hadi.assalem@gmail.com

Protecting Windows Systems from Rootkit

اشراف :

د.م محسن الحسين

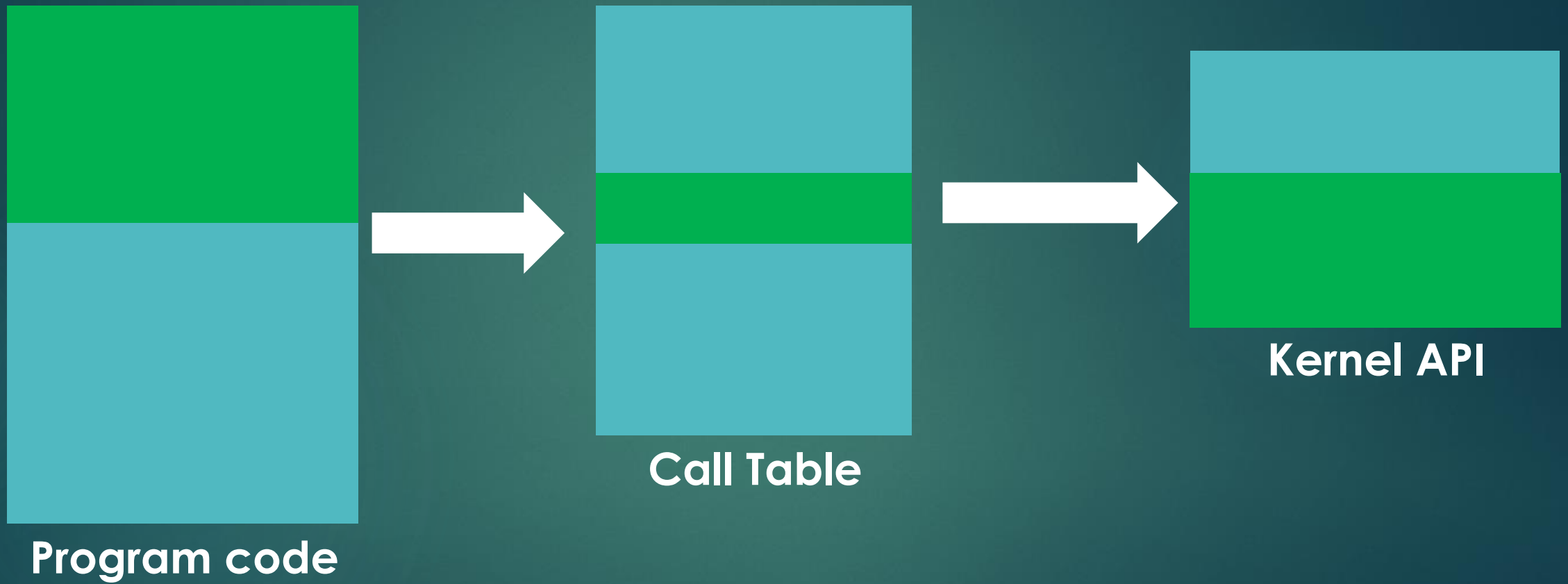
تقديم :

هادي السالم – يوسف إبراهيم – محمد نور شحيمة

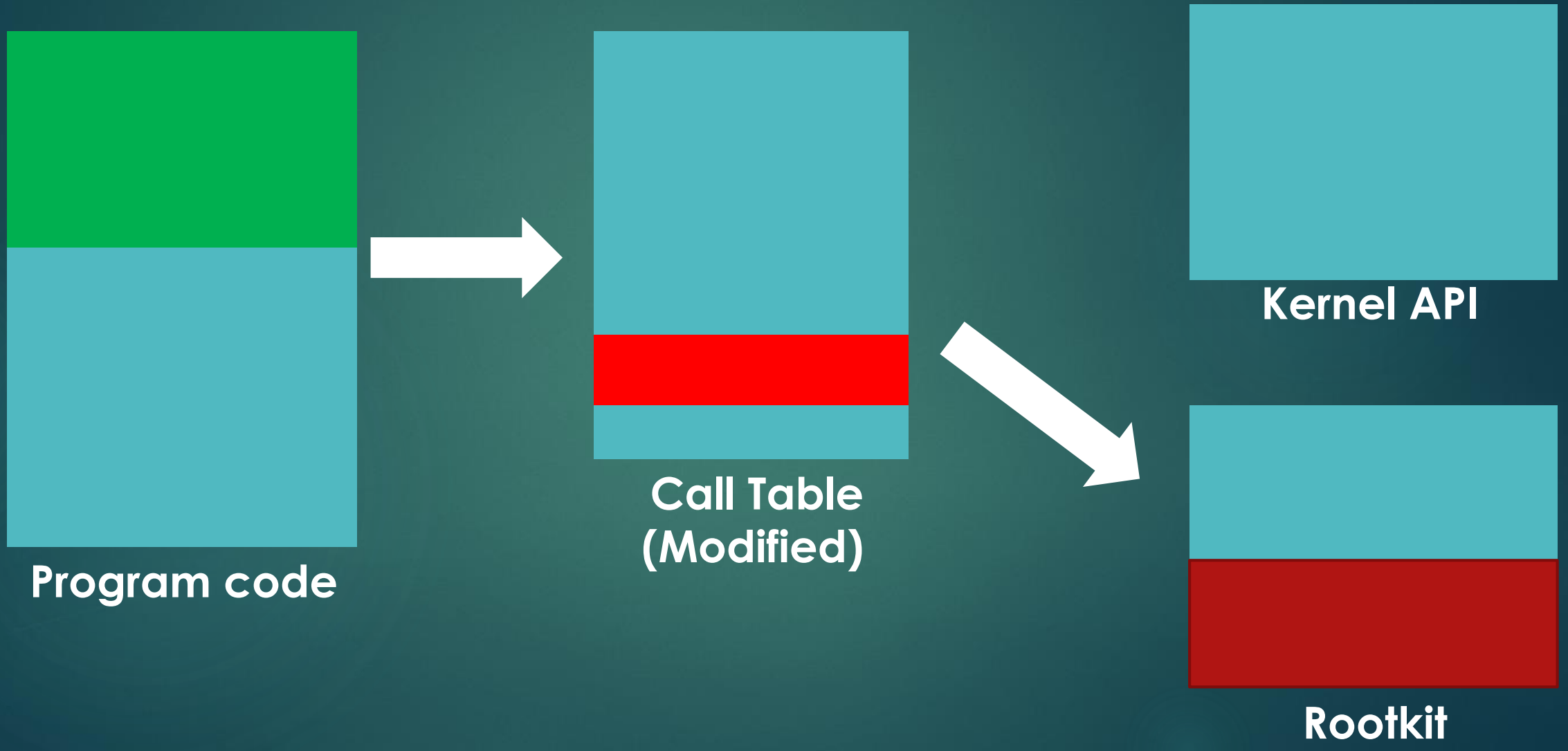
Project Path:

- إخفاء العمليات (Hiding Processes) .
- إخفاء الملفات والمجلدات (Hiding files and directories).
- إخفاء مدخلات ال Registry (Hiding registry entries).
- انشاء Backdoor .
- انشاء Key Logger .
- انشاء وحدة تحكم عن بعد (للتحكم بالRootkit).
- تخطي الجدار الناري (Bypassing the firewall).
- انشاء Rootkit غير قابل للكشف من قبل Antivirus.
- انشاء أداة لكشف الRootkit .

Normal Behavior:



Hooking(Rootkit Behavior):



Dll Injection Mechanism:

Dll In

Overview

Step 1

Process B

Attach

`OpenProcess();`

Process A

Step 2

Process B

Choose: DLL Path or Full DLL

Allocate Memory

`VirtualAllocEx();`

Process A

Step 3

Process B

Copy DLL/Determine Addresses

`WriteProcessMemory();`

DLL Path: `LoadLibraryA();`

Full DLL: `Get..Offset();`

Process A

DLL

Step 4

Process B

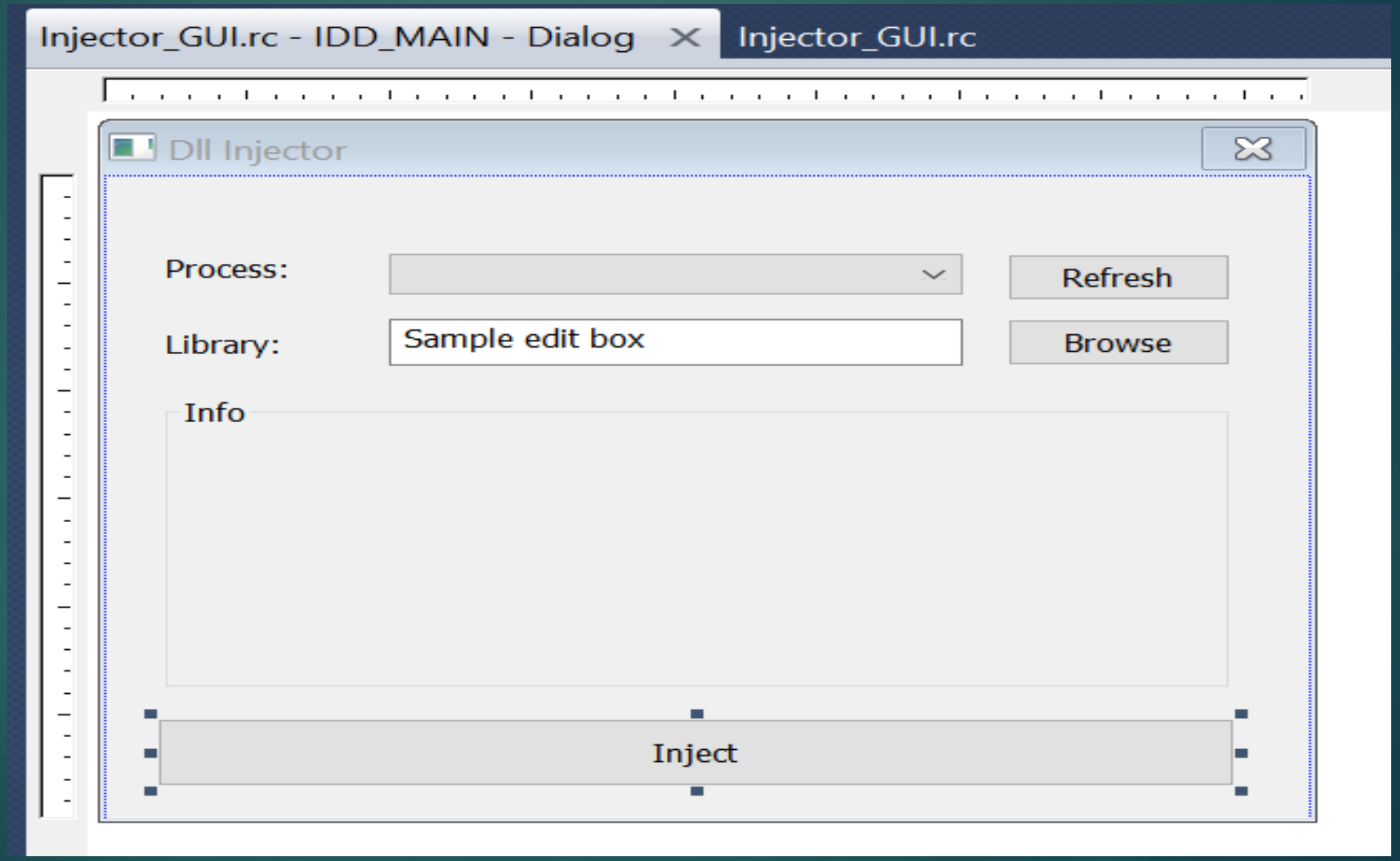
Execute

`CreateRemoteThread();`
`NtCreateThreadEx();`
`RtlCreateUserThread();`
`.`
`.`
`.`

Process A

DLL

Create Dll Injection tool:



Normal
Task Manager

Infected
Task Manager

Process A

Process B

Process C

Process A

Process B

Process C

Hiding files and directories :

Normal
Files Manager

File A

File B

File C

Infected
Files Manager

File A

File B

File C

Hiding registry entries

Normal Registries Viewer

Entry A

Entry B

Entry C

Infected Registries Viewer

Entry A

Entry B

Entry C

Attacker
(Windows 10)

Victim
(Windows 7)

Http (Get, Post)

Command Encrypted with Double Base64

: Antivirus

- هو برنامج أمن (security) يهدف إلى إعطاء حماية أفضل من تلك التي يوفرها نظام التشغيل الأساسي التي تستخدم كحل وقائي ومع ذلك عندما يفشل الحل الوقائي يتم استخدام برنامج antivirus لتطهير البرامج المصابة أو إزالة البرامج الضارة من نظام التشغيل .
- برنامج الantivirus يستخدم تقنيات مختلفة لتحديد البرامج الخبيثة (malicious software) التي غالبا تملك خاصية الحماية الذاتية وتخفي نفسها في عمق نظام التشغيل .
- البرامج الضارة المتقدمة (malware) ربما تستخدم وظائف نظام التشغيل غير الموثقة (undocumented functions) وتقنيات غامضة من أجل الاستمرار وتجنب الكشف عنها .
- وبسبب انتشار الهجمات على نطاق واسع هذه الأيام تم تصميم برامج Antivirus للتعامل مع جميع أنواع الحمولة الخبيثة (malicious payloads) الآتية من مصادر موثوقة أو غير موثوقة .
- بعض المدخلات الخبيثة التي يحاول ال Antivirus حماية نظام التشغيل منها هي الحزم الشبكية , مرفقات البريد الإلكتروني و استغلال الثغرات في مستعرضات الويب , فضلا عن البرامج القابلة للتنفيذ التي قد تقوم بأفعال قد تؤدي إلى تلف نظام التشغيل ..... .
- مكونات الAntivirus وهي النواة, command-line scanner , GUI scanner , daemons , file system filter drivers , network filter drivers , وأي أدوات دعم أخرى.

المفهوم المغلوط حول برامج ال Antivirus :

- معظم المستخدمون يعتقدون أن المنتجات الأمنية ستصمد ضد جميع المخاطر و إنه بمجرد تنصيب برامج ال Antivirus سيتم الحفاظ على حواسيبهم بأمان , هذا الاعتقاد ليس سليم تماما .
- و لتوضيح لماذا برامج الAntivirus قد لا تصمد في وجه جميع المخاطر الأمنية سوف نلقي نظرة حول المهام التي يؤديها برنامج Antivirus حديث :

1- اكتشاف القوالب المعروفة لل malicious و السلوكيات السيئة في البرامج.

2- اكتشاف القوالب المعروفة الخبيثة في الوثائق وصفحات الويب .

3- اكتشاف القوالب المعروفة الخبيثة في الحزم الشبكية .

4- محاولة التكيف واكتشاف سلوكيات وقوالب سيئة جديدة بالاعتماد على تجارب سابقة .

كما نلاحظ أنه تم استخدام الكلمة (معروفة) في كل مهام الAntivirus بالتالي قد لا تكون منتجات ال Antivirus صامدة في وجه البرمجيات الخبيثة غير المعروفة و التسويق لهذه المنتجات قد يجعل المستخدم يظن أنها ستحمي حاسوبه ضد كل المخاطر الأمنية ولكن هذا بعيد كل البعد عن الحقيقة .

بعض خصائص منتجات الAntivirus

- القدر على مسح الملفات المضغوطة والتنفيذية .
- أدوات للقيام بمسح الملفات أو المجلدات عند الرغبة وفي الزمن الحقيقي .
- حماية ذاتية ضد البرامج الضارة (malware) .
- جدار حماية .
- موجه أوامر و واجهة رسومية .
- وحدة تحكم للإدارة .
- الخفة وتحقيق الخدمة المطلوبة .

ميزات متقدمة للAntivirus

- فلاتر الحزم والجدار الناري (packet filters and firewalls) : ظهر نوع جديد من البرامج الضارة يدعى الديدان (worms) التي شكلت نقاط ضعف لبعض البرامج المستهدفة , و لأن العديد من الديدان تستخدم موارد الشبكة لإصابة الحواسيب , لذلك قررت صناعة ال Antivirus فحص تدفق الشبكات الصادر والوارد .
- الحماية الذاتية (self protection) : الAntivirus يحاول حماية مستخدمي الحاسوب من البرامج الضارة (malware) و أيضا البرامج الضارة تحاول حماية نفسها من الAntivirus , في بعض الحالات البرامج الضارة سوف تحاول قتل (kill) العمليات المتعلقة بالAntivirus لتعطيله , لذلك يجب على الAntivirus حماية نفسه من عمليات التعطيل الشائعة .
- مضاد استغلال (Anti- explolting).

فهم تواقيع الAntivirus

- التواقيع هي جزء أساسي لأي محرك Antivirus , وهي توابع تقطيع صغيرة (small hashes) أو byte_streams التي تحوي معلومات كافية لتحديد فيما إذا كان الملف أو ال buffer يطابق قالب برنامج ضار معروف .
- بعض الخوارزميات التي تستخدم لتوليد تواقيع يمكن أن تملك نسبة عالية من الخطأ الإيجابي (false positive) لكنها سريعة للغاية .
- يوجد تواقيع أخرى أكثر تعقيدا لكنها ذات كلفة عالية ومعدل من الخطأ الإيجابي (false positive) أقل لكن تستغرق وقت طويل لتوليدها .

أنواع التواقيع

- Byte stream : الشكل الأبسط للتوقيع وهي خاصة لملف ال malware والتي تظهر عادة كملفات غير ضارة , بطبيعة الحال هو أسهل أسلوب للكشف عن ال malware هو سريع و سهل التحقيق (aho corasick, knuth pratt ,boyer moore) .
- Check sums : الخوارزمية الأكثر استخداما لمطابقة التوقيع من قبل معظم محركات الAntivirus التي تعتمد على حساب ال CRCs لتحديد الخطر وحالات التعديل على البيانات و أخطاء الإرسال ....
- Custom check sums : معظم الAntivirus تنشئ مجموعة من CRC like signatures
- Cryptographic hashes :تولد توقيع يؤدي إلى نتيجة واحدة تحدد buffer واحد مما يقلل فرص إنتاج الخطأ الإيجابي (false positive) بسبب قلة التصادمات وهذا النوع يملك أربع خصائص :

1- من السهل حساب قيمة ال hash لأي رسالة معطاة .

2-لا يمكن إيجاد الرسالة من خلال hashمعطى .

3- لا يمكن تغيير الرسالة دون إعادة حساب ال hash .

4-من غير الممكن أن يكون لرسالتين مختلفتين نفس ال hash .

تواقيع متقدمة (advanced signatures)

- Fuzzy hashing .
- Graph based hashes for executable files .

1- call graph : مخطط بياني موجه يظهر العلاقات بين كل التوابع في البرنامج
(مخطط يعرض جميع المستدعيين و الاستدعاءات لكل تابع في قطعة برمجية).

2- flow graph : مخطط بياني موجه يظهر العلاقات بين الكتل الأساسية لتابع محدد .

Antivirus Software Evasion

- . Evading Signatures
- . Evading Scanners
- . Evading Heuristic Engines