



# دليل الاستجابة للحوادث السيبرانية

## Incident Response Guide

تأليف واعداد: ثامر الشمري

Twitter:T44T\_

٥	.....المقدمة
٦	.....مدخل
٧	..... منهجية الاستجابة للحوادث السيبرانية (NIST STANDARD)
٧	..... الاستعداد:
٧	..... الاكتشاف والتحليل:
٧	..... الاحتواء والازالة والتعافي:
٨	..... الدروس المستفادة والتقارير:
٨	..... أبرز الحوادث السيبرانية الشائعة وطرق التعامل معها
٨	.....1- البريد الالكتروني
٨	..... أ.البريد التصيدي (Phishing)
٩	..... ب.البريد المزجج أو اقتحامي (Spam)
١٠	..... ت.الحملات الهجومية (Campaign)
١٠	..... ث.الاستهداف (Targeting)
١١	.....2- الشبكة
١١	..... أ.التحكم والسيطرة (C&C/Callback)
١٢	..... ب.الدودة الرقمية(Worms)
١٣	..... ت.فايروس الفدية (Ransomware)
١٤	..... ث.هجوم كسر كلمة المرور (Brute Force Attack)
١٤	..... ج.برمجيات التعدين (Minar)
١٤	..... ح.برمجيات المزعجة (Ads, PUP)
١٤	.....3- الهندسة الاجتماعية ( Social Engraining )
١٥	.....4- خدمات الويب.....
١٥	..... أ.حجب الخدمة (DDos Attack)
١٦	..... ب.تشويه مواقع الانترنت (Defaced)
١٧	.....5- تسريب البيانات (Information Leakage)
١٧	..... اشياء لا يجب عملها اثناء الاستجابة للحوادث السيبرانية
١٨	..... إيقاف سلسلة الهجوم (CYBER KILL-CHAIN)
١٨	..... تصنيف الثغرات الأمنية

٢٠	خطوات تخفيف المخاطر (MITIGATION)
٢١	تحديد أولويات الاستجابة للحوادث
٢١	أبرز الأدوات والمواقع المقترحة للتحليل والأكتشاف
٢١	ادوات لجمع مؤشرات الاختراق (IOC)
٢٢	أ. Sysinternals utilities
٢٢	ب. AVZ
٢٣	ت. YARA
٢٣	ادوات لعمل نسخة من النظام والذاكرة
٢٤	أ. GRR Rapid Response
٢٤	ب. Forensic Toolkit
٢٥	ت. DumpIt
٢٥	ث. Kape
٢٦	ادوات ومواقع لتحليل التهديدات المحتملة والبرامج الخبيثة
٢٦	أ. Kaspersky Threat Intelligence Portal
٢٧	ب. VirusTotal
٢٨	ت. Anyrun
٢٨	ث. HyberAnalsis
٢٩	ج. Cuckco
٢٩	ادوات لتحليل الذاكرة العشوائية
٢٩	أ. Volatility
٣٠	ب. Rekall
٣٠	ادوات لتحليل القرص الصلب
٣٠	• The Sleuth Kit(TSK)
٣١	ادوات للبحث عن النصوص (Strings)
٣١	• Strings Utility
٣١	تقارير معلومات استباقية (Threat Intelligence Reports)
٣٢	مصطلحات
٣٢	المصادر

تُركت هذه الصفحة فارغة عمدًا

# شكر وتقدير

كل الشكر والتقدير والعرفان للأصدقاء اللي ساعدوني في أنجاز هذا الدليل بالتدقيق والمراجعة والاضافة.

مالك الدوسري

[@Malajab](#)

محمد السحيبي

[@Msuhaymi](#)

لا يخفى على الجميع أهمية الامن السيبراني في الوقت الحالي حيث ان مع تطور التقنية تزداد الحاجة الى وجود بيئة سيبرانية امنة وموثوقة، وتشير الاحصائيات مؤخرا ان معدل الحوادث السيبرانية ازداد بشكل ملحوظ لذلك وجدت الحاجة لإيجاد دليل ارشادي للاستجابة للحوادث بالشكل الصحيح، والتأكد من تطبيقها بشكل صحيح وذلك لضمان التعافي وعدم عودة المهاجم مره اخرى للبيئة المستهدفة.

تمت كتابة هذا الدليل الإرشادي ليساعد محللين الأمن السيبراني للاستجابة للحوادث السيبرانية ويقدمها كخطوات تسلسلية مرتبة. ولا يخفى على الجميع بأن الحوادث تختلف فيما بينها مما يصعب كذلك حصر طرق الاستجابة ولا يوجد طريقة واحدة فقط متبعة ومعتمدة بل ان لكل حادثة طريقة مختلفة الى حد ما، وننوه بأن الطرق المذكورة هنا غالباً هي المستخدمة في الاستجابة، لذا يجب ان نشير بأن الاستجابة والتعامل مع الحادثة مبني على خبرات متراكمه من محلي الاستجابة للحوادث، وقد توجد له رؤية مختلفة في بعض الاحيان والدليل هنا يفترض بأن القارئ لديه الخبرة والمهارات الاساسية للاستجابة للحوادث السيبرانية كالتحليل وغيرها.

## منهجية الاستجابة للحوادث السيبرانية (NIST standard)



### الاستعداد:

تدريب وتجهيز فريق الاستجابة للحوادث السيبرانية، حصر الاصول التقنية في البنية التحتية للأنظمة والشبكات والتطبيقات وبالأخص الحساس منها والتأكد من استيفاء الشروط الخاصة بضوابط الامن السيبراني وتجهيز برمجيات خاصة بالاستجابة للحوادث السيبرانية وكذلك التحقق من وجود سجلات من جميع البرمجيات والخوادم بالإضافة بناء خطة للاستجابة للحوادث السيبرانية عند وقوعها.

### الاكتشاف والتحليل:

يتم الاكتشاف والتحليل حسب المراحل ادناه:

- المراقبة
- الرصد والاكتشاف
- التحليل
- التقرير الاولي

### الاحتواء والازالة والتعافي:

- حصر الاصول التقنية المصابة وتحديدتها.
- اخذ نسخة رقمية للأجهزة المصابة والبدء بتحليلها.
- تحليل البرمجيات والملفات الضارة.
- حصر مؤشرات الاختراق.
- حجب مؤشرات الاختراق من الشبكة.
- التأكد من خلو الشبكة من مؤشرات الاختراق.
- عزل الأنظمة المصابة.

- إعادة تهيئة الانظمة المصابة.
- تفعيل خطة التعافي

## الدروس المستفادة والتقارير:

- عمل تقرير شامل عن الحادثة.
- مراقبة جميع الأنشطة المشبوهة التي تم اكتشافها من الحادثة من خلال مركز السجلات المركزية.
- حصر الدروس المستفادة من الحادثة.

## أبرز الحوادث السيبرانية الشائعة وطرق التعامل معها

تم تقسيم الحوادث السيبرانية الى خمسة اقسام رئيسية وهي:

- ١- البريد الالكتروني
- ٢- الشبكة
- ٣- الهندسة الاجتماعية
- ٤- خدمات الويب
- ٥- تسريب البيانات

### ١- البريد الالكتروني

يعتبر البريد الالكتروني الوسيلة المفضلة لدى المهاجمين للوصول الى الشبكة لذا تعتبر من أهم القنوات التي يجب زيادة الحماية فيها.



### تصنيف البريد الالكتروني الضار:

- البريد التصيدي (Phishing)
- البريد المزعج أو اقتحامي (Spam)
- الحملات الهجومية (Campaign)
- الاستهداف (Targeting)

#### أ. البريد التصيدي (Phishing)

التنكر على هيئة جهة جديرة بالثقة عن طريق رسائل بريد إلكترونية للحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور أو تفاصيل بطاقة الائتمان وذلك لأسباب ونوايا ضارة.

## السيناريو الأول:

في حال ان المستخدم أستقبل الرسالة وتفاعل مع البريد الالكتروني التصيدي بالضغط على الرابط أو فتح المرفق، عليك اتباع الارشادات ادناه:

### الاجراء:

- عزل النظام عن الشبكة.
- تغيير كلمة السر الخاصة بالمستخدم وكذلك اي كلمات سر مستخدمة او محفوظه بالنظام.
- فحص الملفات أو الروابط المتضمنة بالبريد من خلال معمل خاص لفحص الفيروسات ومعزول عن الشبكة الداخلية والعمل على استخراج مؤشرات الاختراق IOCs.
- التحليل من خلال مركز السجلات المركزية (SEIM) من اتصالات مشبوهة انشئت من قبل نظامه او أجهزة أخرى داخل المنظمة.
- التأكد من عدم وجود أي حالات تصيد مشابهة في البريد الالكتروني للمستخدمين الاخرين من خلال إدارة بوابة البريد الالكتروني وفي حال وجود مستقبلين اخرين يتم ارسال تنبيه أمني بعدم التجاوب والابلاغ.
- حجب مصدر الرسالة وكذلك الروابط الضارة من خلال انظمة الحماية.
- فحص النظام من خلال برمجيات الحماية والتأكد من خلوها من برمجيات الضارة.
- استعادة النظام المصاب للشبكة بعد التأكد من خلوها من الأنشطة الضارة.

## السيناريو الثاني:

في حال ان المستخدم أستقبل الرسالة ولم يتفاعل مع البريد الالكتروني عليك اتباع الارشادات ادناه:

### الاجراء:

- فحص الملفات أو الروابط المتضمنة بالبريد من خلال معمل خاص لفحص الفيروسات ومعزول عن الشبكة الداخلية واستخراج مؤشرات الاختراق IOCs.
- التأكد من ان المستخدمين لم يقوموا بالتفاعل سواء القيام بفتح الرابط الضار او الملفات المرفقة أو بالرد على المرسل وتستطيع التحقق من ذلك من خلال مركز السجلات المركزية (SEIM) او إدارة البوابة الالكتروني للبريد.
- التأكد من عدم وجود أي حالات تصيد مشابهة في البريد الالكتروني للمستخدمين الاخرين من خلال إدارة بوابة البريد الالكتروني وفي حال وجود مستقبلين اخرين يتم ارسال تنبيه أمني بعدم التجاوب والابلاغ.
- حجب مصدر الرسالة وكذلك الروابط الضارة من خلال انظمة الحماية.

## السيناريو الثالث:

في حال وجود بلاغ أمني من مستخدم بوجود رسائل بريدية يشته بها مع معرفته مصدر البريد ويتوقع استقباله لذا يتم التعامل مع البلاغ كالآتي:

### الاجراء:

- تحليل مصدر الرسالة والتأكد من العنوان المرسل منه حقيقي او مزيف من خلال ترويسة البريد (Email Header).
- تحليل الملفات او الروابط من خلال معمل لتحليل الفايروسات بنظام خارج الشبكة والتأكد من خلوها من اي ملفات ضارة.

## ب. البريد المزعج أو اقتحامي (Spam)

هو استخدام أنظمة الإرسال الإلكترونية لإرسال رسائل لا يرغب المستخدم بتلقيها.

## الاجراء:

يتم حجب مصدر الرسالة من قبل برامج الحماية أو من خلال تطبيق البريد الالكتروني من قبل المستخدم وتحويل اي رسالة تأتي من المرسل لصندوق البريد المزعج.

## ت. الحملات الهجومية (Campaign)

هي هجمات منسقة تستهدف عدد من المستخدمين بهدف الحصول على معلومات حساسة او سرقة معلومات شخصية.

## الاجراء:

- تحديد المستخدمين الذين استقبلوا الرسالة من خلال بوابة البريد الالكتروني وارسال تنبيه لهم بعدم التعامل مع رسائل مجهولة المصدر.
- فحص الملفات أو الروابط المتضمنة بالبريد من خلال معمل خاص لفحص الفيروسات ومعزول عن الشبكة الداخلية واستخراج مؤشرات الاختراق IOCs.
- التحليل من خلال مركز السجلات المركزية (SEIM) من اتصالات مشبوهة انشئت من قبل نظامه او أجهزة أخرى داخل المنظمة.
- حجب مصدر الرسالة وكذلك الروابط الضارة من خلال برمجيات الحماية.

## ث. الاستهداف (Targeting)

هو استهداف شخص او مجموعة اشخاص ببريد الالكتروني ضار بهدف إيصال برمجية ضارة او سرقة معلومات حساسة.

## السيناريو الأول:

في حال ان المستخدم أستقبل الرسالة ولم يتفاعل مع البريد الالكتروني عليك اتباع الارشادات ادناه:

## الاجراء:

- فحص الملفات أو الروابط المتضمنة بالبريد من خلال معمل خاص لفحص الفيروسات ومعزول عن الشبكة الداخلية واستخراج مؤشرات الاختراق IOCs.
- التأكد من ان المستخدمين لم يقوموا بالتفاعل سواء القيام بفتح الرابط الضار او الملفات المرفقة أو بالرد على المرسل وتستطيع التحقق من ذلك من خلال مركز السجلات المركزية (SEIM) او إدارة البوابة الالكتروني للبريد.
- التأكد من عدم وجود أي حالات تصيد مشابهة في البريد الالكتروني للمستخدمين الاخرين من خلال إدارة بوابة البريد الالكتروني وفي حال وجود مستقبلين اخرين يتم ارسال تنبيه أمني بعدم التجاوب والابلاغ.
- حجب مصدر الرسالة وكذلك الروابط الضارة من خلال انظمة الحماية.

## السيناريو الثاني:

في حال ان المستخدم أستقبل الرسالة وتفاعل مع البريد الالكتروني بالضغط على الرابط أو فتح المرفق، عليك اتباع الارشادات ادناه:

## الاجراء:

- يتم عزل نظام الموظف عن الشبكة.
- تغيير كلمة السر الخاصة بالمستخدم وكذلك اي كلمات سر مفعلة او محفوظه بالنظام.
- فحص الملفات أو الروابط المتضمنة بالرسالة من خلال معمل خاص لفحص الفيروسات المعزول عن الشبكة الداخلية واستخراج مؤشرات الاختراق IOCs.
- التحليل من خلال مركز السجلات المركزية (SEIM) من اتصالات مشبوهة انشئت من قبل نظامه او أجهزة أخرى.
- التأكد من عدم استقبال الرسالة من موظفين آخرين من خلال بوابة البريد الالكتروني وفي حال وجود مستقبلين اخرين يتم ارسال تنبيه أمني لهم بعدم فتح الرسالة وعدم التعامل مع رسائل البريد.
- حجب مصدر الرسالة وكذلك الروابط الضارة من خلال برمجيات الحماية.
- اعادة تهيئة النظام في حال تم التأكد في وجود اصابة برمجيات خبيثة في النظام.

## ٢- الشبكة

في حال ظهور أي تنبيهات أمنية من خلال احدى برمجيات الحماية مثل ( AV, EDR, Email & Network security).



## انواع الهجمات:

- التحكم والسيطرة (Callback)
- الدودة الرقمية (Worms)
- فايروس الفدية (Ransomware)
- هجوم كسر كلمة المرور (Brute Force Attack)
- برمجيات التعدين (Minar)
- برمجيات المزعجة (Ads, PUP)

## أ. التحكم والسيطرة (C&C/Callback)

تبدأ البرمجيات الضارة بعد اصابة الجهاز بالاتصال مع خادم المهاجم لأرسال واستقبال الأوامر.

## - الاستعداد:

- تحديد جهات الاتصال لأجل التواصل السريع والتي تشمل فريق الشبكات، الانظمة، أمن المعلومات وفريق المطورين.
- المعرفة الكاملة بتصميم الشبكة الداخلية.
- التأكد من تحديث جميع برمجيات الأنظمة الأمنية.

#### - الاكتشاف والتحليل:

تحليل الاتصالات الخارجة والقادمة للنظام لمعرفة حجم الأثر الذي تسبب فيه الاختراق من خلال مركز سجلات المركزية.

#### - الاحتواء والازالة والتعافي:

- فصل النظام عن الشبكة (من خلال EDR أو يدويا).
- حجب العناوين المشبوه الذي تواصل معه نظام المصاب.
- تهيئة كلمات السر لجميع الحسابات المفعلة بالنظام وحسابات مدراء الأنظمة في حال رصد استخدامها.
- الاستحواذ على نسخة من النظام المصاب ونسخة من الذاكرة العشوائية RAM.
- استخراج IOCs من خلال الأدلة الموجودة بالنظام المصاب والشبكة وعمل فحص على البيئة من خلال برمجيات مثل AV، YARA Rule، EDR .
- تهيئة النظام أو استعادة نسخة احتياطية بعد التأكد من سلامة بياناتها.
- تفعيل خطة التعافي من الحادثة.
- الدروس المستفادة من الحادثة.
- مراقبة الشبكة من اي أنشطة مشبوه.

#### ب. الدودة الرقمية (Worms)

دودة الحاسوب هي برامج صغيرة قائمة بذاتها غير معتمدة على غيرها صنعت للقيام بأعمال تدميرية أو لغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم للإنترنت أو إلحاق الضرر بهم أو بالمتصلين بهم، تمتاز بسرعة الانتشار ويصعب التخلص منها.

#### - الاستعداد:

- تحديد جهات الاتصال لأجل التواصل السريع والتي تشمل فريق الشبكات، الانظمة، أمن المعلومات وفريق المطورين.
- المعرفة الكاملة بتصميم الشبكة الداخلية.
- التأكد من تحديث جميع برمجيات الأنظمة الأمنية.

#### - الاكتشاف والتحليل:

- تحليل الاتصالات الخارجة والقادمة للنظام لمعرفة حجم الأثر الذي تسبب فيه الاختراق من خلال مركز سجلات الأحداث.
- تحديد نوع الفايروس وكيفية انتشاره داخل الشبكة.

#### - الاحتواء والازالة والتعافي:

- عزل الشبكة المصابة (Zone area) من الوصول للإنترنت.
- فصل النظام عن الشبكة (من خلال EDR أو يدويا).
- عزل الشبكة المصابة (Zone area) من الشبكة الداخلية.
- تحييد الانتشار في الشبكة من خلال عمل تحديث للأنظمة الغير مصابة وحجب الاتصالات وايقاف تشغيل الاجهزة.
- حجب العناوين المشبوه الذي تواصل معه نظام المصاب.
- الاستحواذ على نسخة من النظام المصاب ونسخة من الذاكرة العشوائية RAM.
- تهيئة كلمات السر لجميع الحسابات المفعلة بالنظام وحسابات مدراء الأنظمة في حال رصد استخدامها.

- معرفة طرق الازالة من خلال مراسلة الدعم للمنتجات المستخدمة في المنظمة "مثل مايكروسوفت" او البحث في المواقع المتخصصة في الحماية.
- استخراج IOCs من خلال الادلة الموجودة بالنظام المصاب والشبكة وعمل فحص على البيئة من خلال برمجيات أمنية مثل AV, EDR, YaRa Rule.
- تهيئة النظام أو استعادة نسخة احتياطية بعد التأكد من سلامة بياناتها.
- بعد التأكد من احتواء الفيروس يتم استرجاع الشبكة المعزولة للبيئة الحية.
- سماح الوصول للأنترنت للشبكة المعزولة.
- الدروس المستفادة من الحادثة.
- مراقبة الشبكة من اي أنشطة مشبوه.

### ت. فايروس الفدية (Ransomware)

برمجيات ضارة تجعل بيانات وأنظمة الضحية غير قابلة للاستخدام لحين دفعة لمبلغ مالي .

- **الاستعداد:**
  - تحديد جهات الاتصال لأجل التواصل السريع والتي تشمل فريق الشبكات، الانظمة، أمن المعلومات وفريق المطورين.
  - المعرفة الكاملة بتصميم الشبكة الداخلية.
  - التأكد من تحديث جميع برمجيات الأنظمة الأمنية.
- **الاكتشاف والتحليل:**
  - تحليل الاتصالات الخارجة والقادمة للنظام لمعرفة حجم الأثر الذي تسبب فيه الاختراق من خلال مركز سجلات الأحداث.
  - تحديد نوع الفايروس وكيفية انتشاره داخل الشبكة.
- **الاحتواء والازالة والتعافي:**
  - عزل الشبكة المصابة (Zone area) من الوصول للأنترنت.
  - فصل النظام عن الشبكة (من خلال EDR أو يدويا).
  - عزل الشبكة المصابة (Zone area) من الشبكة الداخلية.
  - حجب العناوين المشبوه الذي تواصل معه نظام المصاب.
  - تحييد الانتشار في الشبكة من خلال عمل تحديث للأنظمة الغير مصابة وحجب الاتصالات وايقاف تشغيل الاجهزة.
  - تهيئة كلمات السر لجميع الحسابات المفعلة بالنظام وحسابات مدراء الأنظمة في حال رصد استخدامها.
  - الاستحواذ على نسخة من النظام المصاب ونسخة من الذاكرة العشوائية RAM.
  - استخراج IOCs من خلال الادلة الموجودة بالنظام المصاب والشبكة وعمل فحص على البيئة من خلال برمجيات أمنية مثل AV, EDR, YaRa Rule.
  - معرفة طرق الازالة من خلال مراسلة الدعم للمنتجات المستخدمة في المنظمة "مثل مايكروسوفت" او البحث في المواقع المتخصصة في الحماية.

- استعادة نسخة احتياطية بعد التأكد من سلامة بياناتها.
- في حال الرغبة باستعادة الملفات المشفرة يتم البحث عن برمجيات فك التشفير.
- بعد التأكد من احتواء الفيروس يتم استرجاع الشبكة المعزولة للبيئة الحية.
- سماح الوصول للإنترنت للشبكة المعزولة.
- الدروس المستفادة من الحادثة.
- مراقبة الشبكة من اي انشطة مشبوه

### ث. هجوم كسر كلمة المرور (Brute Force Attack)

قيام المهاجم بمحاولات متعددة ومؤتمته لكسر كلمات المرور وذلك لغرض الوصول الغير مصرح به للحسابات.  
الاجراء:

- حجب عنوان المهاجم.
- البحث عن كيفية معرفة المهاجم عن حساب المستخدم في الهجوم.(قد يكشف وجود تسريب للبيانات)
- تحديد عدد المحاولات الخاطئة لأغلاق الحسابات في حال وجود هجمات كسر كلمات المرور.

### ج. برمجيات التعدين (Minar)

استغلال موارد الجهاز ببرمجيات ضارة بهدف القيام بعمليات تعدين العملات الرقمية.  
الاجراء:

- إرسال تنبيه أمني للدعم الفني لفحص النظام لأزالة البرمجيات الضارة.
- يتم حجب الموقع الالكتروني المصاب الذي يحتوي على برمجيات التعدين.
- يتم مراسلة صاحب الموقع بوجود برمجيات ضارة تم زرعها في داخل الموقع الالكتروني.

### ح. برمجيات المزعجة (Ads, PUP)

برمجيات مزعجة تقوم بتثبيت نفسها بتدخل أو بدون تدخل المستخدم ، وذلك لأهداف الإعلانات أو التجسس .  
الاجراء:

- إرسال تنبيه أمني للدعم الفني لفحص النظام والتأكد من سلامته من البرمجيات الغير مرغوبة.

## ٣- الهندسة الاجتماعية ( Social Engraining )

يقوم المهاجمين باستخدام إحدى منصات التواصل الاجتماعي لمحاولة خداع المستخدمين.



### السيناريو الأول:

المهاجم قام بالتسجيل في إحدى المواقع الاجتماعية وأدعى بأنه ينتمي للجهة الخاصة بك.

### الاجراء:

- تتواصل الجهة من خلال حسابها الرسمي مع الدعم الفني للموقع وأبلغهم بأن المستخدم لا ينتمي اليهم ويجب اغلاق الحساب.

### السيناريو الثاني:

المهاجم يدعي بأنه ينتمي الى جهة ما وقام بالتواصل مع إحدى الموظفين لديك لأجل تقديم عرض وظيفي وقام المهاجم بإرسال ملف وورد ضار لأجل الوظيفة الجديدة، واكتشفت إحدى برمجيات الحماية الملف الضار وقامت بإيقافه قبل أن يتم فتحه واصدرت تنبيه على ذلك.

### الاجراء:

- استخراج IOCs من الملف وعمل فحص على البيئة من خلال برمجيات أمنية مثل AV , EDR, YaRa Rule.
- ارسال تنبيه لجميع الموظفين بعدم التعامل مع المهاجم.

### السيناريو الثالث:

المهاجم يدعي بأنه ينتمي الى جهة ما وقام بالتواصل مع إحدى الموظفين لديك لأجل تقديم عرض وظيفي وقام المهاجم بإرسال ملف وورد ضار لأجل الوظيفة الجديدة، واكتشفت إحدى برمجيات الحماية الملف الضار واصدرت تنبيه على ذلك ولم تقم بإيقافه.

### الاجراء:

- الاستجابة تعتمد على نوع الملف الضار الذي قام الموظف بفتحه وبناءا على ذلك يتم التعامل معها.(Callback, Worm, Phishing etc.).

## ٤- خدمات الويب

تعتبر مواقع الأنترنت هي البوابة الخارجية التي من خلالها يستطيع المهاجم من الحاق الضرر بالجهة المستهدفة لذا تعتبر من أهم البوابات التي يجب حمايتها.



### أ. حجب الخدمة (DDos Attack)

محاولة لتعطيل النظام ، وجعل خدماته غير متوافرة عن طريق إرسال طلبات كثيرة من أكثر من مصدر في الوقت نفسه.

### - الاستعداد:

- التواصل مع مقدم مزود خدمة الانترنت لمعرفة ماهي الخدمات المقدمة لتصدي لهجمات حجب الخدمة وماهي الاجراءات التي يجب اتباعها عند التعرض لهجوم.
- انشاء قائمة من العنواين البيضاء والمنافذ التي يجب تصفيتها عند حدوث اي هجمة.
- تحديد جميع تفاصيل البنية التقنية من أصحاب الخوادم والخدمات وتصميم الشبكة.
- تحصين الخوادم والانظمة والشبكة التي قد تستهدف للهجوم.
- معرفة حجم تدفق البيانات الطبيعي في الشبكة لأجل اكتشاف اي ارتفاع مفاجئ في حجم التدفق والذي يشير بوجود هجمة قائمة.
- تحديد جهات الاتصال لأجل التواصل السريع والتي تشمل مزود خدمة الانترنت وفريق الشبكات والانظمة وفريق أمن المعلومات.
- تجهيز خطة الاستجابة للخدمات في حال تعرضها للهجوم.

#### - الاكتشاف والتحليل:

- تحديد العنواين والمنافذ والروابط وكذلك البروتوكول المستخدمة في الهجوم.

#### - الاحتواء والازالة والتعافي:

- حجب العنواين أو المنافذ المستخدمة في الهجوم من خلال برمجيات الانظمة الأمنية.
- تصفية الاتصالات القادمة للحد من أثر هجمات تعطيل الخدمة من خلال قائمة عنواين بيضاء او جغرافياً.
- تحويل حركة المرور الى خدمات التي تساعد في صد مثل هذه الهجمات.
- التواصل مع مزود خدمة الانترنت للتصدي للهجمة.
- اعادة جميع الخدمات المتأثرة الى حالتها السابقة مع التأكد بعدم وجود بطئ في الشبكة.
- الدروس المستفادة من الحادثة.
- مراقبة الشبكة من اي انشطة مشبوه

#### ب. تشويه مواقع الانترنت (Defaced)

الوصول الغير مصرح به لمواقع الإنترنت وتغير محتوى الصفحة.

#### - الاستعداد:

- تجهيز نسخة احتياطية محدثة للموقع الالكتروني لاستخدامها بشكل سريع.
- تحديد اجراءات معتمدة لتحويل الزوار الى النسخة الاحتياطية.
- استخدام برمجيات تكتشف بشكل عاجل اي تعديل في المحتوى قد يحدث في الموقع الالكتروني.

#### - الاكتشاف والتحليل:

- مراقبة محتوى صفحات المواقع الالكترونية لاكتشاف اي تعديل.
- فحص قواعد البيانات من وجود اي ملفات خبيثة.

#### - الاحتواء والازالة والتعافي:

- عزل خادم الويب المصاب عن الشبكة.
- حجب العنواين المرتبطة بالهجوم.
- الاستحواذ على نسخة من النظام المصاب ونسخة من الذاكرة العشوائية RAM.
- استخراج IOCs من خلال الادلة الموجودة بالنظام المصاب والشبكة وعمل فحص على البيئة من خلال برمجيات أمنية مثل AV , EDR, YaRa Rule.
- البحث عن كيفية طريقة دخول المهاجم في الخادم والبدء في اصلاح المشكلة.
- التأكد من أن الثغرة المستخدمة في الهجوم ليست متواجدة في مواقع اخرى.
- مراجعة جميع الخدمات المرتبطة في الخادم المصاب، والتأكد من عدم اصابتها.
- اعادة تهيئة جميع كلمات المرور للحسابات المرتبطة بالخادم.
- تفعيل نسخة خادم الويب الاحتياطية واسترجاع الخدمة.
- الدروس المستفادة من الحادثة.

- مراقبة الشبكة من اي انشطة مشبوه

## ٥- تسريب البيانات (Information Leakage)

تسريب البيانات عبارة عن نقل بيانات من المنظمة الى جهة خارجية غير مصرح لها الاطلاع عليها.



- الاستعدادات:
  - تصنيف البيانات داخل المنظمة.
  - تجهيز خطة استجابة للبيانات المسربة.
  - الاشتراك في خدمات استخبارات التهديد (Threat Intelligence) لمعرفة اي تسريب بيانات للمنظمة.
  - تطبيق برمجيات أمنية لمنع حدوث تسرب البيانات.

- الاكتشاف والتحليل:
  - تحديد سبب التسرب هل حدث من الداخل أو من طرف ثالث.
  - البحث من خلال محركات البحث او قواعد بيانات خارجية لأي تسرب بيانات.
  - اداة منع تسرب البيانات تساعد في اكتشاف سبب التسرب (DLP).

- الاحتواء والازالة والتعافي:
  - تعليق حساب الموظف بعد التأكد أن التسرب حدث من خلاله.
  - عزل الجهاز لعمل تحليلات جنائية رقمية على النظام.
  - اعادة تهيئة كلمات السر للحسابات التي ظهرت في التسرب.
  - التواصل مع الموقع الالكتروني التي تم كشف البيانات فيه لحذف البيانات فوراً.
  - تحليل البيانات المسربة واتخاذ اللازم لجعلها عديمة الفائدة.

## اشياء لا يجب عملها اثناء الاستجابة للحوادث السيبرانية

- عدم إيقاف الانظمة المصابة بل يفضل عزلها عن الشبكة بعد التحليل الاولي للحادثة.
- عند أخذ نسخة كاملة من النظام لا يجب العبث بها وانما يتم اخذ نسخة اضافية لأجل التحليل.
- التأكد بعد اخذ نسخة من الذاكرة العشوائية RAM بعدم وجود تشفير على مستوى القرص الصلب وفي حال وجوده يجب عمل نسخة للنظام قبل إيقاف تشغيله.
- استخدام حسابات مدراء الانظمة للاستجابة للحادثة.
- تشغيل برمجيات على الانظمة المصابة غير مخصصة للاستجابة للحوادث.
- استرجاع نسخة احتياطية من النظام المصاب مما يسبب في عودة المهاجم بعد عملية التعافي، بل يجب فحص والتأكد من سلامة النسخة الاحتياطية من وجود اي برمجيات ضارة.

## إيقاف سلسلة الهجوم (Cyber kill-chain)

المخترقين دائما يتبعون سلسلة من المراحل للوصول للهدف وعليك تحديد ماهي المرحلة الحالية التي تم رصد الحادثة فيها والبدء في إيقافها وكذلك معرفة كيف تمت المراحل السابقة لعمل الية دفاعية مستقبلا.

### خطوات السلسلة:

١. عمليات الفحص (reconnaissance):  
عمليات الفحص النشطة او الغير نشطة والتي تهدف لجمع أكبر قدر من المعلومات عن المنظمة المستهدف.
٢. اعداد وتجهيز البرمجيات الضارة (Weaponization):  
تجهيز الأدوات والثغرات المناسبة للاستهداف.
٣. إيصال البرمجيات الضارة (Delivery):  
تحديد طريقة توصيل البرمجيات الضارة عبر أحد الطرق التالية:
  - البريد الالكتروني
  - الانظمة المتصلة بالانترنت
  - ذواكر التخزين المتنقلة USB
٤. الاستغلال (Exploitation):  
استغلال ثغرة في نظام التشغيل او الخدمات وغيرها لتشغيل برمجيات التنصت والاختراق وخلافها.
٥. التثبيت (Installation):  
تثبيت برمجيات ضارة بالنظام.
٦. التحكم والسيطرة (COMMAND & CONTROL):  
فتح قناة للتحكم والسيطرة بالنظام عن بعد.
٧. الهدف (Objectives):  
بعد الوصول الكامل يسعى المخترق الآن لتحقيق الهدف من الاختراق اما تشفير الملفات او تدمير البنية التحتية او سرقة المعلومات.

## تصنيف الثغرات الأمنية

بشكل يومي تكتشف ثغرات أمنية على برمجيات، أنظمة التشغيل او تطبيقات الويب ومن الممكن الحصول عليها من جهات خارجية متخصصة او مسؤولة (NCA-NCSC, Threat Intelligence, Vendors)، او من أحد المهتمين في الأمن السيبراني يقدم تقرير بوجود ثغرة قام باكتشافها. حيث ان هناك دراسات تمت عام ٢٠٢٠ ان عملية ظهور الثغرة وتوافر التحديث تقدر تقريبا ٩ أيام، وتشير تقارير عالمية مثل تقرير (لشركة FireEye) ان الوقت ما بين اصدار التحديث واستغلال الثغرة من قبل المهاجمين تصل أحيانا الى ساعتين فقط من ظهور التحديث.

يعتمد التعامل مع الحادثة الناشئة من الثغرات بناء على مدى خطورتها وحساسية النظام المكتشف فيه الثغرة وهنا يتم التصنيف على أربع فئات (حرج، عالي، متوسطة، منخفضة).

**أ. حرج:**

في حال وجود الخدمة خارجيا يتم فورا حجب الوصول لها من الخارج حتى يتم تحديث النظام او حل المشكلة. (في حال عدم القدرة على حجب الخدمة يتم فورا العمل على تخفيف الخطر من تقنين صلاحيات الوصول او حجب الأوامر المستخدمة في الثغرة او حتى حجب بعض المنافذ المستغلة.)  
في حال وجود الخدمة داخليا يتم العمل على تحديثها فورا على الا تزيد الفترة المتفق عليها داخل المنظمة.

**ب. عالي:**

في حال وجود الخدمة داخليا/خارجية يتم العمل على تحديثها فورا على الا تزيد الفترة المتفق عليها داخل المنظمة.

**ت. متوسط:**

في حال وجود الخدمة داخليا/خارجية يتم العمل على تحديثها فورا على الا تزيد الفترة المتفق عليها داخل المنظمة.

**ث. منخفض:**

في حال وجود الخدمة داخليا/خارجية يتم العمل على تحديثها فورا على الا تزيد الفترة المتفق عليها داخل المنظمة.

## خطوات تخفيف المخاطر (Mitigation)

يوجد خدمات حساسة لا يمكن إيقافها فوراً بسبب احتياج الاعمال لذا نلجأ الى تخفيف الخطر وطرد المهاجم.  
الخطوات:

- عمل تحديث لأغلاق ثغرات النظام في حال وجود ثغرة قائمة.
- حجب العنوانين المشبوهة التي تم اكتشافها من خلال التحليل ويفضل عمل تقييد الوصول للخدمات والأنظمة على حسب الموقع الجغرافي.
- تغيير جميع كلمات المرور المرتبطة بالخدمة المصابة.
- مراقبة الخدمة او النظام من خلال مركز السجلات المركزي SEIM.

## تحديد أولويات الاستجابة للحوادث

الوقت هو العنصر المهم للاستجابة للحوادث لذا كلما قلت الفترة الزمنية بين بداية الهجمة واكتشافها سوف تقل اضرار المترتبة من الهجمة. قد يواجه فريق الاستجابة العديد من التنبيهات الأمنية في آن واحد، وليس لديهم الوقت الكافي للاستجابة لجميعها، لذا عليك في هذي الحالة تحديد ماهي التنبيهات الأمنية ذات أولوية قصوى حالياً وترتيبها من الأهم حتى الأقل أهمية.

تحديد الأولوية يتم بناء على العوامل التالية:

- مكان الجهاز المصاب في الشبكة (DataBase Zone, Users Zone, Webserver zone, etc).
- قيمة البيانات المحفوظة في الجهاز المصاب. (مثلاً: بيانات محفوظة بجهاز موظف عادي لا تقارن في بيانات موظف آخر يعمل في مختبر للأبحاث السرية).
- نوع وعدد الحوادث التي حدثت على نفس الجهاز.
- موثوقية مؤشرات الأختراق المرتبطة بالحادثة.
- نشاط الشركة وماهي الحوادث التي تسبب لها ضرر بالغ في حال وقوعها (مثال: شركة ابحاث وتطوير تعتبر من أكبر مخاوفها هي فايروسات الفدية وتسريب البيانات لذا تعتبرها ذات اولوية في حال وقوعها).

## أبرز الأدوات والمواقع المقترحة للتحليل والأكتشاف

### ادوات لجمع مؤشرات الاختراق (IOC)

يوجد العديد من الادوات التي تساعد في جمع مؤشرات الأختراق التي من خلالها يتم اكتشاف أنشطة المهاجم وهنا سوف يتم ذكر بعضاً منها.

- Sysinternals utilities
- AVZ
- YARA

## أ. Sysinternals utilities

مجموعة من الأدوات لغرض المراقبة والادارة للأنظمة التي تعمل على نظام ويندوز ويوجد أكثر من ٦٠ أداة فيها، كما تتيح الأدوات لمحلي أمن المعلومات على جمع مؤشرات الاختراق وتحليل الأنظمة المصابة.



يمكنك تحميلها من هنا <https://technet.microsoft.com/en-us/sysinternals/default.aspx>

## ب. AVZ

أداة تساعد في التحليل والاستعادة.

File	Startup method	Description	Type
C:\PROGRAM~1\MICROS~3\Office15\MLCFG32.CPL	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\Windows\CurrentVex64	
C:\PROGRA~2\MICROS~2\Office15\GROOVEEX.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\PROGRA~2\MICROS~2\Office15\GROOVEEX.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\PROGRA~2\MICROS~2\Office15\GROOVEEX.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\PROGRA~2\MICROS~2\Office15\GROOVEEX.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE15\ymosshext.dll	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE15\OLKFSTUB.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Wind	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\Program Files (x86)\Microsoft Office\Office15\NAMEEXT.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\Program Files (x86)\Microsoft Office\Office15\OLKFSTUB.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\Program Files\7-Zip\7-zip32.dll	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\Program Files\Microsoft Office\Office15\ync.exe	Registry key	HKEY_CURRENT_USER, Software\Microsoft\Windows\CurrentVersion\32	
C:\Program Files\Realtek\Audio\HDA\RD64.exe	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\64	
C:\Program Files\Windows Sidebar\SideBar.exe	Registry key	HKEY_USERS, S-1-5-19\Software\Microsoft\Windows\CurrentVersion\32	
C:\Program Files\Windows Sidebar\SideBar.exe	Registry key	HKEY_USERS, S-1-5-20\Software\Microsoft\Windows\CurrentVersion\32	
C:\Windows\CCM\SMSCFGRC.cpl	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\Windows\CurrentVex64	
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\aspnet_isapi.dll	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\2.0.50727\64	
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\4.0.30319\64	
C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\2.0.50727\32	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\4.0.30319\32	
C:\Windows\SysWOW64\3codeca.acm	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\NT\CurrentVex32	
C:\Windows\SysWOW64\webcheck.dll	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	
C:\Windows\SysWOW64\webcheck.dll	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\32	

يمكنك تحميلها من هنا <http://www.z-oleg.com/secur/avz/download.php>

## ت. YARA

أداة صممت لمساعدة محللي البرمجيات ضارة لتحديد وتصنيف الفايروسات الضارة. تعمل على أكثر من بيئة تشغيل مثل ويندوز، لينكس ونظام ماك OS X وتستخدم من خلال سطر الأوامر أو سكربت بايثون.

الصورة أدناه تمثل YARA Rule والتي تذكر بأن في حال تطابق شرط واحد من الشروط الثلاثة في أي ملف يجب أن يتم اعتبار الملف بأنه مصدر تهديد.

```
rule silent_banker : banker
{
  meta:
    description = "This is just an example"
    thread_level = 3
    in_the_wild = true
    strings:
      $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
      $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
      $c = "UVODFRYSIHLNWPBJXQZAKCBGMT"
    condition:
      $a or $b or $c
}
```

يمكنك تحميلها من هنا <http://virustotal.github.io/yara>

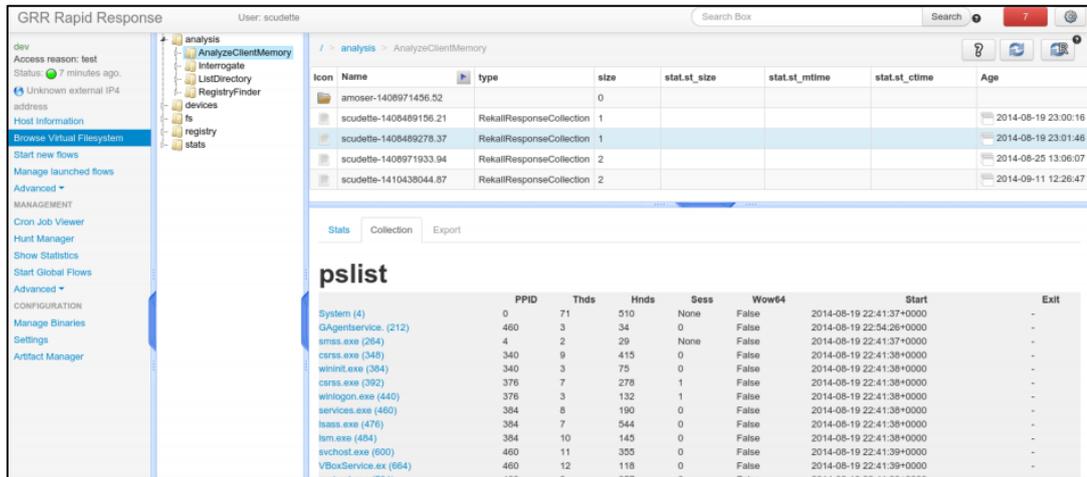
## ادوات لعمل نسخة من النظام والذاكرة

في هذا القسم سوف نشرح عدد من الأدوات واستخداماتها لإنشاء نسخ احتياطية من الانظمة المصابة والذاكرة العشوائية.

- GRR Rapid Response
- Forensic Toolkit
- DumpIt
- Kape

## أ. GRR Rapid Response

أداة استجابة للحوادث الأمنية تساعد المحلل على عمل نسخة من الأنظمة المصابة عن بعد وكذلك تحليل البيانات المستخرجة من النسخ.



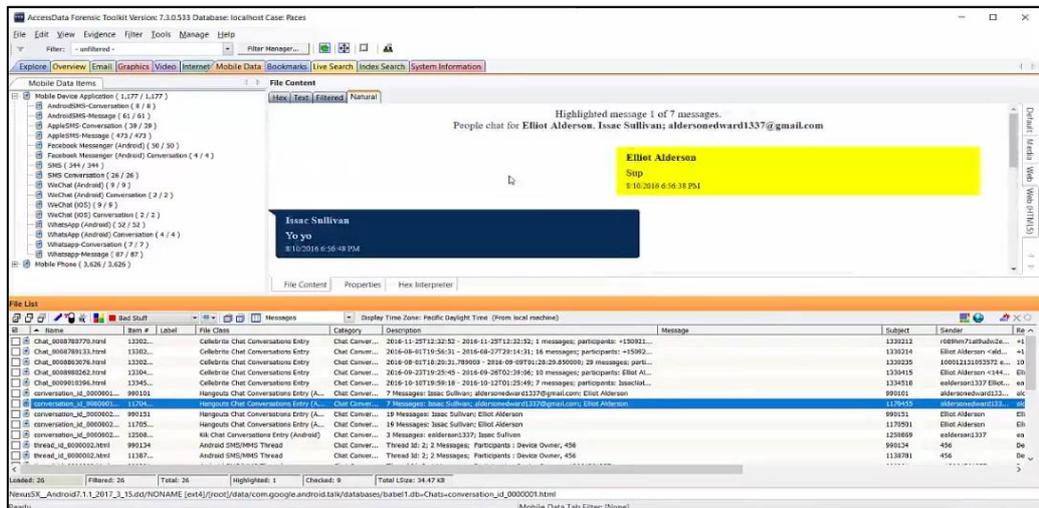
### أبرز المميزات في الأداة:

- تحليل الذاكرة وسجلات الويندوز عن بعد.
- تحليل القرص الصلب عن بعد.

يمكنك تحميلها من هنا <https://github.com/google/grr>

## ب. Forensic Toolkit

أداة متعددة الاستخدام خاصة بالتحقيق الرقمي "Digital Forensics" وتحتوي على مجموعة من الأدوات ومنها أداة FTK-Imager التي يمكنك من اخذ نسخة من القرص الصلب والذاكرة العشوائية.

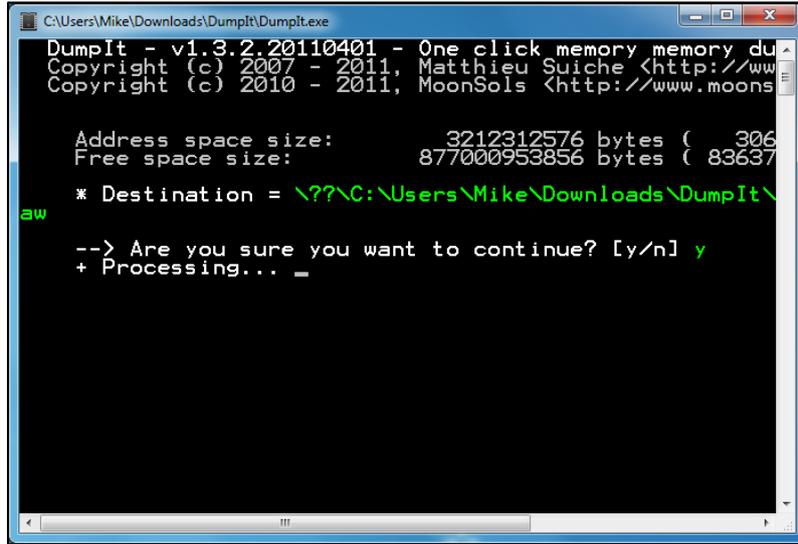


يمكنك تحميلها من هنا

<http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk?/solutions/digital-forensics/ftk>

## ث. DumpIt

أداة تحقيق رقمي وتستخدم بشكل واسع على أخذ نسخة من الذاكرة العشوائية وذلك يرجع لسهولة استخدامها.

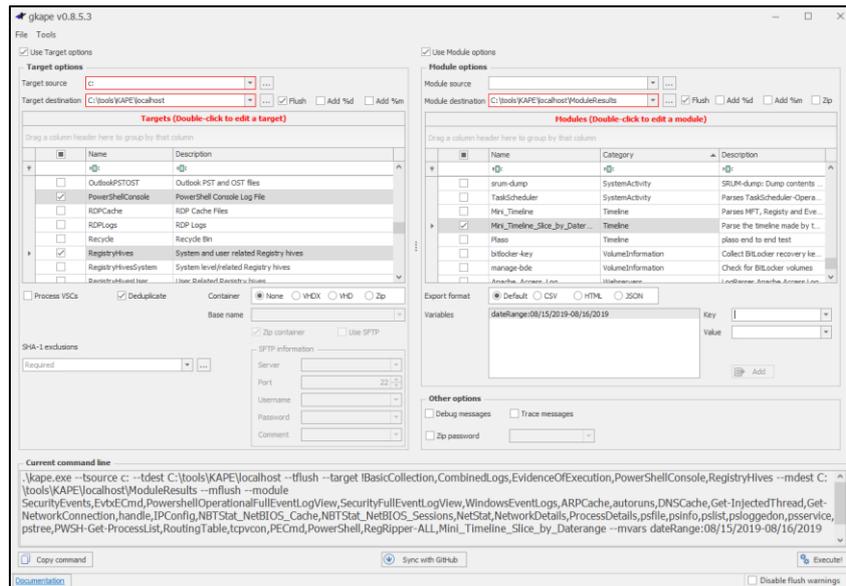


يمكنك تحميلها من هنا

<https://github.com/thimbleweed/All-In-USB/tree/master/utilities/DumpIt>

## ث. Kape

أداة تحقيق رقمي تعمل في أخذ أدلة "Artifacts" محددة ذات قيمة عالية للمحلل من الأجهزة المصابة وتحليلها وتمتاز بالسرعة والكفاءة، وتختلف الاداة عن الأدوات الأخرى بأنها لا تأخذ نسخة كاملة من النظام بل تستخرج الأدلة التي يحتاجها المحلل في التحليل.



يمكنك تحميلها من هنا

<https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape>

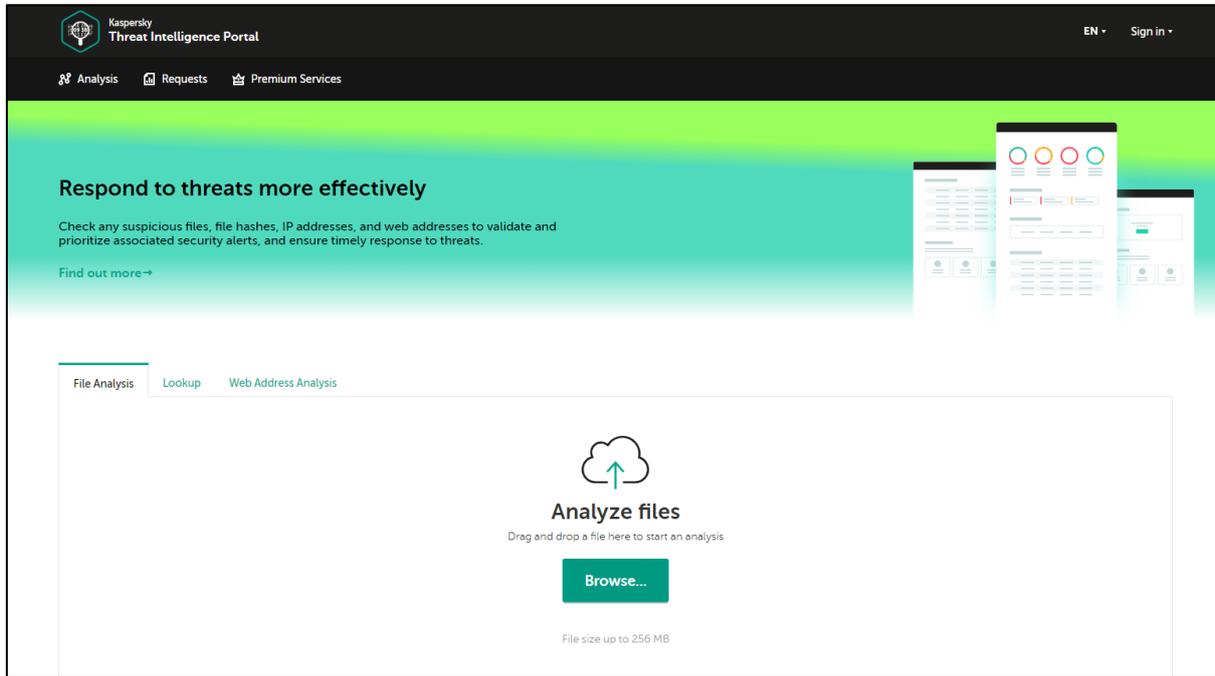
## ادوات ومواقع لتحليل التهديدات المحتملة والبرامج الخبيثة

- Kaspersky Threat Intelligence Portal
- VirusTotal
- Anyrun
- HyberAnalsis
- Cuckco

### أ. Kaspersky Threat Intelligence Portal

منصة تجمع العديد من الادوات التي تساعد في التحليل ومنها:

- Threat Lookup
- Whois Tracking
- APT Reports
- Sandbox



### أ. Threat Lookup

تحتوي على جميع المعلومات التي تمت من خلال فريق Kaspersky Lab عن التهديدات السيبرانية مما تساعد مختصي أمن المعلومات من منع الهجمات قبل حدوثها.

### ب. Whois Tracking

تظهر لك العناوين والنطاقات وبعض المعلومات عن مصدر التهديد مثل (تاريخ أنشاء النطاق ، الجهة المستضيفة للنطاق او العنوان).

## ت. APT Reports

تساعد تقارير كاسبرسكي في التوعية وزيادة المعرفة لدى المختصين عن الهجمات المتقدمة التي تحدث في الفضاء السيبراني.

## ث. Sandbox

نظام تشغيل مخصص لتحليل الروابط والملفات لأكتشاف التهديدات، ويمكن إستخدامه لتحليل الملفات المشبوهة.

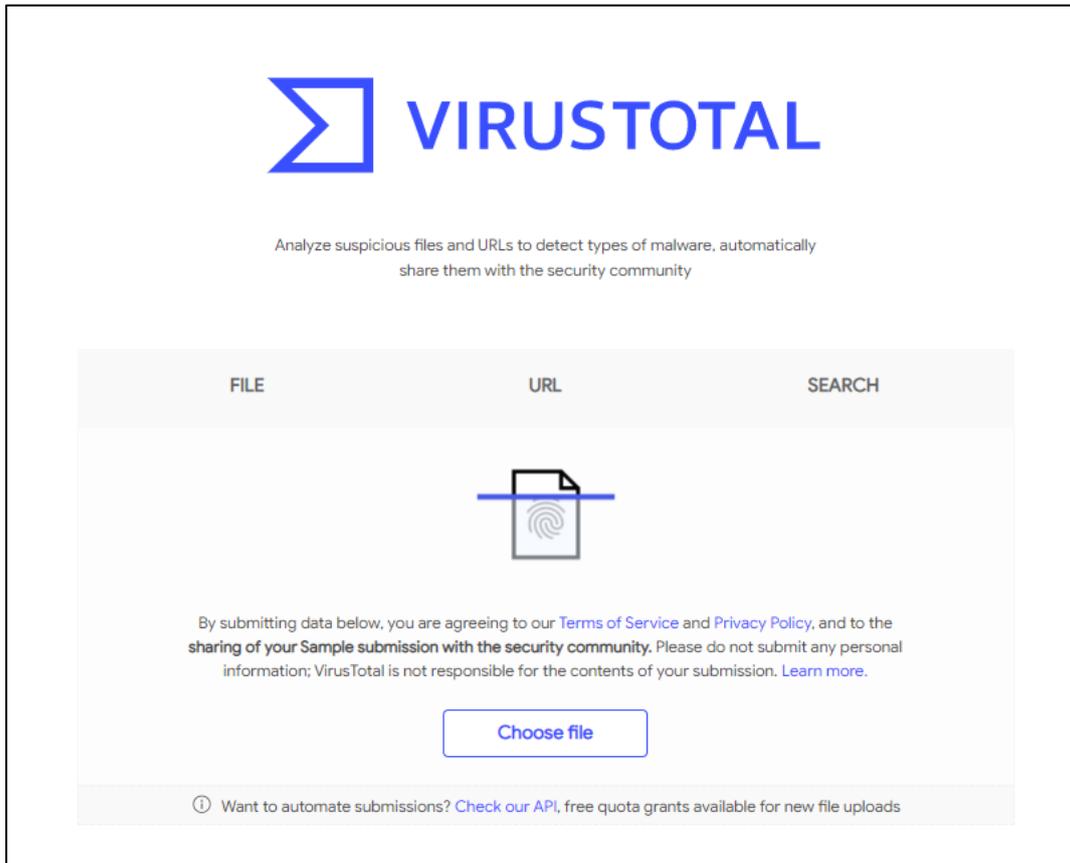
الموقع:

<https://opentip.kaspersky.com>

**تنويه:** عدم تحميل أي ملفات حساسة لدى الجهة الخاصة بك في المواقع التي تتيح خدمة الفحص أون لاین.

## ب. VirusTotal

منصة متخصصة لتحليل الروابط والملفات لأكتشاف التهديدات.



The screenshot displays the VirusTotal website's main interface. At the top, the VirusTotal logo is prominently featured. Below the logo, a tagline reads: "Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community". The interface is divided into three main sections: "FILE", "URL", and "SEARCH". The "FILE" section is currently active, showing a large icon of a document with a fingerprint, indicating the file upload process. Below this icon, there is a disclaimer: "By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more." A "Choose file" button is positioned below the disclaimer. At the bottom of the interface, there is a link: "Want to automate submissions? Check our API, free quota grants available for new file uploads".

الموقع:

<https://www.virustotal.com/gui>

**تنويه:** عدم تحميل أي ملفات حساسة لدى الجهة الخاصة بك في المواقع التي تتيح خدمة الفحص أون لاين.

### ت. Anyrun

منصة تفاعلية مخصصة لاستعراض وتحليل الروابط والملفات لأكتشاف التهديدات.



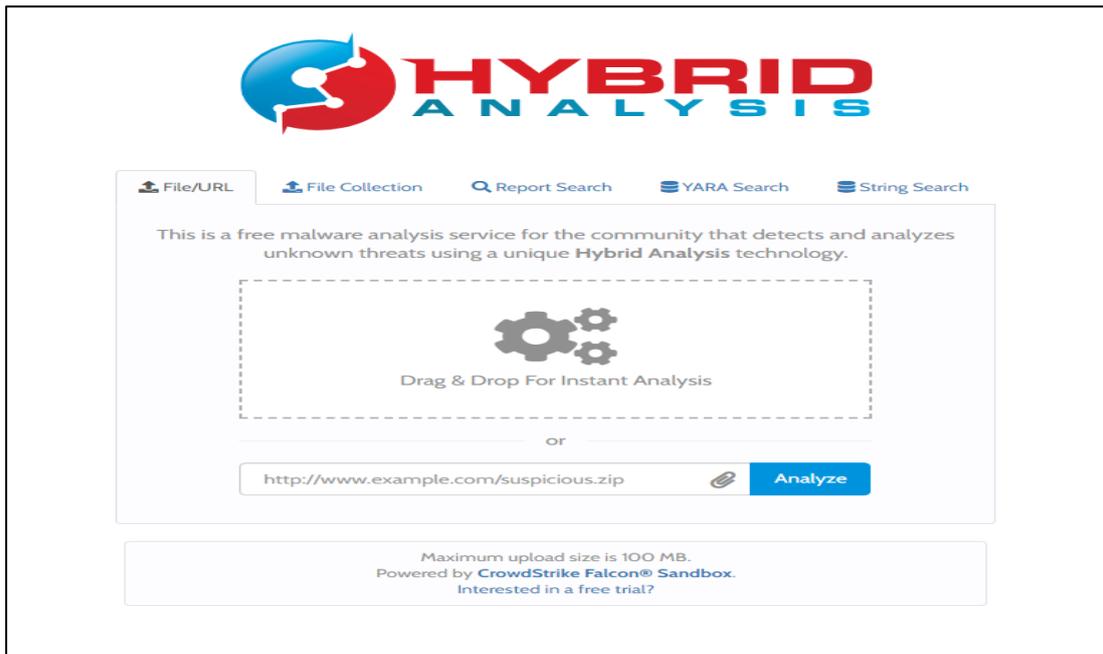
الموقع:

<https://app.any.run>

**تنويه:** عدم تحميل أي ملفات حساسة لدى الجهة الخاصة بك في المواقع التي تتيح خدمة الفحص أون لاين.

### ث. HyberAnalysis

منصة مخصصة لتحليل الروابط والملفات لأكتشاف التهديدات.



الموقع:

<https://www.hybrid-analysis.com>

**تنويه:** عدم تحميل أي ملفات حساسة لدى الجهة الخاصة بك في المواقع التي تتيح خدمة الفحص أون لاين.

## ج. Cuckoo

نظام تشغيل مخصص لتحليل الملفات والروابط المشبوهة حيث يمكن تثبيتها بجهاز غير متصل بشبكة المنظمة وذلك لعمل التحليلات اللازمة من دون أن يتم الاطلاع عليها من جهة خارجية.

الموقع الرسمي:

<https://cuckoosandbox.org>

شرح طريقة التثبيت:

<https://www.binary-zone.com/2020/03/18/howto-setup-and-use-the-cuckoovm-v2>

## ادوات لتحليل الذاكرة العشوائية

- Volatility
- Rekall

### أ. Volatility

اداة تحقيق رقمي تستخدم لأستخراج الادلة من النسخة التي تم الاستحواذ عليها من الحادثة للذاكرة العشوائية.

```
$ python vol.py -f stuxnet.vmem --profile=WinXPSP2x86 dlldump -memory -D stuxout/
Volatility Foundation Volatility Framework 2.5
Process (V) Name      Module Base Module Name  Result
-----
0x820df020 smss.exe    0x048580000 smss.exe    OK: module.376.22df020.48580000.dll
0x821a2da0 csrss.exe   0x075b40000 CSRSRV.dll  OK: module.600.23a2da0.75b40000.dll
0x821a2da0 csrss.exe   0x077f10000 GDI32.dll  Error: DllBase is paged
0x821a2da0 csrss.exe   0x075b60000 winsrv.dll  OK: module.600.23a2da0.75b60000.dll
0x81da5650 winlogon.exe 0x001000000 winlogon.exe OK: module.624.1fa5650.1000000.dll
```

يمكنك تحميلها من هنا <http://www.volatilityfoundation.org>

## ب. Rekal

أداة تحقيق رقمي تستخدم لاستخراج الأدلة من نسخة الذاكرة العشوائية التي تم الاستحواذ عليها من الحادثة. كما تتيح الأداة عمل تحليل للذاكرة العشوائية مباشرة من دون أخذ نسخة لها.

```
user@computer:~/rekall$ rekall -f ~/images/win7.elf
-----

The Rekal
Memory Forensic framework 1.1.0 beta (Bucheneegg).

"We can remember it for you wholesale!"

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License.

See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get started.
-----

win7.elf 12 47 07> pslist
-----> pslist()

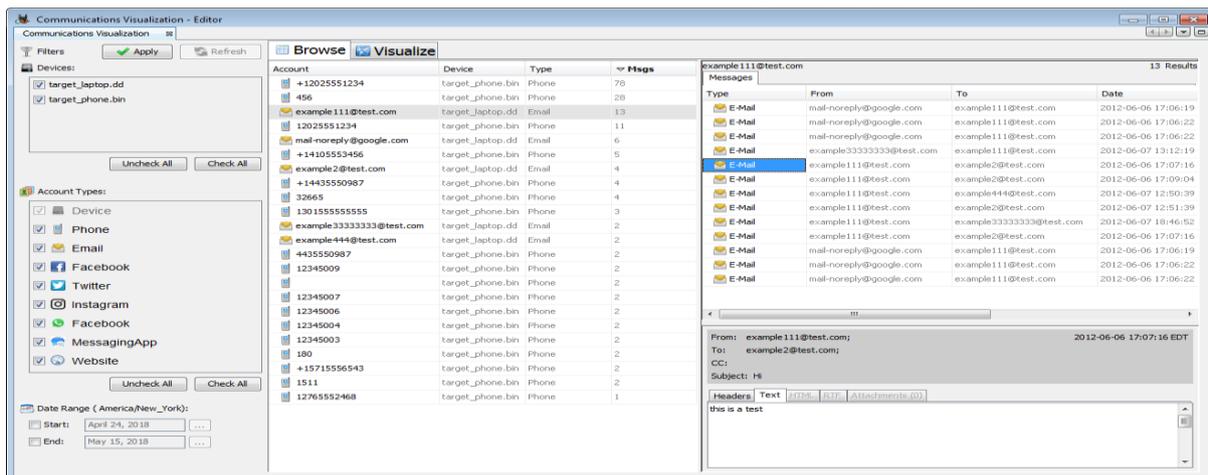
  _EPROCESS   Name      PIO PPID Thds Hnds Sess Wow64 Start
-----
0xfa80008959e0 System 4      0  84  511 -   False 2012-10-01 21:39:51+0000
```

يمكنك تحميلها من هنا <http://www.rekall-forensic.com>

## أدوات لتحليل القرص الصلب

### The Sleuth Kit(TSK) •

مجموعة من سطر الأوامر التي تسمح لك بتحليل القرص الصلب واستعادة الملفات ، ويوجد لها واجهة رسومية وهي أداة Autopsy حيث أنها تعتبر الواجهة رسومية لأداة TSK.



يمكنك تحميل اداة The Sleuth Kit من هنا <http://www.sleuthkit.org/sleuthkit>

يمكنك تحميل اداة Autopsy من هنا <http://www.sleuthkit.org/autopsy/>

## ادوات للبحث عن النصوص (Strings)

### Strings Utility •

اداة تستخدم من خلال سطر اوامر وتوجد في أنظمة تشغيل لينيكس ويونكس والتي بدورها تساعد بالبحث داخل الملفات عن رموز Unicode أو ASCII. كما يمكن البحث عن النصوص من النسخة المستخرجة من الانظمة المصابة مثل البحث عن (الروابط، العناوين، البريد الالكتروني، سجلات الويندوز الخ)

```
fabio@fabio-5400CA:~$ strings file.exe
!This program cannot be run in DOS mode.
Rich
.text
.rdata
.data
.rsrc
SSShL@X
E]u@8
QRP;6
7@JB
A/K?/?
/K7A?7/
JBCA
B@?/A
```

يمكنك تحميلها لنظام الويندوز من هنا

<https://docs.microsoft.com/en-us/sysinternals/downloads/strings>

## تقارير معلومات استباقية (Threat Intelligence Reports)

هناك جهات موثوقة تعمل على جمع ورصد المعلومات للأنشطة المشبوهة في الفضاء السيبراني وتعمل تقارير على السلوك ومؤشرات الاختراق المكتشفة في الهجمة.

### أمثلة على بعض المصادر لتقارير المعلومات الاستباقية

- FireEye
- Verizon
- TrustWave
- Palo Alto Networks
- F-Secure

المصطلح	المعنى
IOC (Indicator Of Compromise)	مؤشرات الاختراق
EndPoints	أجهزة المستخدمين
Wipe	مسح البيانات والكتابة فوقها عدة مرات
Miner	برمجيات التعدين
EDR (Endpoint Detection and Response)	برمجيات الاستجابة للحوادث
SEIM	مركز سجلات المركزية
IR (Incident Response)	الاستجابة للحادثة
Data Loss Prevention (DLP)	اداة منع تسرب البيانات
Artifacts	الادلة الرقمية

- <https://github.com/certsocietegenerale/IRM/tree/master/EN>
- [https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07171449/Incident\\_Response\\_Guide\\_eng.pdf](https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07171449/Incident_Response_Guide_eng.pdf)
- <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- <https://nca.gov.sa/images/glossary.jpg>
- <https://www.fireeye.com/blog/threat-research/2020/04/time-between-disclosure-patch-release-and-vulnerability-exploitation.html#:~:text=12%20percent%20of%20vulnerabilities%20were,week%20following%20the%20patch%20release.&text=15%20percent%20of%20vulnerabilities%20were,one.%20month%20of%20patch%20release>