الفصل 10:
تحليل حمولات البريد الإلكتروني

يركز الفصل التاسع على تحليل البريد الإلكتروني بحد ذاته، ولكن سيعلمك هذا الفصل بعض أساسيات تحليل المرفقات والروابط الضارة والتي تسمى أيضًا "الحمولات" في رسائل البريد الإلكتروني. يغطي الجزء الأول بيئة الاختبار المعزولة وهي طريقة مريحة لتحليل الملفات والروابط التي يحتمل أن تكون ضارة، والجزء الثاني هو مقدمة لتحليل الملفات يدويًا ولكن وكما سيوضحه الفصل هذا أمر سترغب في تجنبه إذا استطعت.

نظرًا لأن هذا الفصل يتناول البرمجيات الضارة، تأكد من أنك قد راجعت الفصل 4 بدقة.

بيئة الاختبار المعزولة

بيئة الاختبار المعزولة هي برنامج يوفر بيئة آمنة لتشغيل برنامج كمبيوتر، وأحد أنواع بيئة الاختبار المعزولة هو **وضع بيئة اختبار للبرمجيات الضارة** حيث يمكن تنفيذ البرمجيات الضارة بطريقة مضبوطة ويمكن تحليل إجراءاتها.

تتيح لك بيئة الاختبار المعزولة التي يوصي به هذا الفصل تحميل ملف لتشغيله أو الاتصال بعنوان موقع ويب لتحميله في المتصفح، وبعد فترة قصيرة ستوفر لك بيئة الاختبار معزولة تقريرًا عن الأنشطة على الجهاز وغالبًا ما يسلط الضوء على الأنشطة إن وجدت التي تشير إلى السلوك الخبيث.

نظرًا لأن البرمجيات الضارة غالبًا ما تستخدم مراحل متعددة، ونتيجة للطمس والتقنيات أخرى المضادة للتحليل غالبًا ما يكون استخدام بيئة اختبار معزولة تعمل بطريقة صحيحة أسرع بكثير من إجراء تحليل يدوي، ويسهل الوصول أيضًا على فهم أساسي لكيفية عمل البرمجيات الضارة.

يمكنك من الناحية النظرية إعداد بيئة الاختبار المعزولة الخاصة بك باستخدام الأجهزة الافتراضية حيث يمكنك إنشاء جهاز افتراضي وعادةً ما يعمل عليه نسخة حديثة من ويندوز والتقاط لقطة ثم تشغيل البرمجيات الضارة على هذا الجهاز الافتراضي وبعد مرور بعض الوقت تنظر إلى ما حدث ثم تعود إلى اللقطة.

لكن هناك العديد من الجوانب السلبية لهذا النهج:

- في حين أن الجهاز الظاهري سيساعدك على تجنب أي ضرر ناتج عن التغييرات التي تطرأ على نظام التشغيل إلا أنك لا تزال تشغله على شبكتك الخاصة، وقد تجد البرمجيات الضارة طرقًا للانتشار من جهاز إلى آخر. قد تتصل أيضًا بالإنترنت وفي حال اكتشاف هذه الاتصالات قد ينتهي عنوان بروتوكول إنترنت الخاص بك في قائمة الحظر، حيث لن تسمح لك بعض الخدمات بالوصول إليها من عنوان بروتوكول إنترنت مدرج في قائمة الحظر.
- سيتعين عليك التحقق يدويًا من جميع التغييرات التي تم إجراؤها على الجهاز الظاهري وتحديد ما إذا كانت تشير إلى سلوك ضار، وسيتعين عليك أيضًا التقاط حركة مرور الشبكة بطريقة ما ومعرفة الاتصالات التي يتم إجراؤها.
- غالبًا ما تبحث تقنيات مكافحة التحليل عن بيئات افتراضية وفي هذه الحالة لن تعمل البرمجيات الضارة إذا اكتشفت وجودها، وبعض الأمثلة على البرمجيات الضارة التي قد تبحث عنها في جهاز افتراضي هي وحدات المعالجة المركزية النموذجية في الأجهزة الافتراضية أو صورة خلفية تكون صورة ويندوز الافتراضية أو محرك أقراص ثابت صغير بشكل غير معقول أو عدد قليل جدًا من الملفات الموجودة على محرك الأقراص الثابتة بخلاف تلك الموجودة بعد التثبيت.
- تقوم بعض البرمجيات الضارة بالاتصال بخادم التحكم الخاص بها الذي يتحقق مما إذا كان قد تم تشغيلها بالفعل من عنوان بروتوكول إنترنت المحدد هذا، وإذا حدث ذلك فلن يتم تشغيلها مرة أخرى.

يمكن معالجة بعض هذه القضايا بسهولة نسبيًا، ولكن بعضها الآخر أكثر تعقيدًا والقائمة أعلاه ليست شاملة بالتأكيد.

لحسن الحظ توجد بيئة اختبار معزولة تم إعدادها بالفعل للتخفيف من هذه التحديات، وأكثرها شعبية هي كوكو (Cuckoo) مفتوحة المصدر. إذا كنت ترغب في تجربة تشغيل بيئة اختبار معزولة من المناسب البدء باستخدام كوكو، وتمت كتابته في الأصل من قبل أشخاص لديهم اتصالات بمجتمع حرية الإنترنت ولذلك تم تصميمه مع مراعاة احتياجات المجتمع المدني.

لكن من الجيد معرفة أن كوكو الأصلي الذي صدر آخر إصداراته في عام 2018 ليس قيد التطوير النشط[47] وبالتالي من غير المرجح أن يكون قادرًا على التعامل مع التهديدات الحالية بشكل صحيح، وتقوم مجموعة من الأشخاص في سيرت إي إي (CERT-EE) (سيرت الوطني الإستوني) بإعادة كتابة كوكو ليعمل على بايثون 3 (Python 3)، ويمكنك متابعة تقدمهم على غيت هب (GitHub)، وإذا كنت ترغب بذلك قم بتثبيت هذا الإصدار من كوكو، ولكن توقع أن تضطر إلى القيام بالكثير من العمل لاستكشاف الأخطاء وإصلاحها كي يعمل.

الخيار الأسهل بكثير هو استخدام بيئات الاختبار المعزولة المستندة إلى السحابة، ويتوفر عدد منها مثل أني دوت رن (ANY.RUN) وهايبرد أناليسس (Hybrid Analysis) وجو ساندبوكس (Joe Sandbox) وترياج (Triage) وحتى نسخة عبر الإنترنت من كوكو. تحتوي جميعها على إصدارات مجانية تسمح لك بتحميل البرمجيات الضارة وعناوين موقع الويب على الرغم من أن بعضها سيتطلب التسجيل،[48] ولكن ينبغي التحذير فكما هو الحال مع فايروس توتال، إن استخدام أحد بيئات الاختبار المعزولة هذه يجعل التحليل متاحًا للجمهور العام بشكل أساسي. إذا بدا من المحتمل أن البرمجية الضارة تستهدفك خصيصًا، ستؤدي الإشارة علنًا إلى أنك تقوم بتحليله بالسماح للمهاجم بمعرفة أنك تحقق فيه.

لكل بيئة اختبار معزولة خصائص فريدة لكنها تشترك أيضًا في العديد من الميزات، وفيما يلي وصف لأداة ترياج ولكن نشجعك على تجربة بيئة اختبار معزولة أخرى أيضًا إذا كانت هناك واحدة تعجبك بشكل خاص يمكنك التعرف على كيفية عملها.

لقطات الشاشة التالية مأخوذة من مستند ضار تم العثور عليه (sha256:
8404d3dc32b0555bc3b076d7fc080d2a341508b4a2c84805a1d5ffc0057e2b39) على مالوير بازار حيث يمكنك تنزيله مجانًا إذا أردت، وتوجد بيئة اختبار معزولة متاحة في الإصدار العام من ترياج.

في ترياج استخدم "إرسال (Submit)" في الزاوية العلوية اليسرى من الصفحة لتحميل ملف، وهذه مفيدة للغاية لأنها تسمح لك بتحميل ملفات محمية بكلمة مرور (كلمة المرور الافتراضية التي يجربها هي "infected" وتذكر أن هذا هو المعيار الذي يستخدم)، لذلك لا داعي للقلق بشأن الاحتفاظ بملف يحتمل أن يكون ضارًا على جهاز الكمبيوتر الخاص بك قبل إرساله.

يمكنك أيضًا إرسال عناوين عنوان موقع الويب إما لتنزيل البرمجيات الضارة مباشرة من عنوان موقع الويب ثم تحليلها أو لتحليل عنوان موقع الويب في المتصفح.

[47] إحدى المشكلات هي أن كوكو كُتب في الأصل للنسخة 2 من لغة بايثون وهي نسخة مهجورة من اللغة.

[48] في وقت كتابة هذا التقرير يمكن استخدام هايبرد أناليسس وكوكو دون تسجيل ويتطلب أني دوت رن وترياج تسجيلًا مجانيًا ويتطلب جو ساندبوكس التسجيل والموافقة على الحساب.

يمكنك في الصفحة التالية اختيار إعدادات مختلفة لبيئة الاختبار المعزولة، والأهم من ذلك هو نظام التشغيل. وكما سترى يمكنك الاختيار من بين إصدارات مختلفة من ويندوز أو ماك أو إس أو آندرويد أو لينوكس. إذا لم تختر أي شيء هنا فيمكنك أن تطلب من ترياج اختيار نظام تشغيل واحد أو أكثر لك وهذا عادة ما سينجح.

يمكنك أيضًا اختيار إعدادات لغة الجهاز، علمًا أن الإعداد الافتراضي هو en-us: إنجليزية الولايات المتحدة الأمريكية. علمًا أن البرمجيات الضارة التي تستهدف منطقة معينة أو مجموعة من الأشخاص لا تعمل أحيانًا إلا على أجهزة بلغة معينة. يمكنك اختيار ما إذا كنت تريد الاحتفاظ بالوصول إلى الإنترنت (الافتراضي) أو إيقافه أو الاتصال عبر تور (Tor)، حيث تقوم الكثير من البرمجيات الضارة بالاتصال بخادم يتحكم فيه المتطفل، وإذا كان هذا مصدر قلق محتمل بالنسبة لك مثل عدم رغبتك في إبلاغ المتطفل بأنك تقوم بعملية التحليل، يمكنك محاولة تشغيل بيئة اختبار معزولة مع تعطيل اتصال الإنترنت أو تعيينه بحيث تحاكي طلبات الويب التعليمات البرمجية للإرجاع من النوع إرجاع 200 أو 404. تقوم بعض البرمجيات الضارة بإجراء فحص سريع بحثًا عن بعض مواقع الويب لمعرفة ما إذا كان يتم تشغيلها في بيئة دون اتصال بالإنترنت وهذا من شأنه أن يزيف أنواع الاتصال هذه، ولكن قد لا تعمل بعض البرمجيات الضارة.

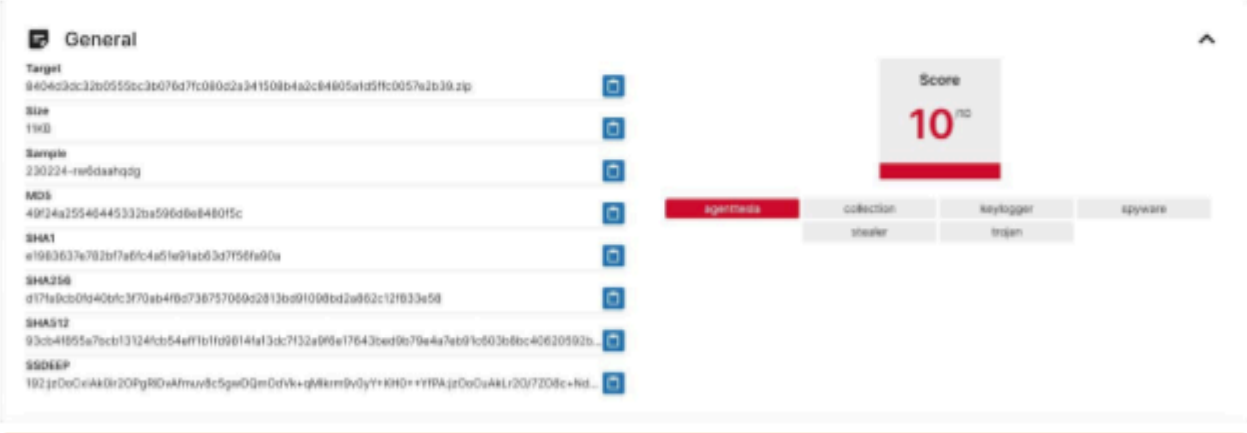
يمكنك أيضًا تعيين مهلة وسيتوقف التنفيذ بعد توقف النشاط لبعض الوقت (بعد دقيقتين ونصف افتراضيًا)، وتتمثل إحدى تقنيات مكافحة التحليل الشائعة في انتظار البرمجيات الضارة لبعض الوقت قبل إجراء أي نشاط ضار ولذلك في بعض الحالات قد ترغب في زيادة المهلة.

يمكنك أخيرًا تغيير المتصفح الذي يستخدم في بيئة الاختبار المعزولة لفتح مواقع الويب، وقد يكون هذا مفيدًا في بعض الأحيان في حالة تشغيل التهديد المحتمل الذي تقوم بتحليله فقط في متصفح معين.

يمكنك الآن البدء في تحليل الملف (أو عنوان موقع الويب) الذي يفتح في بيئة اختبار معزولة.

من الأشياء المميزة في ترياج هو أنه يمكنك رؤية ما يحدث على نظام التشغيل الافتراضي أو أنظمة التشغيل الافتراضية على بيئة الاختبار المعزولة حيث يمكنه تشغيل تحليلات متعددة بالتوازي ويمكنه أيضًا التفاعل مع نظام التشغيل هذا. في بعض الأحيان قد يكون هذا مفيدًا على سبيل المثال إذا كانت البرمجيات الضارة تراقب نظامك وتسجل مرات النقر على زر، ولكن في معظم الحالات يكفي تشغيل بيئة الاختبار المعزولة في الخلفية.

بعد اكتمال بيئة الاختبار المعزولة يمكنك عرض التحليل لأن هذا الأمر هو أكثر أمر يهمك.



صفحة "اللمحة العامة" هي المكان الذي سترغب على الأرجح في النظر إليه أولًا، حيث يمنحك ملخصًا لتحليل بيئة اختبار معزولة. في هذه الحالة نرى أن ترياج يعطي العينة درجة 10 من أصل 10 ووضع عليها وسم "agenttesla". يُعدّ إيجنت تيسلا (Agent Tesla) برمجية ضارة شائع تستخدم لسرقة معلومات مثل بيانات الاعتماد من جهاز مصاب، وستلاحظ أيضًا وسومًا مثل "stealer" (أداة سرقة) و"keylogger" (أداة تسجيل مفاتيح) و"spyware" (برمجية تجسس) توضح أكثر أنه سيئ.

في معظم الحالات يكفي ذلك لأنك تعلم أن الملف الذي أردت تحليله هو إيجنت تيسلا، وهناك ما يكفي من التحليلات لإيجنت تيسلا المتاحة على الإنترنت لتوفير فكرة عما يفعله. ونظرًا لأن إيجنت تيسلا شائع إلى حد ما سيعرف ترايا‌ج أيضًا كيفية استخراج معلومات التكوين من البرمجيات الضارة وسيعرضها في قسم "تكوين البرمجيات الضارة (Malware Config)".

السؤال 10.1. استنادًا إلى التكوين المستخرج من البرمجيات الضارة، كيف يستخرج متغير إيجنت تيسلا هذا المعلومات من جهاز مصاب؟ (انظر الملحق للعثور على الإجابة.)

يوضح لك قسم "الأهداف" مرة أخرى أن هذا هو إيجنت تيسلا ولكنه يعرض أيضًا أنشطته الخبيثة فعلى سبيل المثال تقوم عملية مدرجة في قائمة الحظر بإجراء طلب على شبكة ويتم تنزيل ملف "MZ/PE"[49]. تذكر أن الملف الذي تقوم بتحليله هو مستند أوفيس وهو مشبوه للغاية لأنه يحاول تنزيل الملفات!

يعرض هذا القسم أيضًا أمورًا أخرى تحاول البرمجيات الضارة القيام بها مثل الوصول إلى ملفات تكوين بروتوكول نقل الملفات والبيانات من عملاء البريد الإلكتروني ومتصفحات الويب، وهذا النشاط شائع للبرمجيات الضارة التي تسرق المعلومات. حتى لو كنت تحاول تحليل البرمجيات الضارة التي لم تتعرف عليها بيئة الاختبار المعزولة، فإن هذا النشاط مشبوه للغاية.

هناك أيضًا قسم متعلق بـ "مصفوفة ميتر أتاك (MITRE ATT&CK Matrix)"، حيث إن أتاك (ATT&CK) هي "إطار عمل" يستخدمه محللو التهديدات كلغة شائعة وأسهل للفهم لوصف وتوثيق التكتيكات والتقنيات التي يستخدمها المتطفلون. في هذه الحالة، تعرض لك علامة التبويب هذه التقنيات (مثل جمع رسائل البريد الإلكتروني أو تعديل السجل) التي تستخدمها هذا البرمجية الضارة. تم تصميم أتاك مع وضع الشركات في الاعتبار ويركز على التهديدات وليس على عينات البرمجيات الضارة الفردية ولكن لن يضر إلقاء نظرة على التقنيات المسجلة في هذا القسم.

يتيح لك قسم "مراقبة إعادة التشغيل (Replay Monitor)" تكرار ما فعلته البرمجيات الضارة بنظام التشغيل وهذا ميزة مفيدة حقًا لفهم ما حدث بصريًا، وأخيرًا إذا حاولت البرمجيات الضارة تنزيل أي ملفات جديدة من الإنترنت، فيمكنك عرضها في قسم "التنزيل" وربما تنزيلها بنفسك لإجراء تحليل إضافي، لكن احذر لأن تكون هذه الملفات ضارة وتعامل معها بعناية!

بغض النظر عن صفحة "لمحة عامة (Overview)"، ستحتاج أيضًا إلى إلقاء نظرة على علامات التبويب في بيئة اختبار معزولة المقابلة لسلوك الملف، وفي هذه الحالة تم تشغيل الملف على كل من ويندوز 7 و ويندوز 10.

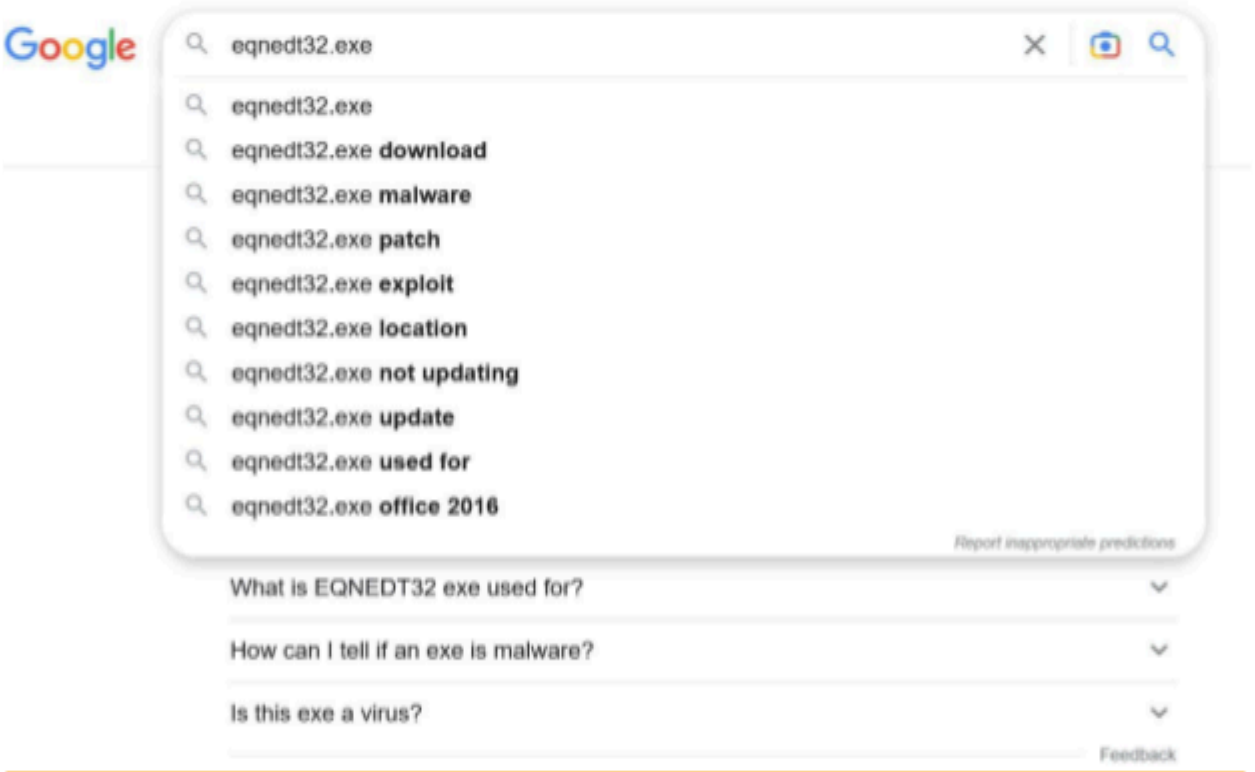
دعونا نلقي نظرة على ويندوز 7 أولًا. ستجد المعلومات الأكثر إثارة للاهتمام في علامة التبويب "التقرير (Report)"، وكان بعضها متاحًا أيضًا على صفحة "لمحة عامة" لكنك ستلاحظ بعض المعلومات الإضافية. على سبيل المثال، في قسم "التوقيعات" يذكر إن الملف يشغل محرر المعادلات (Equation Editor) وأن "محرر المعادلات هو مكون أوفيس قديم غالبًا ما تستهدفه الثغرات مثل CVE-2017-11882". ومن المثير للاهتمام أن هذه الثغرة تستغل بشكل شائع لاستهداف المجتمع المدني ڤريك ماشين.

في قسم "العمليات" يمكنك معرفة العمليات التي بدأتها البرمجيات الضارة بعد فتح الملف، ويمكنك أن ترى أربع عمليات بدأت: WINWORD.EXE وsplwow64.exe وEQNEDT32.EXE وarnolded4874.exe – وترى أن الأخيرة بدأت مرتين، وليس من المتوقع أن تعرف ما يعنيه كل هذا، ولكن يمكن أن تكون هذه العمليات مفيدة عند محاولة فهم ما يحدث.

سيخبرك محرك البحث أن WINWORD.EXE هو مايكروسوفت وورد وهو أمر منطقي لأن هذا ملف وورد، حيث سيعمل وورد عند فتح ملف البرمجيات الضارة. العملية الثانية splwow64exe هي أيضًا برنامج سليم ويتعلق بجعل برامج 32 بت تعمل على نظام تشغيل 64 بت.

[49] يعني PE "ملفًا قابل للتنفيذ متنقلًا"، في حين أن MZ يشير إلى أول بايتين من ملف PE، وتُعد كل من الملفات التنفيذية .exe على ويندوز ومكتبات dll. ويندوز أمثلة على هذه الملفات.

EQNEDT32.EXE هو سليم أيضًا، ولكن بالنظر إلى اقتراحات محرك البحث لهذا الملف، سترى "البرمجيات الضارة" و"الثغرة" مذكورة بشكل متكرر مما يشير إلى أنها تستخدم بشكل شائع لتنفيذ البرمجيات الضارة. وفي الواقع هذا هو محرر المعادلات المذكور سابقًا.



أخيرًا هناك عدد قليل جدًا من النتائج حول arnolded4874.exe في غوغل، وفي وقت كتابة هذا التقرير هناك نتيجة واحدة فقط وهي عينتنا الخاصة في مالوير بازار، والملف الذي يبدأ عملية ذات اسم فريد هو موضع شك كبير!

في الواقع في القسم التالي المسمى "الشبكة (Network)"، نلاحظ طلب بروتوكول نقل النص التشعبي الذي تم تقديمه إلى عنوان موقع ويب يحتوي على هذا الملف بالذات، لكن قامت البرمجيات الضارة بتنزيل هذا الملف من الإنترنت ثم تشغيله على نظامك الافتراضي. حتى مع تجاهل جميع العلامات التحذيرية السابقة، يجب أن يكون هذا أمرًا مهمًا جدًا لمستند أوفيس.

إذا لم تمنحك علامات التبويب هذه معلومات كافية، فقد ترغب في إلقاء نظرة خاطفة على علامات التبويب الأخرى حيث يمكنك رؤية نشاط إضافي مثل كامل نشاط الشبكة والملفات التي تم الوصول إليها ومفاتيح التسجيل التي تمت قراءتها وتعيينها. يمكن أن ترتبط مفاتيح التسجيل بالإعدادات العامة على ويندوز، وهناك الكثير من المعلومات هنا ويستغرق الأمر خبرة لفهم جميع التفاصيل ولكن قد تجد بعض الأدلة هنا لفهم أي سلوك ضار محتمل بشكل أفضل، لكن في كثير من الأحيان توفر لك علامة تبويب "تقرير" جميع المعلومات التي تحتاجها.

تذكر أنه تم تشغيل العينة أيضًا على نظام التشغيل ويندوز 10، ومن المثير للاهتمام أنه لا يحدث أي شيء ضار في هذه الحالة، لاحظ درجة 1 بدلًا من درجة 10 (من أصل 10) لنظام التشغيل ويندوز 7.

هناك أسباب مختلفة لهذا الأمر، والسبب الأكثر منطقية في هذه الحالة هو أن الثغرة لم تنجح: تم إصلاح الثغرة CVE-2017-11882 في أواخر عام 2017. وقد صدر ويندوز 10 عام 2020 لذلك يتضمن التصحيح الذي أصلح تلك الثغرة الأمنية.

قد تكون الأسباب الأخرى التي تجعل الملف الضار لا يظهر أي نشاط ضار هي قيام المهاجم بإيقاف بيئة الاختبار المعزولة من تشغيله باستخدام تقنيات مكافحة التحليل أو مورد عبر الإنترنت يحاول البرمجية الضارة الاتصال به لم يعد متاحًا، وتذكر أن مجرد كون الملف ضارًا لا يعني أن تشغيله في بيئة اختبار معزولة سيظهر دائمًا نشاطًا ضارًا.

التمرين 10.2. قم بتنزيل العينة 37419d3a8a50d2e5bc0eef676a37d6757ba43a64eff868edb4af5c386900235f من مالوير بازار وقم بتشغيلها في ترایاج، وشارك أكبر عدد ممكن من مؤشرات السلوك الضار كما يمكنك العثور عليه في علامة التبويب "التقارير".

التمرين 10.3. قم بتنزيل العينة a43e0864905fe7afd6d8dbf26bd27d898a2effd386e81cfbc08cae9cf94ed968 من مالوير بازار وقم بتشغيلها داخل ترایاج وابحث عن المؤشرات الضارة، وإذا لم يمنحك التحليل درجة 10 من أصل 10 قم بتشغيله مرة أخرى، ولكن هذه المرة تفاعل مع الجهاز وانقر على "التالي" في التحذير كما يطلب منك ون نوت (OneNote). هل يغير هذا السلوك الذي تم اكتشافه بواسطة بيئة الاختبار المعزولة والنتيجة؟

التمرين 10.4. (اختياري) إذا كنت تستخدم بيئة اختبار معزولة أخرى عبر الإنترنت بانتظام قم بتشغيل العينات من التمرينين السابقين في بيئة الاختبار المعزولة هذا أيضًا. ما هي مؤشرات السلوك الخبيث التي تجدها؟

التمرين 10.5. (اختياري) ابحث عن بعض البرمجيات الضارة الحديثة وقم بتشغيلها في بيئة اختبار معزولة من اختيارك للتعرف على كيفية عمل بيئة الاختبار المعزولة، ويُعدّ مالوير بازار مكانًا رائعًا للعثور على الكثير من البرمجيات الضارة الجديدة، ولكن من الأفضل أن تجد مقالة تحلل البرمجيات الضارة وتحملها ثم يمكنك مقارنة مخرجات بيئة اختبار معزولة مع التحليل الوارد في المقالة لفهم نتائج بيئة اختبار معزولة الخاص بك.

تحليل المرفقات يدويًا

في القسم السابق تعلمت مدى فائدة بيئات الاختبار المعزولة عندما يتعلق الأمر بتحليل مرفقات البريد الإلكتروني أو الروابط الموجودة في رسائل البريد الإلكتروني، وفي معظم الحالات ستعطيك بيئة الاختبار المعزولة جميع المعلومات التي تحتاجها. ولكن في بعض الأحيان تريد أن تفهم مرفقًا ضارًا محتملًا أكثر لأنه يساعدك على القيام بعملك أو ببساطة لأنك فضولي، ويساعدك هذا القسم على فهم كيفية إجراء التحليل اليدوي لأجل تحقيق أكثر تعمقًا.

كان البريد الإلكتروني ناقلًا شائعًا لنشر البرمجيات الضارة منذ أواخر التسعينيات (عندما كان لا يزال يشار إلى البرمجيات الضارة باسم الفيروسات[50]). سيؤدي مجرد فتح مرفق بريد إلكتروني إلى إصابة جهاز الكمبيوتر الخاص بك وبعد ذلك ستقوم البرمجيات الضارة بأشياء سيئة وتستخدم حساب بريدك الإلكتروني لإرسال نسخة من نفسها إلى جميع جهات الاتصال الخاصة بك.

بالنسبة لمؤلفي البرمجيات الضارة أصبحت الأمور أكثر صعوبة هذه الأيام، وتجعل عوامل تصفية الرسائل غير المرغوب فيها الفعالة من الصعب جدًا إرسال ملف قابل للتنفيذ[51] من أي نوع بما في ذلك البرمجيات الضارة،[52] إلى هدف. وتتمتع أجهزة الكمبيوتر أيضًا بحماية أفضل، مثل برنامج مكافحة الفيروسات المدمج، ضد الملفات الضارة التي يتم تنزيلها من الإنترنت أو المضمنة في الأرشيفات مثل ملفات .zip.

[50] كانت تعمل فيروسات الكمبيوتر القديمة بشكل مشابه للفيروسات البيولوجية من حيث إصابتها الملفات السليمة وعملها بمجرد تشغيل ملف "المضيف"، لكن هذه الفيروسات نادرة للغاية هذه الأيام ولا يزال مصطلح "فيروس" يستخدم في كثير من الأحيان للإشارة إلى البرمجيات الضارة نفسها.

[51] ملف يعمل على الكمبيوتر. قد يشمل ذلك البرامج المشروعة ولكن أيضًا الكثير من البرمجيات الضارة، وفي ويندوز غالبًا ما يكون ملحق الملفات التنفيذية هو .exe.

[52] في بعض الحالات لا تُنقل البرمجيات الضارة إلى مجلد الرسائل غير المرغوب فيها، وتتجاهل عوامل تصفية الرسائل غير المرغوب فيها الكثير من رسائل البريد الإلكتروني دون إخطار المستخدم وبالأخص الرسائل الضارة، وقد تقوم أيضًا بإزالة المرفقات الضارة تلقائيًا.

وبالتالي فإن مصممي البرمجيات الضارة يحاولون إيجاد طرق لتجنب ذلك، وينطوي كل ذلك تقريبًا على إقناع المستلم بالتصرف سواء عن طريق النقر على رابط أو تمكين تعليمات الماكرو أو تجاوز قواعد الأمان التي تمنع الإصابة التلقائية بالبرمجيات الضارة.

يحول ذلك عملية تسليم البرمجيات الضارة إلى لعبة قط وفأر، حيث يستمر بائعو الأمن في تحسين اكتشافهم لأنواع الملفات الجديدة ويجعل بائعو البرامج مثل مايكروسوفت من الصعب إساءة استخدام برامجهم بواسطة البرمجيات الضارة، ولكن مصممي البرمجيات الضارة يستمرون في إيجاد طرق جديدة لإيصال البرمجيات الضارة.

نتيجة لذلك لا ينبغي أن يكون هدفك - بصفتك شخصًا يستجيب للحوادث الأمنية - وهدف هذه الوحدة التدريبية هو معرفة كيفية تحليل كل نوع ممكن من الحمولة، ولكن بالأحرى فهم الأساسيات ومعرفة مكان البحث إذا وجدت نوعًا جديدًا من الحمولة.

المرفقات والروابط هما طريقتان مختلفتان يمكن للمهاجمين من خلالهما إضافة حمولة (قد تكون ضارة) إلى رسالة بريد إلكتروني، لكن من الشائع ألا يحتوي المرفق إلا على رابط للحمولة الفعلية أو أن يقوم رابط بتنزيل ملف ضار يمثل الحمولة الحقيقية. وفي بعض الأحيان يحتوي المرفق على رابط يقوم بتنزيل ملف آخر.

مستندات أوفيس الضارة

كما ذكرنا سابقًا يمكن أن تحتوي ملفات مايكروسوفت أوفيس مثل مستندات وورد وجداول بيانات إكسل وعروض باوربوينت التقديمية على واحد أو أكثر من تعليمات الماكرو وهي أجزاء من التعليمات البرمجية التي يتم تشغيلها تلقائيًا، وهناك أسباب مشروعة لاستخدام المؤسسات لتعليمات الماكرو في مثل هذه المستندات لكن تعليمات الماكرو كانت شائعة منذ فترة طويلة بين مصممي البرمجيات الضارة.

مع مطلع القرن العشرين، أصبحت وحدات الماكرو تعمل تلقائيًا بمجرد فتح الملف. وأدى ذلك إلى ظهور رسائل بريد إلكتروني ضخمة حيث تحتوي رسائل بريد إلكتروني تحتوي على مرفقات تقوم عند فتح المرفق بتشغيل تعليمات ماكرو ترسل نسخة من المرفق عبر البريد الإلكتروني إلى كل شخص في دفتر العناوين. من المفهوم أن مايكروسوفت عطلت التشغيل التلقائي لتعليمات الماكرو، ومنذ ما يقرب من عقد من الزمان بدا أن البرمجيات الضارة الكلية أصبحت شيئًا من الماضي.

لكن في حوالي عام 2014 انتقل مصممو البرمجيات الضارة إلى تكتيك جديد يستخدم الانتحال بالهندسة الاجتماعية لجعل المستخدم يقوم بتمكين تعليمات الماكرو حيث سيعرض الملف، على سبيل المثال، صفحة غير واضحة، ومن المفترض أن تدعو الحاجة إلى تفعيل تعليمات الماكرو لإظهار المحتوى وغالبًا ما يذكر شيء مثل "لأسباب أمنية"، وأصبح هذا ناقل إصابة رئيسية للعديد من أنواع البرمجيات الضارة المختلفة.

في الآونة الأخيرة أجرت مايكروسوفت بعض التغييرات التي تجعل من الصعب على الجهات الفاعلة في البرمجيات الضارة حمل المستخدمين على تشغيل تعليمات الماكرو، ولذلك تستخدمها الجهات الفاعلة في البرمجيات الضارة بشكل أقل تكرارًا، ولكن قد لا تزال تصادفها في عملك.

أفضل أداة لتحليل مستندات أوفيس هي oledump.py، وهي أداة كتبها الباحث الأمني البلجيكي ديدييه ستيفنز (Didier Stevens) (كتب أيضًا emldump.py، والتي استخدمناها سابقًا) وتم تضمينه في ريمنوكس (REMnux) والذي ربما قمت بإعداده في الفصل 6، ولكن إذا لم تكن قد قمت بذلك فإن الفيديو في التمرين التالي يشرح كيفية تثبيته.

التمرين 10.6. شاهد ورشة عمل ديدييه على يوتيوب حول تحليل المستندات الضارة. نظرًا لأنك ربما قمت بتثبيت ريمنوكس، يمكنك تخطي الفيديو الأول حول إعداد oledump، ولكن ضع في اعتبارك ما يلي إذا كنت تريد المتابعة مع ما يفعله ديدييه:

- إذا كنت ترغب في تشغيل oledump على ريمنوكس، فقط قم بتشغيل oledumppy متبوعًا بالوسيطات وليس oledump.py/. مثل ما يفعله ديدييه.[53]

[53] إذا قمت بتشغيل أمر على سطر الأوامر، يبحث لينوكس عن ملف قابل للتنفيذ بهذا الاسم في أحد الدلائل العديدة (توضح لك `echo $PATH` أيها)، وإذا كنت ترغب في تشغيل ملف من المسار الحالي عليك إضافة المسار وفي لينوكس يمكنك تحديد المسار الحالي من خلال إضافة نقطة واحدة. يشرح ذلك سبب أنه في الفيديو حيث يتم تثبيت oledump في المسار المحلي يأتي قبل الأمر الخط المائل والنقطة "./".

- ضع قبل أسماء المكونات الإضافية /opt/oledump-files/ لأنه يتم تخزينها في ذلك المسار.
- هذه ورشة عمل طويلة ونوصيك فقط بالجلوس ومشاهدة الفيديو (ربما بسرعة أعلى قليلًا حيث يمكن أن يكون بطيئًا قليلًا) وعدم التركيز على جميع التفاصيل، ولا بأس حقًا إذا كنت لا تفهم أو تتذكر كل شيء وتأكد فقط من أنه في النهاية أنك تعلم:
- كيفية استخدام oledump لإظهار الأجزاء المختلفة من ملف أوفيس (التمرين 1)
- كيفية استخدام oledump لإظهار تعليمات ماكرو فيجوال بيسك مضمنة في مستند (تمرين 6)
- غالبًا ما تستخدم تعليمات ماكرو فيجوال بيسك الضارة تشويشًا على التعليمات البرمجية (التمرين 17) والسلاسل/عناوين موقع الويب (التمرين 20).
- لم تُشرح أوامر نظام لينوكس `less` و`head` صراحة في ورشة العمل ولكن هذا الموقع ويبك ماشينهو مقدمة جيدة إذا لم تكن على دراية بها.

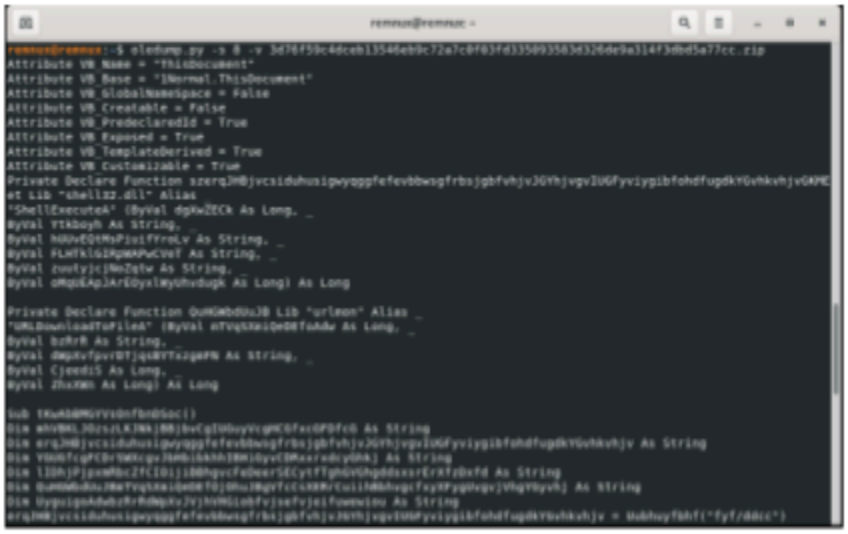
السؤال 10.7. يشرح ديدييه سبب كون أدوات التنزيل أكثر فائدة بشكل عام لمؤلفي البرمجيات الضارة من أدوات الدروبر. هل يمكنك التفكير في ميزة تتميز أخرى تتمتع بها أدوات التنزيل بالنسبة لمؤلفي البرمجيات الضارة؟ (انظر الملحق للعثور على الإجابة.)

دعونا نستخدم oledump في الممارسة العملية. سنفعل ذلك على الملف ذو شفرة التجزئة sha256 3d76f59c4dceb13546eb9c72a7c0f03fd335093583d326de9a314f3dbd5a77cc الذي تم تحميله إلى مالوير بازار قبل كتابة هذا الدليل مباشرة. كما هو شائع فإن الملف الذي يتم تنزيله هو ملف مضغوط محمي بكلمة مرور "infected".

يوفر مالوير بازار بالفعل الكثير من المعلومات الأخرى حول الملف والتي يمكن أن تكون مفيدة إذا كنت ترغب في تحليلها، ولكن لنتظاهر بأننا وجدنا هذا الملف مرفقًا برسالة بريد إلكتروني، ولا توجد معلومات عامة متاحة عنه.

كما أوضح ديدييه في مقاطع الفيديو الخاصة به، يعمل oledump على الملف المضغوط، ويمكننا استخدامه لمعرفة ما إذا كان الملف يحتوي على تعليمات ماكرو فيجوال بيسك وهو ما يحدث في الجزء 8:

يمكننا الآن عرض تعليمات الماكرو:



لا تتناسب جميع تعليمات الماكرو مع الشاشة. إذا قمت بتشغيل هذا بنفسك، يمكنك إضافة `| less` في نهاية الأمر للاطلاع على كامل الخرج، ويمكنك استخدام شريط التمرير على يمين نافذة الوحدة الطرفية لمشاهدة المزيد.

بالعودة خطوة إلى الخلف، استخدم منشئ الملف الطمس الشديد وتعليمات ماكرو فيجوال بيسك، وحتى لو لم تكن مبرمجًا سيجعلك ذلك متأكدًا تقريبًا من أن هذا الملف ضار. إذا كنت تجري تحليلك فقط للتحقق مما إذا كان ضارًا فيمكنك التوقف هنا واستخلاص استنتاجاتك، ولكن قد ترغب في الاستمرار في تحليلك لفهم المزيد عن هذا الملف.

نظرًا لأن أدوات التنزيل أكثر شيوعًا من أدوات دروبر، لنبحث عن عناوين موقع الويب. لا يعمل المكون الإضافي `http_heuristics` من ديدييه هنا (جربه بنفسك للتأكيد) وهذا ليس مفاجئًا، فإذا كان من السهل استخراج عنوان موقع الويب من المستند كانت منتجات الأمان ستفعل ذلك وقد تتحقق من النطاق أو عنوان موقع الويب مقابل قائمة الحظر. ونتيجة لذلك، يخفي مؤلفو البرمجيات الضارة عناوين موقع الويب بشكل جيد ويستمرون في إيجاد طرق جديدة للقيام بذلك.

دعونا نبحث عن السلاسل في المستند، أي شيء بين علامتي اقتباس مزدوجتين (" . . . ")، وهناك حوالي اثني عشر منها لكن معظمها قصير جدًا بحيث لا يحتوي على عنوان موقع الويب غامض. الاستثناء الوحيد هو سلسلة `.fyf/higehsvj0tuofuopdeffg0npd/ujmjlufn/xxx00;tquui`

تستطيع أن تفعل أحد أمرين: أولهما ملاحظة أن هذه السلسلة هي وسيطة الدالة Uubhuyfbhf والتي تعرف أكثر في التعليمة البرمجية، وإذا كنت تفهم البرمجة بعض الشيء سيكون بإمكانك التعرف على ما تفعله هذه الدالة وملاحظة أنها في الواقع تزيل طمس السلسلة إلى عنوان موقع الويب.

يمكنك أيضًا إلقاء نظرة على السلسلة بعناية أكبر وملاحظة أن عنوان موقع الويب يبدأ بـ http:// أو https:// والذي يحتوي على حرفي "t" وإشارتي "/". في نهاية السلسلة لدينا هناك حرفا u وصفران، وإذا نظرت بعناية أكبر قليلًا ستلاحظ أنه عند كتابة tquui بالعكس نحصل على iuuqt وذلك يعني https ولكن بعد دفع أحرفها بحرف واحد ضمن الأبجدية.

إذا لاحظت بعد ذلك أن ":" يتبعها "؛" في جدول الشفرة القياسية الأمريكية لتبادل المعلومات (ASCII) و"0" تتبعها "/"، فستكون اكتشفت الترميز لفك ترميز السلسلة ونحتاج إلى عكسها، وثم النظر إلى الحرف السابق لكل حرف في جدول الشفرة القياسية الأمريكية لتبادل المعلومات. إذا كنت تعرف البرمجة فيمكنك كتابة برمجية نصي قصير ليقوم بذلك أو يمكنك فقط إلغاء طمس السلسلة يدويًا وسترى أنها تُظهر[54]

`https://www.metkilit[.]com/feedcontents/iurgdfhg.exe`

في الواقع، إذا بحثنا عن عينتنا على فايروس توتال، فسنلاحظ أنها تتصل بالنطاق `www.metkilit[.]com`. لكن تذكر أننا تظاهرنا في هذه التجربة بعدم وجود شيء معروف في الملف.

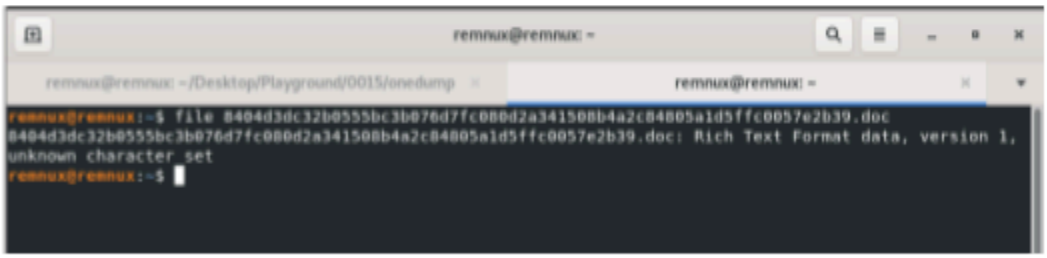
الآن بعد أن أصبح لدينا عنوان موقع الويب يفترض أن البرمجية الضارة تبحث فيه عن التنزيلات يمكننا التحقيق في هذا الأمر بشكل أكبر إذا أردنا ذلك، وفي وقت لاحق من هذا الدليل سنلقي نظرة موجزة على تحليل عناوين موقع الويب.

أن تفهم كيفية عمل طمس عنوان موقع الويب هو أمر وأن تكون قادرًا على العثور عليه بنفسك هو أمر آخر، ولكن لأجل ذلك تحتاج إلى أمرين آخرين هما الحظ والخبرة. تحتاج الحظ لأن الطمس في هذه الحالة كان بسيطًا إلى حد ما وأيضًا لأنك تحتاج فقط إلى رؤيته. عند إجراء تحليل مشابه من المفيد دائمًا العمل ضمن المجموعة، من المرجح أن يكتشف شخصان (أو أكثر) نمطًا ما أكثر من شخص واحد.

[54] تذكر الممارسة الجيدة لإضافة الأقواس المربعة حول النقطة النهائية في اسم النطاق "لإزالة الضرر منها"، وانظر الفصل 7.

دعونا الآن نلقي نظرة على برمجية ضارة أخرى:
8404d3dc32b0555bc3b076d7fc080d2a341508b4a2c84805a1d5ffc0057e2b39، وهي العينة التي قمنا بتحليلها في تراياج أعلاه. إذا قمنا بتشغيل oledump على الملف المضغوط فسنحصل على خطأ مفاده أنه ليس ملفًا مضغوطًا صالحًا، وقد تعتقد أن تفريغ الملف يساعد[55]، ولكن تشغيل oledump على ملف.doc يؤدي إلى نفس الخطأ.

لحسن الحظ يوجد في لينوكس أمر `file` مفيد والذي يخبرنا أن هذا ملف بتنسيق ريتش تيكست فورمات (Rich Text Format):



تحتوي ملفات آر تي إف (RTF) هذه (التي غالبًا ما تحتوي على ملحق .rtf، ولكن كما ترى تأتي أيضًا بتنسيق .doc) على تنسيق مختلف مقارنةً بملفات وورد العادية. ولحسن الحظ هناك أداة أخرى كتبها ديدييه والتي تم تضمينها أيضًا في ريمنوكس وهي rtfdump.py.

مثل oledump تُظهر لك rtfdump الأجزاء المختلفة التي يتكون منها المستند.

على غرار oledump يمكننا تفريغ محتويات كل قسم، لكن لسوء الحظ ليست الأمور بهذه البساطة بعد هذه الخطوة. عندما يشمل مستند أوفيس على تعليمات ماكرو فيجوال بيسك ضارة، فإن البرمجيات الضارة هي ميزة في أوفيس حتى لو كانت غير مرغوب فيها إلى حد ما، ولكن في هذه الحالة تعمل البرمجيات الضارة على شكل خلل وبتعبير أدق يستخدم ثغرة أمنية في أوفيس تسمى CVE-2017-11882. وهذا يجعل من الصعب العثور على البرمجيات الضارة، بالإضافة إلى الصعوبات الناجمة عن الطمس في الشفرة الضارة.

لفك تشفير البرمجيات الضارة ربما يتعين على المحلل فهم الأعمال الداخلية لملفات آر تي إف والثغرة CVE-2017-11882 وقد يضطر حتى إلى تكييف أداة rtfdump، وفي الواقع يواصل ديدييه إضافة ميزات جديدة إلى أدواته استجابة لتحديات جديدة مثل هذه.

قد يكون عدم التمكن من فك تشفير البرمجيات الضارة أمرًا محبطًا ومحرجًا بعض الشيء، لكن هذا واقع تحليل البرمجيات الضارة. وأحد الدروس المهمة في هذا المثال هو أننا تمكنا من تحليل الملف في تراياج مما أعطانا كل ما نحتاجه، ويوفر هذا حجة إضافية لاستخدام بيئات الاختبار المعزولة بدلًا من الاعتماد فقط على التحليلات اليدوية.

[55] تذكر من الفصل 7 أنك ستحتاج على الأرجح إلى تشغيل `7z x [file]` بدلًا من `unzip [file]`.

التمرين 10.8. (اختياري) لأجل توضيح المثال نوفر لكم HYPERLINK "https://isc.sans.edu/forums/diary/Dissecting%2Ba%2BCVE201711882%2BExploit/24272/" \h

تكتسب الخبرة من خلال الممارسة وقراءة ما يفعله الآخرون، وهذه عملية طويلة وحتى بعد اكتسابها غالبًا ما يواجه محللو البرمجيات الضارة المتقدمون عقبات. لا تدع ذلك يثبط عزيمتك ولا تدع نفسك تشعر بأنه عليك أن تكون قادرًا على التعامل مع أي مرفق، فحتى المحللون من ذوي الخبرة يواجهون مشاكل بانتظام.

مرفقات بي دي إف (PDF)

ملفات بي دي إف هي مرفقات شائعة أخرى، كان هناك وقت كانت فيه الثغرات الأمنية أكثر شيوعًا في أدوبي ريدر (Adobe Reader) وهو قارئ بي دي إف الأكثر شيوعًا، وكان استخدام ملفات بي دي إف الضارة طريقة شائعة لإصابة الأجهزة التي تشغل إصدار قارئ بي دي أف أقدم.

هذا أقل شيوعًا هذه الأيام لكن ملفات بي دي إف الضارة لا تزال موجودة، وفي بعض الأحيان يُضمّن مستند آخر فيها مثل مستند أوفيس ضار وفي أحيان أخرى تحتوي فقط على رابط يقوم بتنزيل حمولة المرحلة التالية.

مرة أخرى بنى ديدييه ستيفنز العديد من الأدواتلتحليل بي دي إف، كما أنشأ ورشة عمل فيديو لعرض بعض هذه الأدوات. ومع ذلك فإن ورشة العمل هذه عمرها 11 عامًا وتركز في الغالب على نوع البرمجيات الضارة بي دي إف التي كانت شائعة في ذلك الوقت. إذا كنت تتعامل بانتظام مع ملفات بي دي إف فقد لا تزال تستفيد من مشاهدة ورشة العمل ولكن اعتبرها اختيارية.

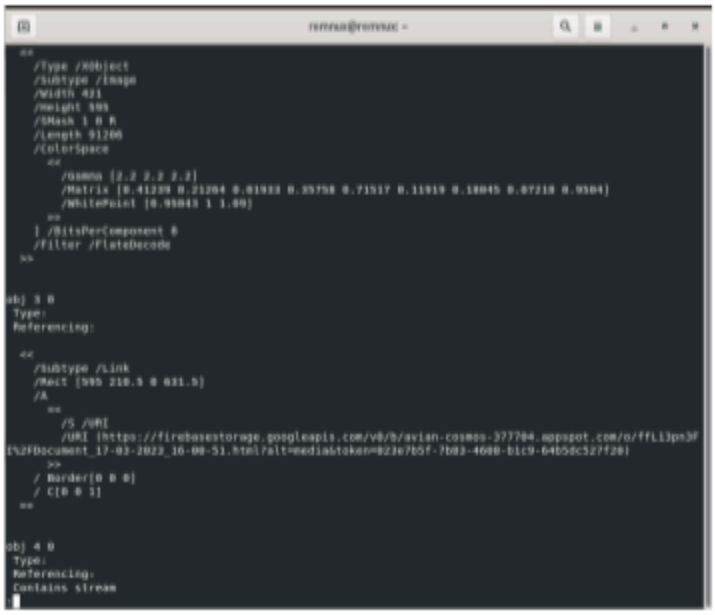
أداة بي دي إف الرئيسية لديدييه هي pdf-parse.py، والتي كما يوحي الاسم تحلل ملف بي دي إف.

لنأخذ مرة أخرى عينة تم تنزيلها من مالوير بازار:
26509fa876a07966824bed8e5b0a6e0626b37d68355871fac49b2fa636d7fe6e.

لنقم أولًا بتشغيل:

```
pdf-parser.py
26509fa876a07966824bed8e5b0a6e0626b37d68355871fac49b2fa636d7fe6e.pdf |less
```

على سطر واحد لتصفح المكونات المختلفة للملف، ولاحظ كيف يتكون ملف بي دي إف من كائنات مرقمة مختلفة. إذا استعرضنا الكائنات، فسنلاحظ عنوان موقع الويب في الكائن 3 المستضاف على وحدة تخزين فاير بيس من غوغل. هذه خدمة سليمة، وفي حال لم تكن تعرف ذلك يمكن لبحث سريع على الإنترنت أن يوضح ذلك، ولكنها تستخدم عادة لاستضافة البرمجيات الضارة.

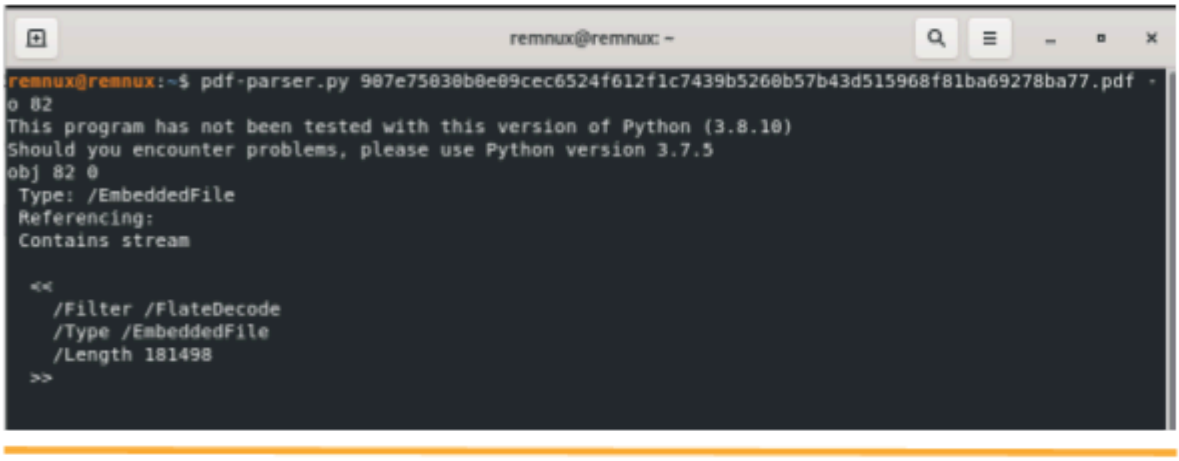


وهنا تنتهي العملية، فقد استخرجنا عنوان موقع الويب من ملف بي دي إف وهذا كل ما تحتاج إلى معرفته. (لأجل التأكد يمكنك التحقق من الكائنات الأخرى في الملف لضمان من عدم وجود شيء آخر.)

ملف بي دي إف آخر يمكنك تجريبه هو 907e75030b0e09cec6524f612f1c7439b5260b57b43d515968f81ba69278ba77.

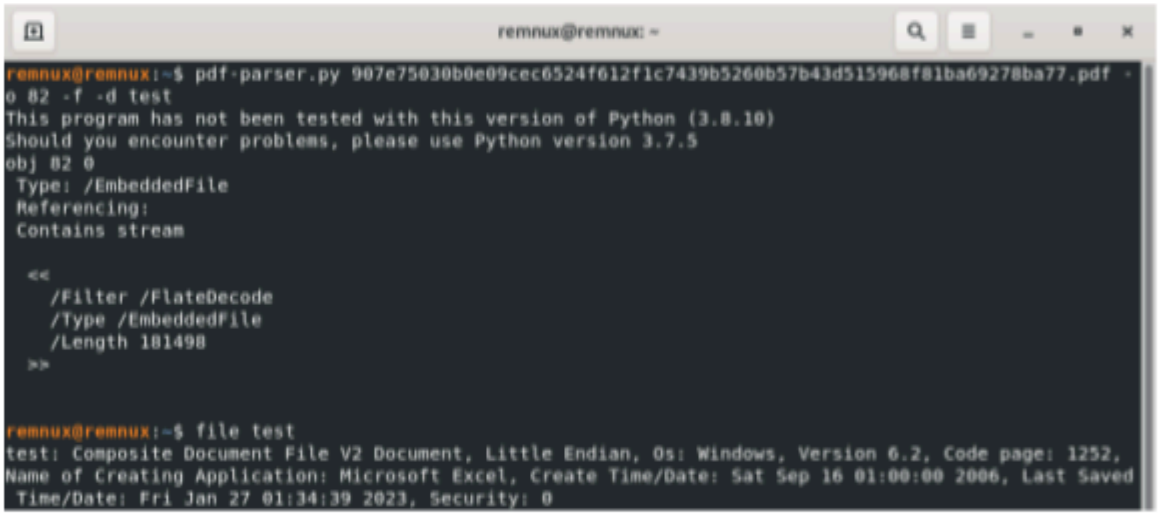
لتصفح الكائنات المختلفة يمكننا تشغيل pdf-parser.py على هذا الملف متبوعًا بوسيط `| less`، لكن لسوء الحظ لا ينتج عن هذا عنوان موقع الويب ولذلك نحتاج إلى دراسة الكائنات بعناية أكبر. قد يكون من المفيد النظر إلى أطوال الكائنات: يبلغ طول العديد منها 10 بايت مما يعني أنه من غير المرجح أن تحتوي على أي شيء ضار.

نرى بعض الكائنات الأكبر، بدءًا من الكائن 61 الذي تظهر فيه عبارة `/Subtype /Image`، ويمكنك أن تخمن على الأرجح أنها تحتوي الصور مضمنة في ملف بي دي إف. ولكن بعدها يوجد الكائن 82 وهو ملف مضمن (`/Type /EmbeddedFile`)، ويتيح لنا إضافة الخيار `-o` إلى نهاية الأمر الذي أدخلناه للتو إظهار هذا الكائن فقط:



تقوم أداة pdf-parser باستخراج الكائن باستخدام الخيار `-d` (بمعنى "تفريغ (dump)") متبوعًا باسم ملف. نظرًا لأن الكائن مشفر (انظر `/Filter /FlateDecode`)، يمكننا أيضًا استخدام `-f` لفك تشفيره.

نقوم هنا بتخزين البيانات المستخرجة في ملف ونختبرها ثم نستخدم أمر الملف للعثور على ماهية الكائن. وكما يتضح لنا إنه مستند إكسل! يمكننا تحليله بشكل أكبر باستخدام oledump في حال رغبنا بذلك.



تمرين 10.9. استخدم الخيار `-d` في `pdfdump.py` لاستخراج صورة واحدة من ODF.

تمرين 10.10. استخدم أداة pdf-parser لتحليل ملف بي دي إف ad517cb885ee279ec6ca95cd7402da998ec5461461f745c2f075085ef49b4eb6.

تمرين 10.11. (اختياري) افتح ملفَي بي دي إف في ترايا‌ج أو بيئة اختبار معزولة أخرى تختارها وتأكد مما أظهره التحليل اليدوي.

أنواع المرفقات الأخرى

هناك العديد من أنواع المرفقات الأخرى المستخدمة لنشر البرمجيات الضارة ويستمر الفاعلون الخبيثون في العثور على مرفقات جديدة لاستخدامها، وكما ذكرنا سابقًا لا داعي لتوقع أن تتمكن من معرفة كيفية تحليلها جميعًا. فإذا صادفت نوع ملف جديد لا تعرف كيفية التعامل معه ابحث عنه على الإنترنت، فمن المحتمل جدًا أن يكون شخص ما قد كتب أداة و/أو دليلًا حول كيفية تحليل هذا النوع المعين من الملفات.

قد يكون هذا الشخص هو ديدييه ستيفنز، ومن المفيد متابعة مدوّنته ومنشوراته على إنترنت ستورم سينتر بلوغ (Internet Storm Center blog).

على سبيل المثال، في الأشهر الأولى من عام 2023 كتب ديدييه كيفية تحليل ملفات ون نوت وي‌باك ماشين وملفات إتش تي إيه (HTA) وي‌باك ماشين.

تحليل روابط

على عكس المستند الضار لا يحتوي رابط الويب (أو عنوان موقع الويب) أي شيء فعلي وإنما مجرد رابط لمورد في مكان آخر، قد تكون هذه صفحة لغة تمييز النص التشعبي أو برمجية ضارة أو حتى صفحة تحتوي على خطأ 404. ويعتمد ما يعيده الرابط في بعض الأحيان على كيفية ووقت تقديم جهازك للطلب. تتوقف العديد من عناوين موقع الويب عن العمل بعد مرور بعض الوقت وهو ما ينطبق بشكل خاص على الروابط الضارة، لكن حتى عندما يكون هذا هو الحال لا يزال التحليل ممكنًا.

أولًا هناك اسم النطاق الذي تم استخدامه، غالبًا ما يكون هذا هبة كبيرة عندما تحاول تحديد ما إذا كان الرابط ضارًا أم لا. ارجع إلى الفصل 7 للتذكير بكيفية استخدام فايروس توتال للحصول على مزيد من المعلومات حول اسم نطاق يحتمل أن يكون ضارًا.

ثانيًا يمكنك الاطلاع على الحمولات عند محاولة الوصول إلى الرابط، وهنا ستحتاج إلى الحظ فربما تمت إزالة المورد أو تغييره. وحتى إذا كان المورد لا يزال موجودًا، فقد لا يقدمه لك الخادم الضار حسب عنوان بروتوكول إنترنت الخاص بك أو متصفح الويب أو بعض الخصائص الأخرى، وبالطبع ستحتاج إلى تنزيله في بيئة آمنة، مثل ريمنوكس. يمنحك التمرين الاختياري 10.12 أدناه بعض الإرشادات حول كيفية القيام بذلك.

بشكل عام من الأكثر أمانًا فتح عنوان موقع الويب في بيئة اختبار معزولة، ولن يساعدك هذا إذا تمت إزالة المورد أو تغييره ولكن إذا كان لا يزال موجودًا فسيكون فتحه في بيئة اختبار معزولة أقل خطورة. تذكر أنه في قسم "التنزيلات" في ترايا‌ج يمنحك إمكانية الوصول إلى الملفات التي تم تنزيلها في حال كنت ترغب في تحليلها أكثر.

في أوائل عام 2010، كانت "التنزيلات غير المصرح بها" طريقة شائعة لإصابة أجهزة الكمبيوتر، حيث يكتشف موقع الويب الضار أو المصاب أن متصفحك أو أحد مكوناته الإضافية (مثل فلاش بلاير أو جافا) معرّض للاختراق ويستخدم هذه الثغرة لتثبيت البرمجيات الضارة على جهاز الكمبيوتر الخاص بك، لكن تعمل المتصفحات الحديثة اليوم على حظر الإضافات المحفوفة بالمخاطر

وعادة ما تقوم بتثبيت تحديثات الأمان تلقائيًا مما يجعل مثل هذه التنزيلات غير المصرح بها أكثر ندرة. لكنها لا تزال موجودة وفي بعض الحالات تستغل ثغرات يوم الصفر في المتصفحات.

لهذا السبب لا يزال فتح الروابط المشبوهة في المتصفح ليس بفكرة جيدة حتى لو كان الخطر أصغر بكثير مما كان عليه في السابق.

التمرين 10.12. ابحث عن عنوان موقع الويب ضار حديث فيو آر إل هاوز (URLhaus) وهو موقع ويب ينتمي للأشخاص الذين يشغلون أيضًا مالوير بازار وافتحه في ترایاج أو بيئة اختبار معزولة أخرى من اختيارك. تأكد من أن المحتوى الذي تم تنزيله مرئي في علامة تبويب "التنزيلات" في ترایاج وفي حال لم يحدث شيء جرّب عنوان موقع ويب مختلف. (يدفعك هذا التمرين إلى البحث عمدًا عن عناوين موقع الويب بنفسك بدلًا من اقتراحها)

التمرين 10.13 (اختياري) اقرأ مقالة مدونة ديك_ماشين هذه حول استخدام `curl` لتنزيل المحتوى من عنوان موقع ويب ضار محتمل وتجربته باستخدام بعض عناوين موقع الويب الحديثة من URLhaus.

عملاء بريد إلكتروني معرضون للاستغلال

هناك أخيرًا نوع مختلف من رسائل البريد الإلكتروني الضارة النادرة ولكنها تبقى جديرة بالذكر حيث يجري استغلال ثغرة أمنية في وكيل بريد إلكتروني مباشرة من خلال بريد إلكتروني مصمم خصيصًا. في مارس 2023 اكتشف ديك_ماشين أن مجموعة قرصنة مرتبطة بروسيا تُعرف باسم فانسي بير (Fancy Bear) أو إيه ب تي 28 (APT28) (أو العديد من الأسماء الأخرى) كانت تستخدم ثغرة يوم الصفر في آوتلوك (Outlook) لإصابة أجهزة الكمبيوتر بهذه الطريقة.

لا توجد طريقة عامة لتحليل الرسائل الإلكترونية هذه، فقد يستخدم المهاجمون أنواعًا مختلفة من الثغرات ويحرصون جدًا حيال استخدام ثغرات اليوم الصفر، ففي كثير من الأحيان لا يريد المهاجمون الكشف عن قدرتهم على استغلالها خشية أن يتعرف عليها مطورو برامج البريد الإلكتروني عنها ويقوموا بتصحيحها. بيد أن هذه الحالات نادرة جدًا، ولكن هذا يسلط الضوء على أهمية التأكد من تحديث عملاء البريد وهو أمر يقوم به عملاء البريد الإلكتروني على الويب تلقائيًا.