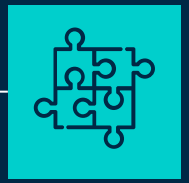
Targeting the Victim

02

The ABCs of APTs

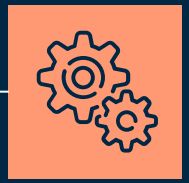
03

Key characteristics of an APT



01

Advanced



02

Persistent

03

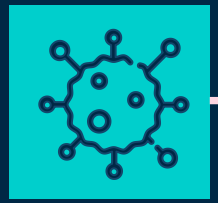
Threat

The Lifecycle of a Modern Attack

04

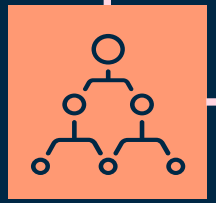
The Lifecycle include :

Infection



Persistence

Communication



Command and Control

Infection

Infection

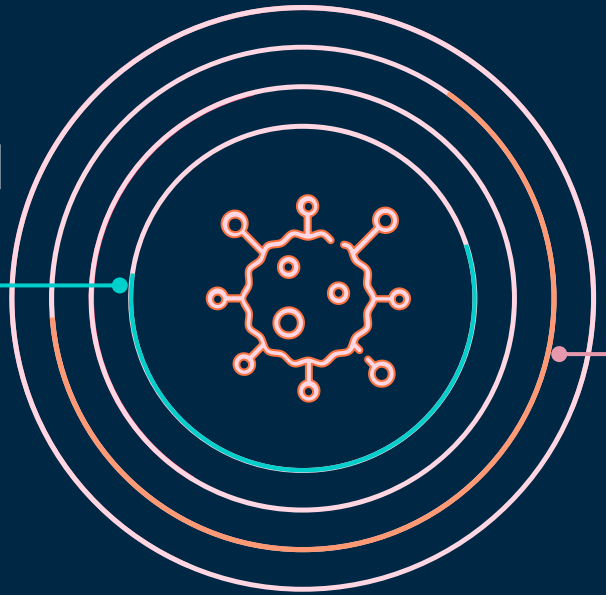
- تبدأ هذه المرحلة باستغلال المخترق لثغرة امنية في برنامج او نظام تشغيل أو عن طريق استغلال الجوانب الإجتماعية.

- تساعد تطبيقات التواصل الاجتماعي المهاجمين في جمع الضحاية 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 shell access ، توفر للمهاجم واجهة سطر أوامر، احد الامثلة عن استغلال Shellعلى 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

Persistence

Some of the tools used by malware :

Communication

Attack Traffic Blocking Techniques :

01

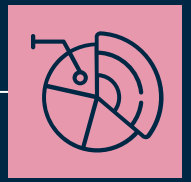
Encryption

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.

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