اساسيات الامن السيبراني

أ. جيهان تركي نصرالدين

بكالوريوس نظم المعلومات

حاصلة على شهادات الامن السيبراني من سيكو

منسقة تقنية معلومات

مدربة معتمدة من المؤسسة العامة للتدريب التقني و المهني

المحاور

- مفهوم الامن السيبراني
- أهمية الامن السيبراني
- اهداف الامن السيبراني
- استراتيجية و ركائز الامن السيبراني
- الفرق بين امن المعلومات و الامن السيبراني
- مبدأ AAA
- البرمجيات الضارة والتصدي لها
- ثغرة برنامج زوم
- برمجيات التجسس والتصدي لها
- الفرق بين الجدار الناري ومكافح الفايروسات
- جرائم الشبكات والتصدي لها
- الشبكة الخاصة الافتراضية
- امن المعلومات للأجهزة الذكية

مفهوم الامن السيبراني

حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من اجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق او تعطيل او تعديل او دخول او استخدام او استغلال غير مشروع.


Data on your computing devices
Financial Data
Medical Data
Your Data
Education Data
Employment
Your Identity
Information Online

أهمية الامن السيبراني

ارتباط المجتمع بالإنترنت واعتماده عليه يحتاج الى حماية البيانات الشخصية و الملكية الفكرية و بيانات المنظمات الحكومية و الشركات .

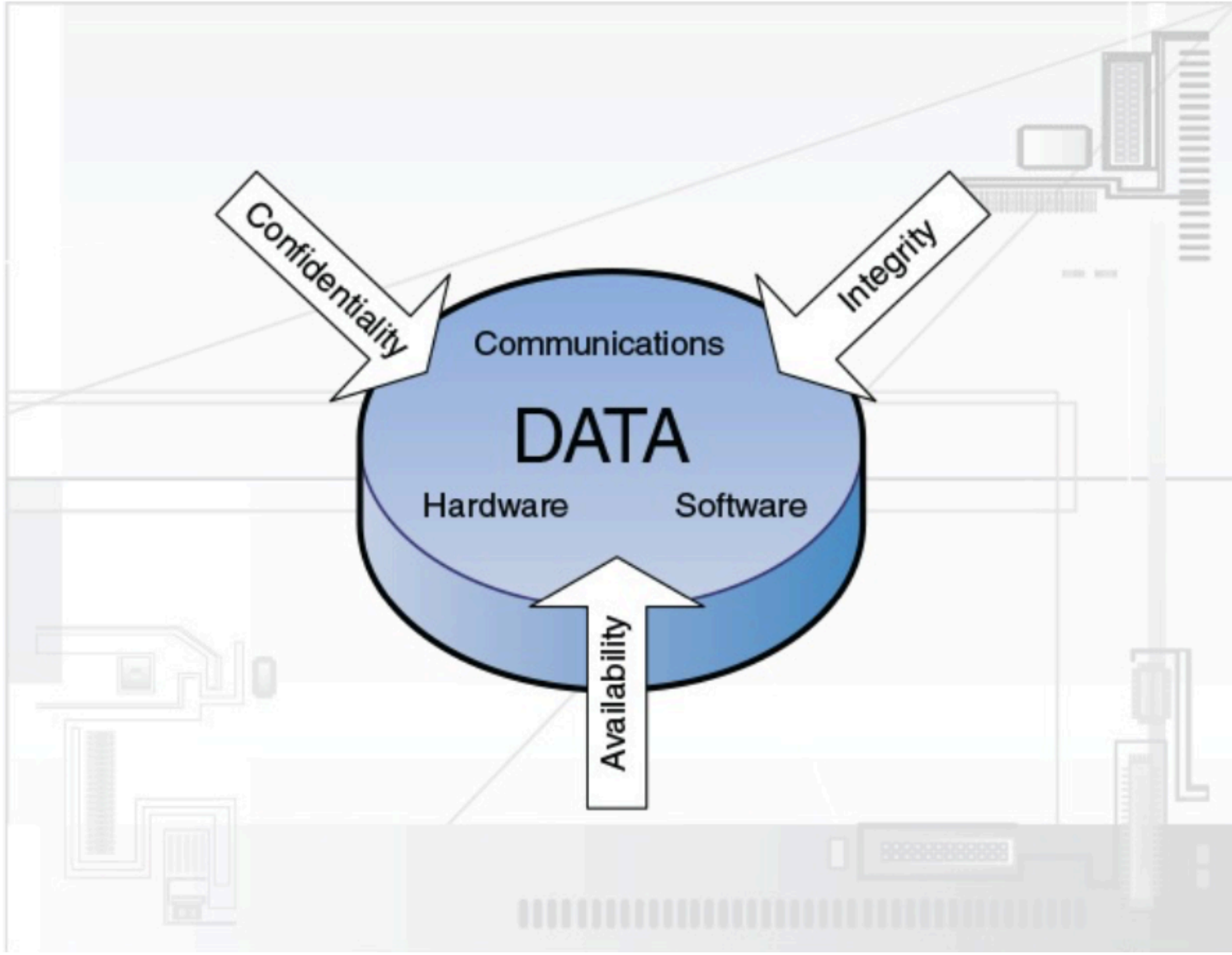
و ظهور الحروب الالكترونية ، لذلك تصنف مسائل الدفاع السيبراني كأولوية في السياسات الدفاعية الوطنية .

اهداف الامن السيبراني

السرية

السلامة

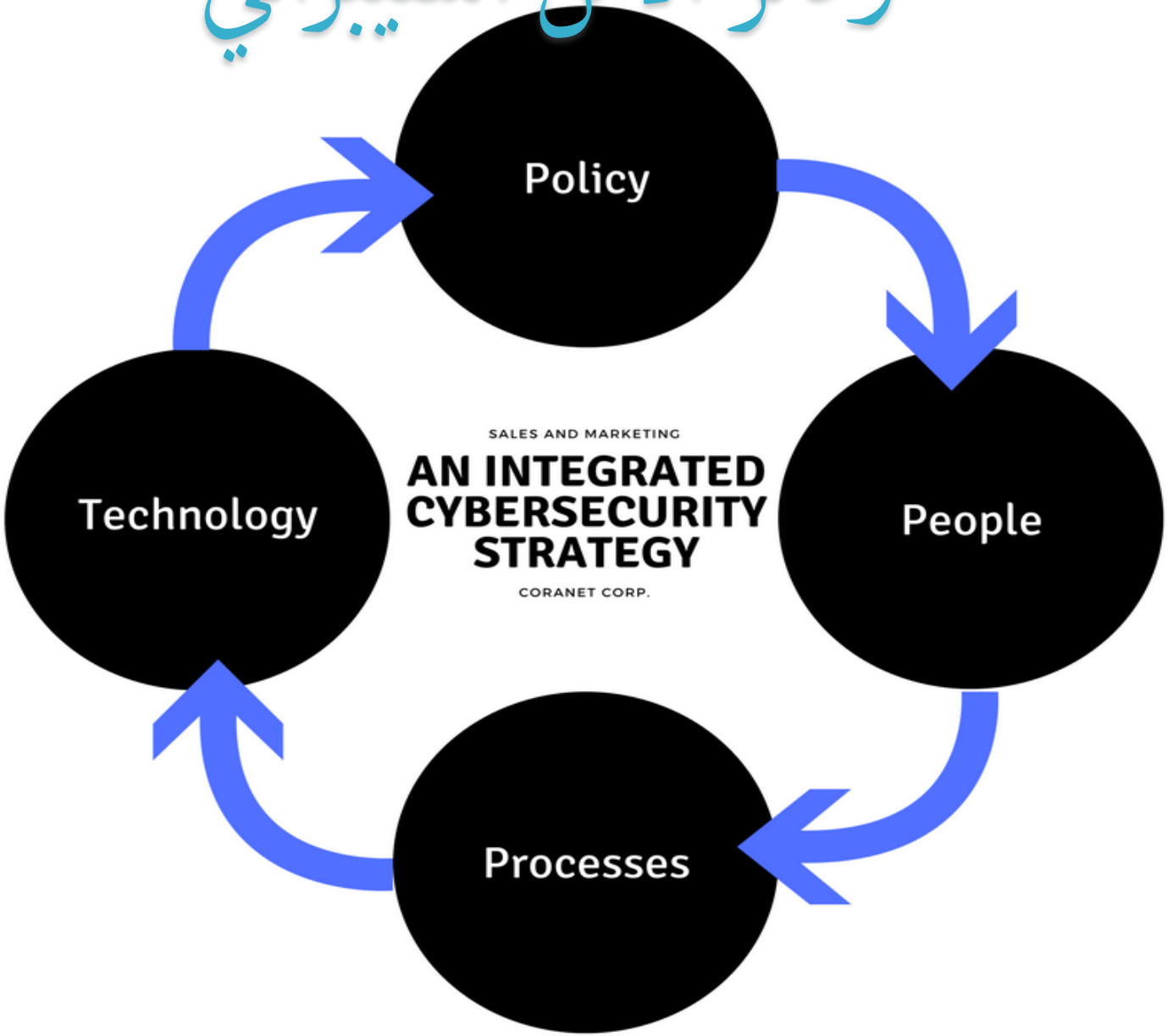
التوافر


Confidentiality
Integrity
Communications
DATA
Hardware
Software
Availability

استراتيجية الامن السيبراني

استراتيجية الأمن السيبراني تهدف إلى استمرار الأعمال والخدمات الإلكترونية الرئيسية التي تقدمها الجهة من خلال **رفع كفاءة** وقدرة إدارة الأمن السيبراني على حمايتها ضد الهجمات والأخطار الالكترونية.

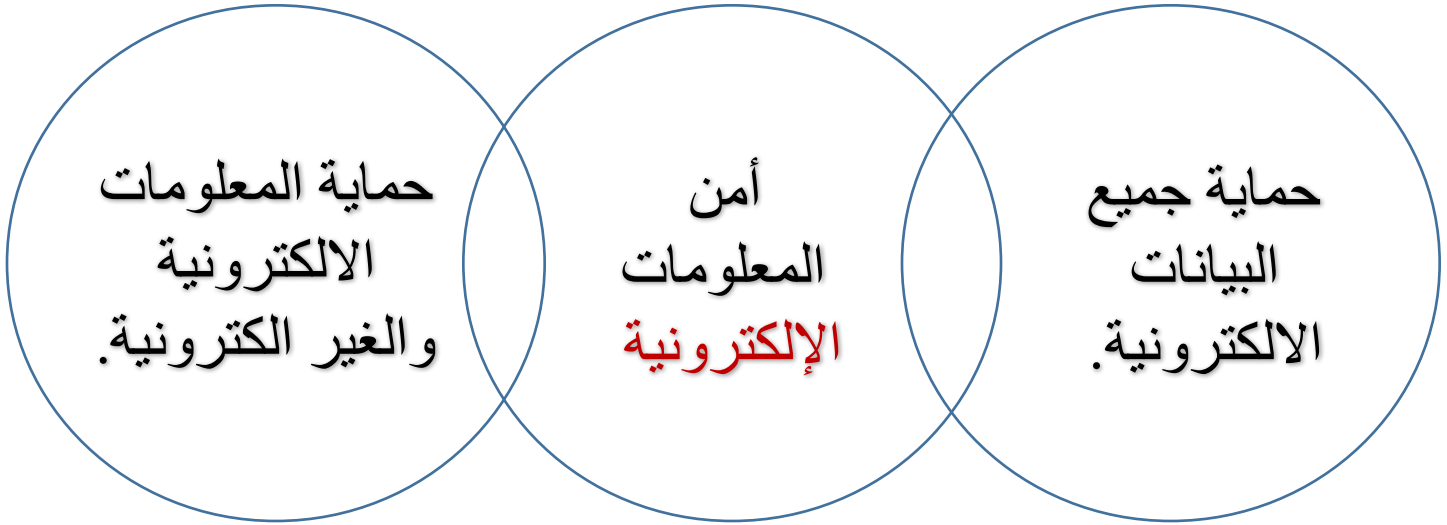
ركائز الامن السيبراني



امن المعلومات و الامن السيبراني

امن المعلومات : حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، او العبث بالمعلومات اثناء التخزين او المعالجة او النقل. والحفاظ على المعلومات وسريتها وتشفيرها بجميع اشكالها.

الامن السيبراني : فالأمن السيبراني يعتني بأمن كل ما يوجد في الفضاء المعلوماتي ومن ضمنه "أمن المعلومات الرقمية".



مبدأ AAA

Authentication:

هي اثبات هوية المستخدم او النظام . مثل اسم المستخدم وكلمة السر .

Authorization:

صلاحيات المستخدم داخل النظام بعد ما تتم المصادقة .

Accounting:

تعني متابعة ما يفعله المستخدمون، ويشمل ذلك ما يمكن للمستخدمين الوصول اليه، والوقت الذي استغرقه المستخدم في استخدام مورد ما ، و اي تعديل او تغيير تم على النظام ومن قام به .

البرمجيات الضارة

برمجيات يُصيب الأنظمة بطريقة خفية لانتهاك سرية او سلامة او توافر البيانات او التطبيقات او نظم التشغيل .

البرمجيات الضارة

الفايروسات

برامج يكتبها مبرمجون ترتبط بالبرامج والملفات بغرض تغيير خصائصها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب

تحتاج للتدخل من الانسان وتربط نفسها بمرفقات أخرى

قادرة على التناسخ والانتشار

بعض أنواع الفايروسات

فايروس الماكرو

فايروس يُلحق بالملفات النصية ويرسل عن طريق البريد الالكتروني و يبدأ بالتنفيذ عن فتح الملف المصاب .


Viruses found (3)
PC is infected by viruses (3)
You can lose all data and your credit card could be stolen.
Click here to remove viruses!
PC is infected
Click to remove viruses
Google Chrome • 0.donaldbluepage.icu
Close

بعض أنواع الفايروسات

فايروس هوكس

تنبيه كاذب عن وجود فايروسات يظهر للمستخدم عن طريق النوافذ المنبثقة او البريد الالكتروني ، هدفه خداع المستخدم لتثبيت برمجيات ضارة .

البرمجيات الضارة

الديدان

برنامج مستقل بذاته وله ملف خاص به.

تستفيد من الثغرات الأمنية في أنظمة التشغيل والتطبيقات

لا تحتاج للتدخل

تنتشر بسرعة في الشبكة و بشكل مستقل،

لا تربط نفسها ببرنامج اخر

البرمجيات الضارة

التروجان

برمجيات تظهر على انها مصممة لإجراءات معينة وهي على العكس ويتم تحميلها دون علم المستخدم عن طريق USB او الالعاب

الفدية :

مصمم ليشفر بيانات الكمبيوتر حتى يتم الدفع مقابلها .

البرمجيات الضارة

برمجيات التجسس

تسجل مواقع الويب التي تدخل اليها او تسجل ضغطات المفاتيح مثل "مسجل المِفاتيح"
تغير اعدادات النظام مثل توجيه المستخدم الى مواقع ويب غير مرغوبة مثل محسن الإنترنت ، الذي يعيد توجيه صفحات خطأ إلى صفحات إعلانات في مواقع الويب الأخرى.

برمجيات الإعلانات

مرتبطة ببرمجيات التجسس لأنها تظهر إعلانات بناء على التجسس على المستخدم.

البرمجيات الضارة

الجذور "الروتكيت"

يصعب اكتشاف مجموعات الجذر لأنه يتم تنشيطها قبل أن يتم تشغيل نظام التشغيل بالكامل.

تقوم بتثبيت الملفات المخفية والعمليات المخفية وحسابات المستخدمين المخفية. و لأنه يمكن تثبيت الجذور المخفية في الأجهزة أو البرامج ، فيمكنها اعتراض البيانات القادمة من اتصالات الشبكة ولوحات المفاتيح.

طريقة حدوث البرمجيات الضارة في الانظمة

- عن طريق مرفقات البريد الالكتروني
- FTP بروتوكول نقل الملفات
- التحميل من الانترنت
- الوسائط المنقولة مثل USB, memory card and CD
- اختراق عنوان URL : يقوم المستخدم بكتابة URL خطأ وبذلك يتم توجيه المتصفح لمواقع غير مرغوبة تجعل النظام مستهدف بالبرمجيات الضارة مثل التجسس
- الأبواب الخلفية

الابواب الخلفية و القنابل المنطقية

الأبواب الخلفية

يتم استخدامها لتجاوز المصادقة العادية وطرق الأمان الأخرى.

القنابل المنطقية

تنفذ الاعمال الضارة عند حصول شرط معين مثل الوقت او اليوم.

اعراض البرمجيات الضارة

- زيادة في استخدام المعالج
- توقف عمل الكمبيوتر
- انخفاض في سرعة التصفح
- حدوث أصوات غريبة.
- تلقي رسائل خطأ غير عادية.
- يحدث تشويه في العرض أو الطباعة.
- ملفات محذوفة او معدلة
- ظهور ملفات ، برامج و ايقونات على سطح المكتب غير معروفة
- زيادة الامتدادات على الملفات مثل .txt.vbs or .txt.exe.
- توقف عمل مكافح الفايروسات
- مشاكل غير مفهومة عند الاتصال بالشبكة

منع البرمجيات الضارة

- تشغيل وتحديث برنامج مكافحة الفيروسات.
- فحص النظام بأكمله بشكل دوري
- تحديث نظام التشغيل
- استخدام جدار حماية


zoom

Hacker Fantastic
@hackerfantastic

How to hack the UK government (multiple options):

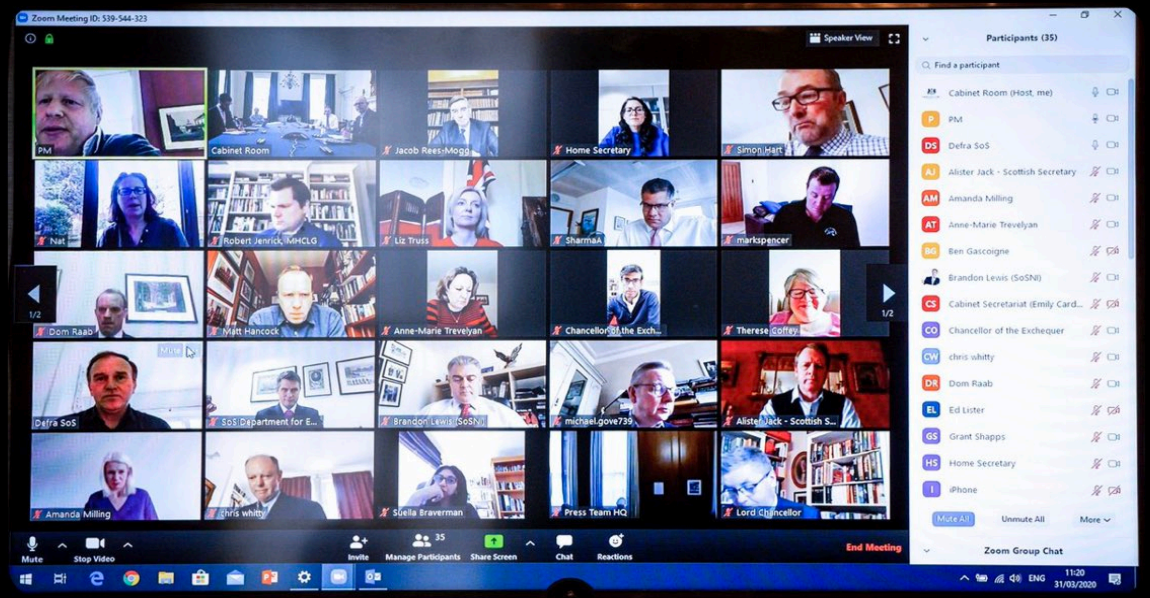
1. PM uses a Windows 10 Desktop target
2. Any PowerPoint RCE exploit.
3. Any Chrome Browser RCE exploit.
4. Zoom client / meeting exploits.
5. Microsoft Outlook RCE exploit.

Join Zoom ID: 539-544-323 & post you're URL/exploit.

Boris Johnson #StayHomeSaveLives
@BorisJohnson

This morning I chaired the first ever digital Cabinet.

Our message to the public is: stay at home, protect the NHS, save lives. #StayHomeSaveLives



اعراض برمجيات التجسس

- تعديل الصفحة الرئيسية الافتراضية لمتصفح الويب.
- ظهور موقع ويب معين في كل مرة تقوم فيها بإجراء بحث.
- ظهور النوافذ المنبثقة الزائدة.
- يتم إيقاف تشغيل برامج جدار الحماية ومكافحة الفيروسات تلقائيًا .
- تظهر البرامج والرموز والمفضلة الجديدة.
- حدوث مشاكل فردية داخل النوافذ (نظام بطيء ، تطبيقات تتصرف بشكل غريب ، وما شابه).

منع برمجيات التجسس

- الحصول على مكافح التجسس
- تعديل اعدادات امان المتصفحات مثل تعطيل الكوكيز وتقييد الدخول للمواقع الضارة
- إزالة البرامج الغير مرغوبة وتعطيل التحكم بالكمبيوتر عن بعد
- التحقق من امان الموقع مثل HTTPS

التصدي لبرمجيات التجسس

- قطع الاتصال بالشبكة
- إزالة البرامج الغير مرغوبة
- إعادة تشغيل الحاسب
- فحص النظام باستخدام برنامج AV لإزالة أي فيروسات ربما تكون قد أصابت النظام مما قد يعيق إزالة برمجيات التجسس
- فحص النظام باستخدام برنامج Anti spyware للتأكد .
- تحقق من إعداد الصفحة الرئيسية في متصفحك

الجدار الناري و مكافح الفايروسات و امن الانترنت

مكافح الفايروسات	الجدار الناري	امن الانترنت
برنامج مصمم لحماية النظام من البرمجيات المدمرة مثل الفايروسات الموجودة في النظام	هو برنامج يتحكم في الاتصالات الداخلة والخارجة والمسموح منها والغير مسموح	مجموعات أمان الإنترنت عادة من أكثر من تطبيق واحد يتم تجميعه في واجهة واحدة .
هدفه الأساسي الكشف ومنع و إزالة جميع أنواع الفايروسات التي تدمر النظام	يحلل حزم البيانات في الشبكة ليحدد المسموح لها بالعبور .	يشمل الحماية من الفيروسات ، جدار ناري ومكافحة البرامج الضارة ، ومكافحة برامج التجسس ، وبرامج حماية البريد الإلكتروني .
يكشف عن الفايروسات و الديدان الموجودة مسبقا في النظام	يراقب حركة المرور الواردة والصادرة لتضغط استراتيجياً على البيانات التي يحتمل أن تكون معرضة للخطر	يحذرك من الموقع الغير آمنة و البرامج الغير الامنة قبل تحميلها من الانترنت ، المواقع غير الامنة للدفع

جرائم الشبكات

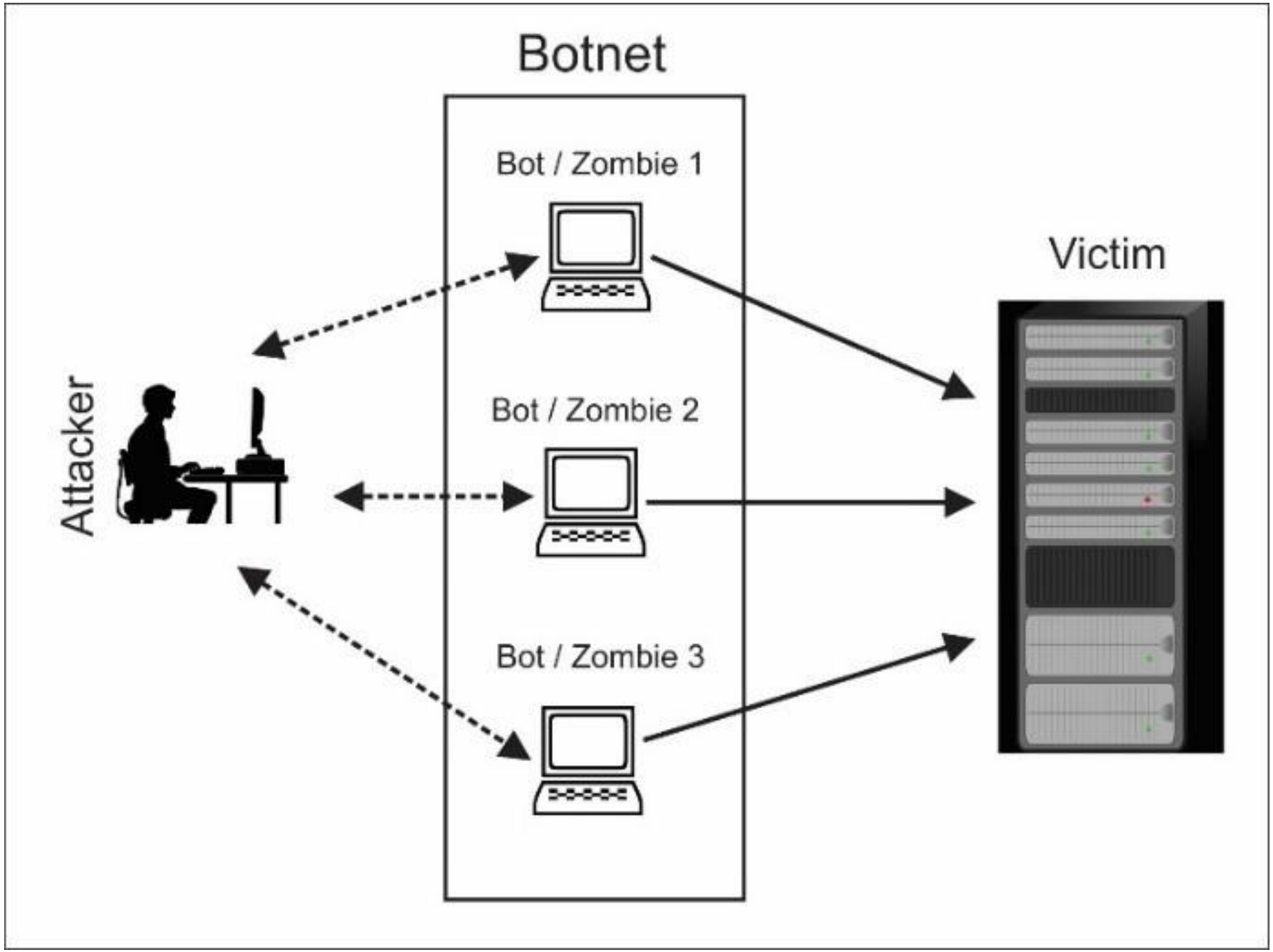
الاستغلال المتعّمد لأنظمة الحاسب الآلي والشبكات والجهات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية بهدف إحداث أضرار .

هجوم حجب الخدمة
Denial Of Services

هجوم حجب الخدمة : هدفه تعطيل موارد الجهاز مثل الخوادم والحواسيب و الراوترات.

طرق حدوث DOS

- **المرور المتضخم Flood Attack :** يتم اغراق السيرفر بكمية كبيرة من البيانات وهذا يسبب بطء في النقل او الاستجابة وتعطيل الجهاز او إيقاف الخدمة.
- **الحزم الخبيثة Ping of Death :** يتم اغراق السيرفر بحزم خبيثة وحجمها كبير يتجاوز العدد المسموح.
- **Fork bomb :** يعمل عن طريق إنشاء عدد كبير من العمليات بسرعة لتعبئة مساحة المعالجة المتاحة في نظام التشغيل و العمليات قادرة على نسخ نفسها وتعطيل النظام.


Botnet
Bot / Zombie 1
Bot / Zombie 2
Bot / Zombie 3
Victim
Attacker

الانتحال
Spoofing

هجوم يتم فيه انتحال شخصية شخص ما أو برنامج ما

- URL spoofing باستخدام Phishing
- IP Spoofing
- MAC Spoofing

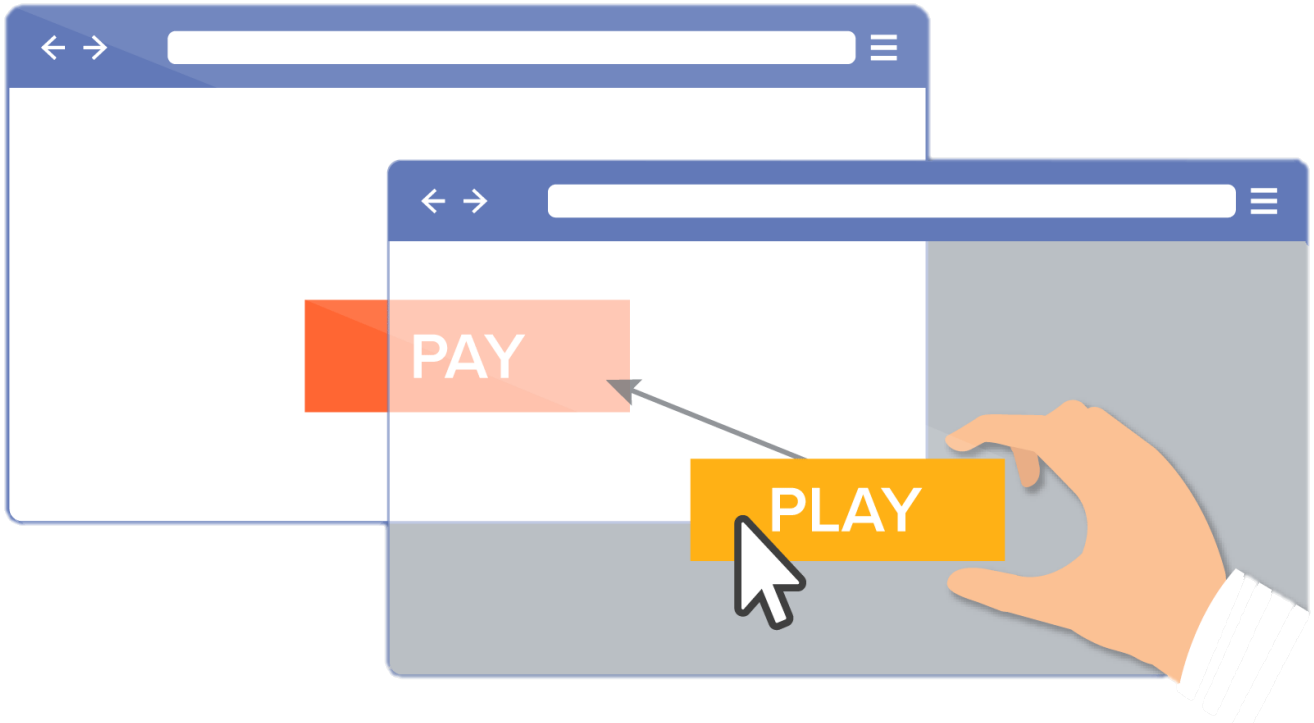
التصيد الالكتروني

هو جريمة إلكترونية يتم فيها الاتصال بالهدف عن طريق البريد الإلكتروني أو الهاتف أو رسالة نصية من قبل شخص يمثل مؤسسة شرعية لجذب الأفراد إلى توفير بيانات حساسة مثل معلومات التعريف الشخصية وتفاصيل البطاقات المصرفية وبطاقات الائتمان وكلمات المرور.

امثلة على التصيد الالكتروني

Clickjacking

يتم خداع المستخدم اثناء تصفح الانترنت بالنقر على أشياء غير المرغوبة ويتم تضمين الروابط المخفية او الأكواد ويتم تنفيذها عند نقر المستخدم عليها .



هجمة الرجل الوسيط

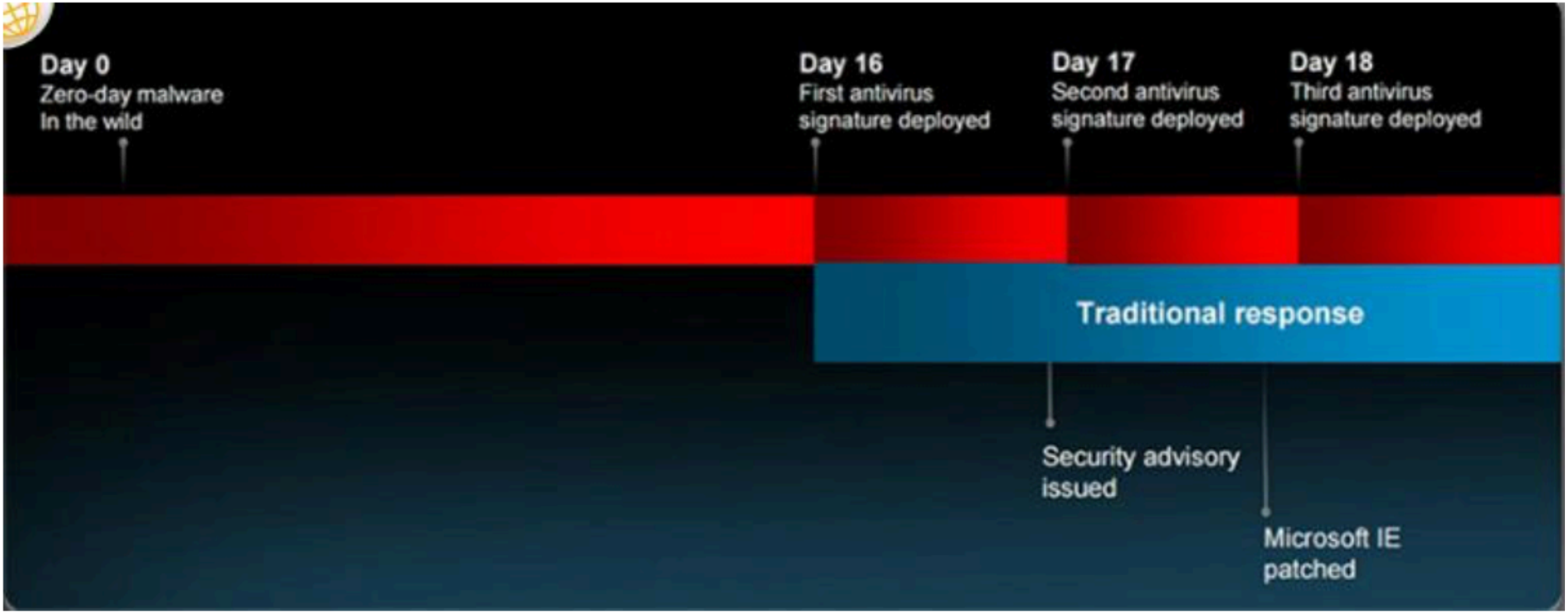
Man in the Middle

هجمة الرجل الوسيط : يقوم المهاجم بعمل هجمة الرجل الوسيط عن طريق التعرض للاتصال بين الحواسيب بهدف سرقة المعلومات التي تمر عبر الشبكة .

يمكن للمهاجم ايضا ان يقوم بالتلاعب في الرسائل وتوصيل معلومات غير صحيحة بين الأجهزة .

هجمات يوم الصفر
(Zero-Day)

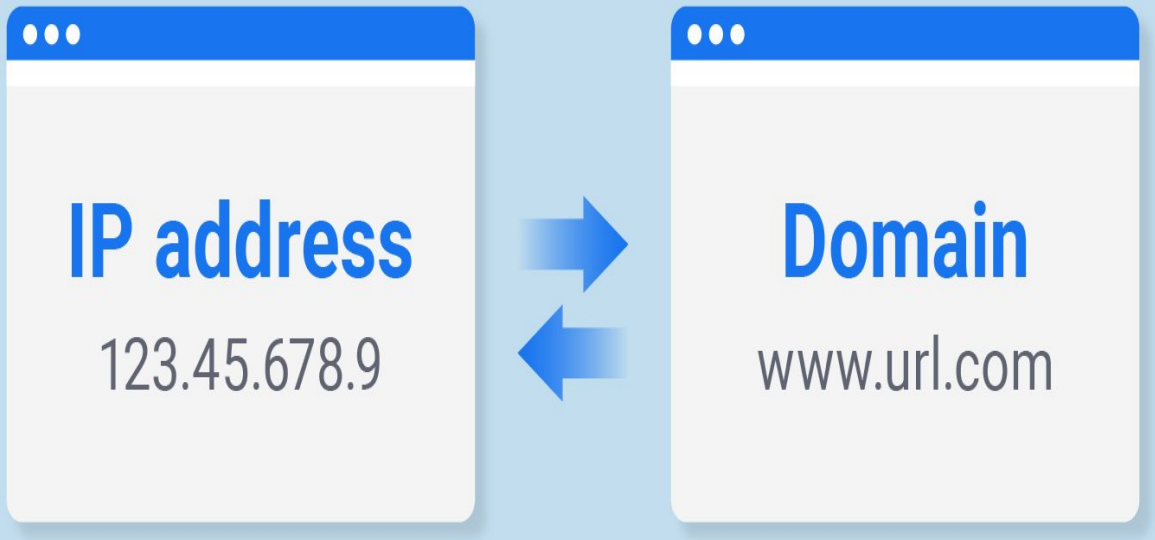
محاولة استغلال للثغرات الغير معروفة او التي لم تبلغ عنها الشركة المصنعة الموجودة في البرمجيات.


Day 0
Zero-day malware
In the wild
Day 16
First antivirus
signature deployed
Day 17
Second antivirus
signature deployed
Day 18
Third antivirus
signature deployed
Traditional response
Security advisory
issued
Microsoft IE
patched

التصدي لجرائم الشبكات

- تحديث الأنظمة والراوتر والسويتشات و تطبيقات او أجهزة جدران الحماية.
- تحديث المتصفحات
- استخدام التصفح المخفي
- الحصول Intrusion Prevention Sestem
- واجراء اختبارات للسيرفرات
- استخدام DNS Black hole List

الثقب الأسود في أنظمة أسماء النطاقات



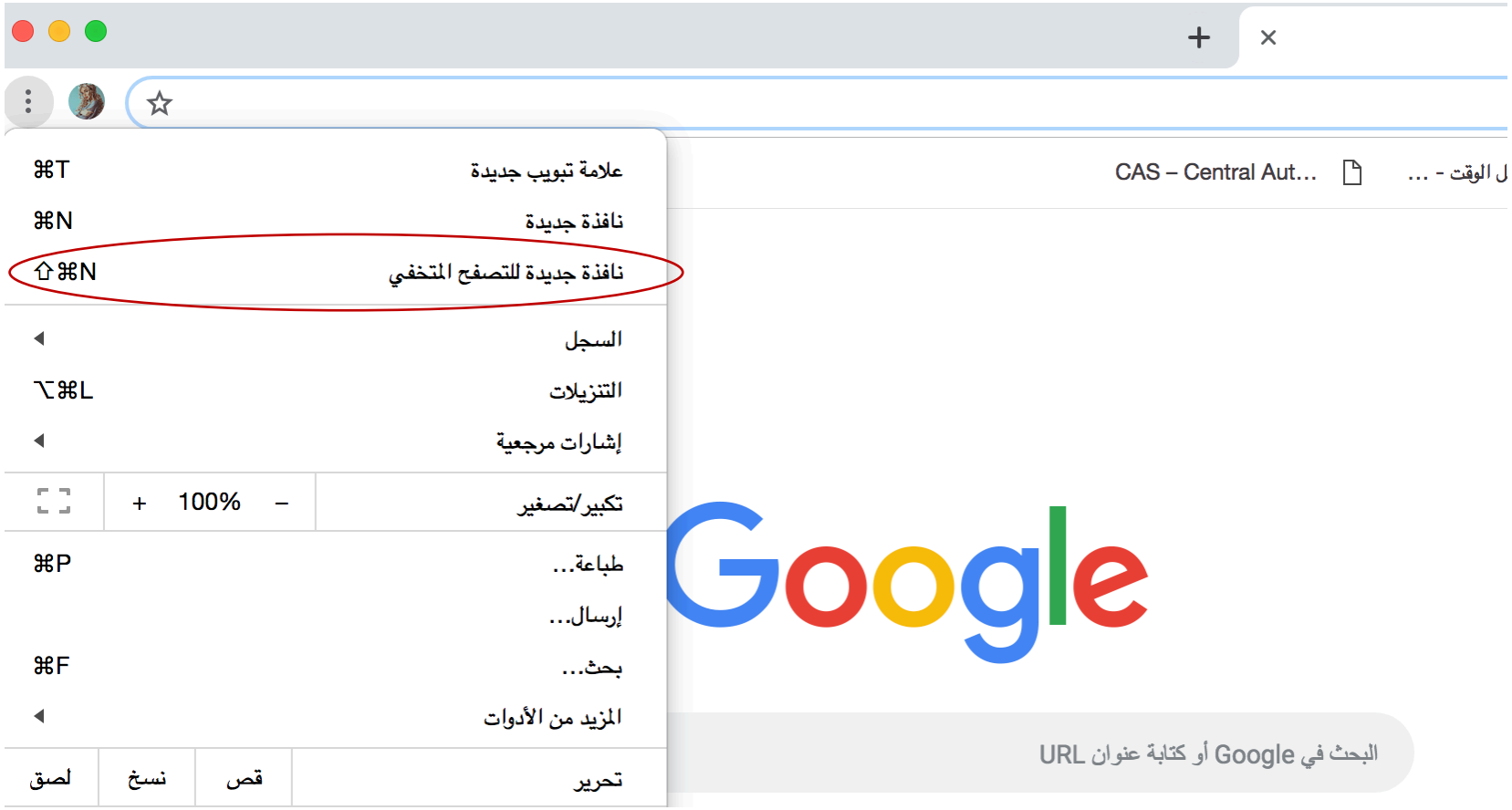
تعرِّف النطاقات المستخدمة بواسطة المهاجمين و النطاقات التي تحتوي على برمجيات ضارة.

DNS Black Hole List

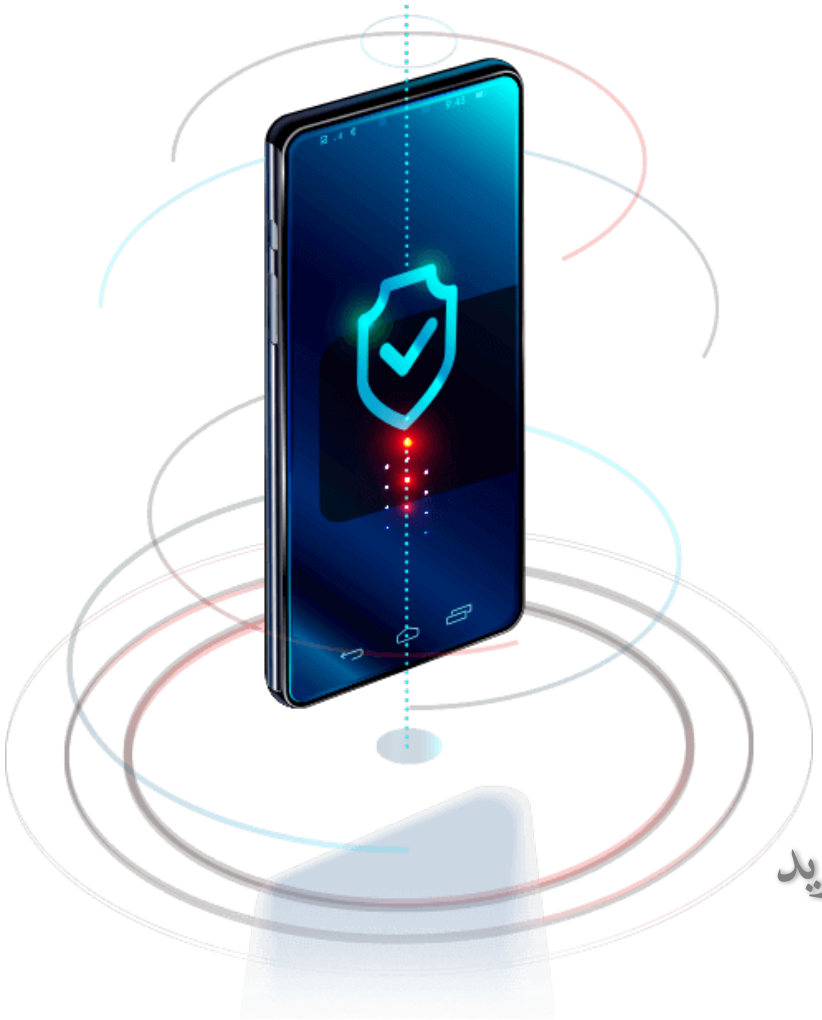
هي قائمة منشورة تحتوي على IP Adress في DNS الذي يحتوي على عنوان الحواسيب والشبكات الضارة مثل DDOS ويمكن تحميلها وتضمينها في DNS Server لحجب أجهزة الزومبي و البوتنيت

التصفح المخفي

- قوقل كروم



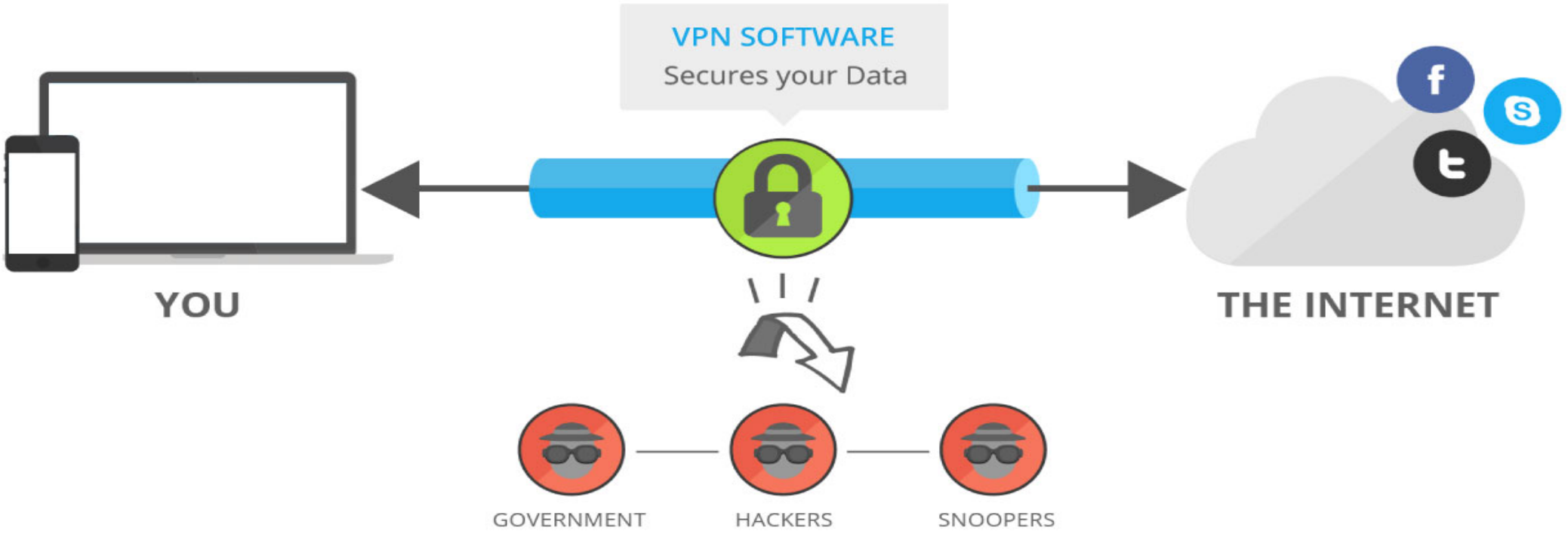
امن المعلومات للأجهزة الذكية



- تأكد دائما انك تحصل على التطبيقات من مصدر موثوق و آمن .
- تأكد من الصلاحيات التي يستطيع التطبيق الوصول اليها .
- تأكد من تحديث التطبيق و نظام التشغيل .
- الخطوات الأساسية لتأمين جهازك النقال :

- إضافة رقم PIN
- تثبيت برامج مكافحة الفايروسات اذا كنت من مستخدمي نظام اندرويد
- تأكد من خاصية البلوتوث

VPN


VPN SOFTWARE
Secures your Data
YOU
THE INTERNET
GOVERNMENT
HACKERS
SNOOPERS

کوییز سریع

تقييم الدورة

@GehanTN

حماية
Hemaya

”يجب أن نعمل لمواجهة التحديات
السيبرانية حتى لا تتحول
إلى عوائق اقتصادية “

سمو ولي العهد
الأمير محمد بن سلمان بن عبدالعزيز