الفصل السابع:
التحليل الذكي للتهديدات وفايروس توتال (VirusTotal)

يركز هذا الفصل على التحليل الذكي للتهديدات واستخدام فايروس توتال.

يساعدك **التحليل الذكي للتهديدات** (أو التحليل الذكي للتهديدات الرقمية، والذي غالبًا ما يكون اختصاره CTI بالإنجليزية) على فهم الهجمات الرقمية وسياقها مثل من المسؤول عنها والروابط الموجودة بين الهجمات المختلفة.

على سبيل المثال، إذا كنت تساعد صحفيًا تلقى بريدًا إلكترونيًا للتصيد الاحتيالي فربما عليك أن تفهم أكثر مما إذا كان البريد الإلكتروني يهدف إلى التصيد الاحتيالي مثل فهم نوع البريد الإلكتروني للتصيد الاحتيالي. هل كان بريد تصيد احتيالي عادي تم إرساله إلى الآلاف أو الملايين من الأهداف العشوائية؟ أم هل تم إرساله إلى شخص معين وربما إلى عدد قليل من الأشخاص الآخرين من قبل ممثل يستهدفهم؟ قد يعتمد ما تقدمه من دعم على إجابات هذه الأسئلة.

وفي حال كان التهديد يتضمن ملفًا أو تطبيقًا ضارًا ("برمجية ضارة") فقد ترغب أيضًا في فهم ما يحاول فعله، حيث يمكن أن يساعدك هذا في التخفيف من التهديد في حالة تشغيل البرمجية الضارة بالإضافة إلى فهم كيفية الدفاع ضده في المستقبل.

يُعدّ التحليل الذكي للتهديدات مجالًا ضخمًا وهناك الكثير من الأمور التي يجب معرفتها عنه، وبالتأكيد أكثر مما يمكن أن يتسع ضمن هذا الدليل، وإذا كنت مهتمًا بالغوص بشكل أعمق فيه فقد كتبت خبيرة التحليل الذكي للتهديدات كاتي نيكلز (Katie Nickels) خطة دراسة ذاتية مؤلفة من جزأين (الجزء الأول وي باك ماشين (wayback machine)؛ الجزء الثاني وي باك ماشين).

فايروس توتال (VirusTotal)

فايروس توتال هي خدمة شائعة عبر الإنترنت يمكن استخدامها للتحليل الذكي للتهديدات من النوع الأساسي وأحيانًا من النوع الأكثر تقدمًا، وتأسست في عام 2004 في إسبانيا واستحوذت عليها غوغل (Google) في عام 2012. لكن في وقت كتابة هذا التقرير (نوفمبر/تشرين الثاني 2022) لم تكن الواجهة الأمامية مدمجة بصورة متكاملة مع خدمات غوغل الأخرى، فعلى سبيل المثال ليست الحسابات على الموقع مرتبطة مباشرة بحساب غوغل.

كانت وظيفة فايروس توتال الأصلية هي أن تكون مستودع برمجيات ضارة، حيث يمكن فحص الملفات في العديد من منتجات مكافحة الفيروسات وربما لا تزال هذه هي الميزة الأكثر شهرة. نظرًا لأن الأشخاص والمؤسسات قاموا بتحميل ملايين البرمجيات الضارة على فايروس توتال على مر السنين، من المرجح أيضًا أن تكون توتال أكبر مستودع للبرمجيات الضارة في العالم مما يجعلها مكانًا رائعًا للبحث عن روابط بين أنواع مختلفة من البرمجيات الضارة.

وما يزيد من فائدة ذلك هو أن فايروس توتال لا يركز فقط على عينات البرمجيات الضارة ولكن يستكشف أيضًا العناصر المختلفة التي تتفاعل معها العينات. يقوم فايروس توتال أيضًا بمسح وتجميع عناوين بروتوكول الإنترنت وأسماء النطاقات وعناوين مواقع ويب والعثور على روابط بينها. حيث يمكنك تحميل مرفق تجده في رسالة بريد إلكتروني والتعرف أنه برمجية ضارة وتتعرف أنه مرتبط بنطاق كان يشير في وقت ما إلى عنوان بروتوكول الإنترنت يرتبط به ملف برمجية ضارة أخرى عند تشغيله، وبالتالي تستنتج أن المرفق الأصلي الذي قمت بتحميله مرتبط بهذا البرمجية الضارة المعروفة.

قبل فتح فايروس توتال، هناك شيئان مهمان يجب ملاحظتهما. أولًا لا تقم فقط بتحميل الملفات إلى فايروس توتال دون فهم ما تفعله وثانيًا، ليست عملية التوصّل إلى هذه الصلات دقيقة ومن السهل استخلاص التوصل إلى نتائج غير صحيحة. على سبيل المثال، تتم إعادة تعيين عناوين بروتوكول الإنترنت بشكل متكرر إلى منظمات جديدة، ولذلك قد يكون عنوان بروتوكول الإنترنت الذي كان ضارًا في الأسبوع الماضي حميدًا هذا الأسبوع. وبالتالي يجب أن نحذر من استخلاص استنتاجات سريعة بالأخص إذا كانت لهذه الاستنتاجات عواقب.

مفاهيم مهمة للاستخبارات المتعلقة بالتحليل الذكي للتهديدات

يُقدّم هذا القسم بعض المفاهيم المهمة التي ستحتاج إلى معرفتها لبقية الفصل والفصول المستقبلية.

يُقدّم هذا الفصل نظرة عامة موجزة عن هذه المفاهيم، لكن نشجعك على استخدام محرك البحث المفضل لديك لاستكشاف كل موضوع بتعمّق أكبر. وربما تكون محركات البحث إحدى أهم الأدوات في عملك المتعلق بالتحليل الذكي للتهديدات. بغض النظر عن مدى تقدم مهاراتك، ستجد دائمًا الحاجة إلى البحث عن الأشياء وغالبًا ما تكون أشياء أساسية مدهشة. وتُعدّ القدرة والشعور بالراحة عند القيام بذلك مهارة مهمة لأي شخص يعمل على التحليل الذكي للتهديدات.

مؤشرات الاختراق

يُشير مصطلح **مؤشر الاختراق** إلى أي أثر أو دليل يُعثر عليه أثناء البحث عن جهاز أو شبكة مخترقة، ويدل ذلك عادةً على عناوين بروتوكول الإنترنت أو النطاقات التي تتصل بها البرمجيات الضارة أو النظام المخترق أو أي ملفات ضارة يتركها المهاجم على نظامك. وفي بعض الأحيان يُشير أيضًا إلى عناوين البريد الإلكتروني أو عناوين البيتكوين أو العبارات الشائعة التي يستخدمها المهاجم أو الآثار الخفية.

إذا كنت ترغب في النشر عن حادث تعاملت معه أو تهديد قمت بتحليله فمن الممارسات الجيدة تضمين ملخص منفصل عن مؤشرات الاختراق التي وجدتها، فهو يساعد الآخرين على التحقق من أنظمتهم وشبكاتهم، على سبيل المثال عن طريق التحقق من سجلات النظام أو الخادم للحصول بحثًا عن دليل على هجوم مماثل.

فيما يلي نظرة أعمق عن بعض مؤشرات الاختراق التي قد تواجهها.

عناوين بروتوكول الإنترنت

عناوين بروتوكول الإنترنت هي عناوين يمكن أن يقرأها الكمبيوتر، وهب مؤلفة من أرقام وأحيانًا أحرف لكل جهاز متصل بالإنترنت. وعلى عكس عنوان الشارع أو رقم الهاتف، غالبًا ما تتم إعادة تعيينها بسرعة من قبل الشبكة حتى تتمكن من استيعاب المزيد من الأجهزة، فعلى سبيل المثال قد تعيد شبكة الواي فاي المنزلية إصدار عنوان بروتوكول إنترنت نفسه إلى جهاز الكمبيوتر المحمول أو هاتفك أو أجهزة صديقك اعتمادًا على التوافر. تُعدّ أسماء النطاقات اللبنة الأساسية للعناوين التي يمكن للبشر قراءتها والتي يمكن أن تستخدمها لزيارة مواقع الويب والتي تقوم أيضًا "بإيجاد" أو الاتصال بنطاق معين من عناوين بروتوكول إنترنت.

عندما نُشير إلى عناوين بروتوكول إنترنت، فإننا نعني عادةً **بروتوكول الإنترنت الإصدار 4** (IPv4)، وهناك أيضًا عناوين **بروتوكول الإنترنت الإصدار 6**، ولكن في هذا الدليل يكون عنوان بروتوكول الإنترنت هو من الإصدار 4، ما لم يُذكر خلاف ذلك. ولا توجد عناوين بروتوكول إنترنت بخلاف الإصدارين 4 و6.

لا يتعين عليك فهم جميع تفاصيل كيفية عمل عناوين بروتوكول إنترنت، لكن من المهم أن تتمكن من القيام بما يلي على الأقل:

- التعرف على شكل عناوين بروتوكول الإنترنت الإصدار 4 وبروتوكول الإنترنت الإصدار 6.
- فهم ماهية عنوان بروتوكول إنترنت الخاص (الإصدار 4) مثل 192.168.1[.]2 [18].
- التعرّف على أداة تور (Tor) وكيف تخفي عنوان بروتوكول الإنترنت الخاص بشخص ما.
- فهم ما تعنيه الشبكة الظاهرية الخاصة وكيفية إخفائها لعنوان بروتوكول إنترنت الخاص بشخص ما.

تتمثل إحدى الطرق التي تسمح لك بالعثور على عنوان بروتوكول إنترنت يجري اتصالًا مشبوهًا في العثور ضمن سجل مواقع الويب لديك على عنوان بروتوكول إنترنت يطلب عنوان موقع ويب يبدو أنه يستغل ثغرة[19]. قد يكون عنوان بروتوكول إنترنت الذي تراه هو عنوان بروتوكول إنترنت العام للممثل الخبيث. لكن تستخدم العديد من الجهات الفاعلة الضارة أحد أنواع الوكلاء، مثل تور أو شبكة ظاهرية خاصة لإخفاء عنوان بروتوكول الإنترنت الخاص بهم. لذلك في هذه الحالة قد لا يكون عنوان بروتوكول إنترنت مناسبًا لبحثك، ولكن معلومة أن "الممثل الخبيث يستخدم أداة تور للاتصال" هي أيضًا أمر من المفيد تتبعه أو مشاركته.

```
44.203.11.113 - - [15/Nov/2022:10:32:23 +0000] "GET /feed/
87.249.108.114 - - [15/Nov/2022:10:34:44 +0000] "HEAD /feed
92.247.181.17 - - [15/Nov/2022:10:37:29 +0000] "GET /feed/
54.211.20.179 - - [15/Nov/2022:10:38:05 +0000] "GET /tag/vi
Chrome/80.0.3987.122 Safari/537.36"
3.81.136.228 - - [15/Nov/2022:10:38:56 +0000] "GET /categor
hrome/80.0.3987.122 Safari/537.36"
195.145.170.187 - - [15/Nov/2022:10:39:09 +0000] "GET /cate
85.119.83.156 - - [15/Nov/2022:10:40:04 +0000] "GET /feeds/
```

عناوين بروتوكول الإنترنت في سجل خادم الويب

إذا كنت ترغب في دراسة عنوان بروتوكول الإنترنت، عليك أن تحاول أن تعرف ما إذاكان:

- يخضع للتحكم الكامل من قبل الممثل الذي يدير صفحة التصيد الاحتيالي (موقعه الخاص، وليس موقع استضافة عام مثل إمجور (imgur) أو يوتيوب (YouTube))، وفي هذه الحالة يمكنك أن تكون واثقًا بشكل معقول من أن المحتوى الآخر المستضاف هناك مرتبط بنفس الممثل.
- مشترك مع محتوى آخر، حيث تستضيف العديد من عناوين بروتوكول الإنترنت خدمات متعددة غير ذات صلة، مثل خادم الويب الذي يخدم مواقع ويب متعددة أو خادم البريد الذي يخدم نطاقات متعددة. لا ترتبط هذه الخدمات بالضرورة ببعضها البعض، ولاحظ أيضًا أن المحتوى السليم في بعض الأحيان يشترك بعنوان بروتوكول الإنترنت ذاته مع أنواع محتوى ضار مختلفة ومتعددة دون أي نوع آخر من الأدلة (على سبيل المثال، صفحات التصيد الاحتيالي التي تبدو متشابهة جدًا)، في هذه الحالة لا يمكنك ربط المحتوى المستضاف على نفس عنوان بروتوكول إنترنت بذات الممثل بثقة.
- يُدار من كيان سليم ولكن تعرض لاختراق بطريقة ما. على سبيل المثال قد يكون ممثل خبيث قد اخترق الخادم، وفي هذه الحالة ستحتاج إلى فهم الاختراق ومتى حدث قبل أن تتمكن من استخلاص أي استنتاجات بناءً على عنوان بروتوكول إنترنت.

غالبًا ما يكون من الصعب معرفة أي من هذه المواقف الثلاثة أنت فيها، ولكن خدمة مثل فايروس توتال يمكن أن تساعدك في ذلك.

أسماء النطاقات وأسماء المضيفين ونظام أسماء النطاقات

اسم النطاق هو جزء من عنوان إنترنت يمكن أن يقرأه الإنسان ويشترى من سجل نطاقات، وفي الغالب نطاق المستوى الأعلى (.com و .org و .co.uk و .in و .br وما شابه.) وكل ما يسبق تلك النقطة مباشرة (google و amazon وinternews وما إلى ذلك). يشير **اسم المضيف** إلى هذا العنوان بالإضافة إلى أي نطاقات فرعية

[18] تجاهل الأقواس المربعة في الوقت الحالي حيث سيتم شرحها في قسم "إزالة الضرر" لاحقًا في هذا الفصل.
[19] هذا أمر شائع للغاية ويتم تنفيذ معظم هذه الطلبات تلقائيًا بالكامل ولا يتم استهدافها، ولا يعني ذلك أن الخادم يعاني من ثغرة أمنية معينة أو حتى أنه يشغّل تلك البرمجية بعينها!

قد يقوم مالك النطاق بإعداده ضمن نطاقه. ومثال على ذلك أن internews[.]org أو google.co[.]uk تُعدُّ أسماء نطاقات وأسماء مضيفين، ولكن www.internews[.]org و mail.google.co[.]uk هي أسماء مضيفين فقط. غالبًا ما يستخدم مصطلحا اسم النطاق واسم المضيف بالتبادل، ولست مضطرًا إلى فهم جميع تفاصيل كيفية عمل أسماء النطاقات وأسماء المضيفين و**أنظمة أسماء النطاقات** لكن من المهم أن تتمكن من القيام بما يلي على الأقل:

- التمييز بين نطاقات المستوى الأعلى لرموز البلاد ونطاقاتالمستوى الأعلى الأخرى
- التعرف على ماهية النطاق الفرعي
- معرفة كيفية استخدام أمر dig على لينوكس (على سبيل المثال، مثيل ريمنوكس الخاص بك) لإجراء عمليات بحث نظام أسماء النطاقات (هذه مقدمة جيدة)
- التعرف على سجلات A وAAAA وMX
- معرفة كيفية العثور على تاريخ تسجيل النطاق باستخدام أمر 'whois'
- التعرّف على مسجّل اسم النطاق

عندما تواجه اسم مضيف أثناء تحليل تهديد، يكون ذلك عادةً بسبب استضافة بعض المحتوى هناك أو بسبب إجراء اتصال باسم المضيف. إذا كنت ترغب في دراسة اسم النطاق أو اسم المضيف بشكل أكبر، عليك تحديد ما إذا كنت في أحد المواقف التالية:

- النطاق سليم ولا يستخدم لأي أغراض ضارة: مثل عنوان internews[.]org. قد تظل البرمجيات الضارة متصلة بالنطاقات المشروعة أحيانًا لسبب واضح (قد تستخدم، على سبيل المثال، موقعًا مثل whatismyipaddress[.]com لتحديد عنوان بروتوكول إنترنت العام للجهاز)، وأحيانًا يكون ذلك طعمًا.
- النطاق سليم ولكنه يستخدم أيضًا لأغراض ضارة: مثل drive.google[.]com الذي من الواضح أنه موقع سليم ولكن تستضاف الكثير من البرمجيات الضارة هناك.
- نطاق شرعي ولكن تم اختراقه واستخدامه لأغراض ضارة: من المحتمل أن يحدث الاختراق على الخادم الذي يشير إليه النطاق ولكن أيضًا على مستوى نظام أسماء النطاقات، وفي الحالة الثانية يمكن أن يساعدك استخدام موقع مثل فايروس توتال في التحقق من سجل نظام أسماء النطاقات.
- تم تسجيل النطاق وإعداده لأغراض ضارة.

عند تسجيل نطاق، لا يقول الممثلون الضارون إنهم سيستخدمونه للتصيد الاحتيالي أو البرمجيات الضارة، ولذلك إذا كنت ترغب في فهم ما إذا كان قد تم إعداد نطاق لأغراض ضارة فسيتعين عليك إجراء بعض التحقيقات.

النطاقات المسجلة لأغراض ضارة:

- عادة ما تكون مسجلة في فترة حديثةنسبيًا.
- غالبًا ما تبدو عشوائية جدًا (على سبيل المثال vniopquiopvqr[.]com) أو تشبه السليمة (على سبيل المثال internews-official[.]org).
- تستخدم في كثير من الأحيان نطاقات المستوى الأعلى غير العادية مثل .top أو .surf.
- في كثير من الأحيان لا يكون لها سجل MX تم إعداده أو تستخدم السجل الافتراضي من المسجل.

لا تكون عمليات بحث نظام أسماء النطاقات عن نطاق ما مرئية للكيان الذي يدير النطاق[20]، ولكن يتم إجراء تحقيق نشط لخادم الويب أو خادم البريد من خلال الاتصال بهذا النطاق. ويجب أن تراعي ما إذا كنت لا تريد أن يرى غيرك أنك تقوم بالتحقيق، ويمكنك استخدام شبكة ظاهرية خاصة أو تور لإخفاء هويتك.

[20] قد يلاحظون وجود عملية بحث تجري إذا كان لنطاق فرعي محدد للغاية، ولكن هذه حالة بعيدة.

إزالة الضرر

عند التعامل مع أسماء نطاقات أو عناوين بروتوكول إنترنت ضارة محتملة، لا تريد أن ينقر عليها شخص ما عن طريق الخطأ. (لاحظ أنه في كثير من الأحيان يتم تحويلها تلقائيًا إلى أسماء) كما لا تريد أن تقوم برامج الأمان بمسح السياق الذي تتم فيه مشاركة الآثار (على سبيل المثال، منتج أمان البريد الإلكتروني) كي لا تقوم بكشف أنها ضارة وإرسال تنبيه.

لذلك يُعتبر من الممارسات الجيدة **إزالة الضرر** من النطاقات وعناوين بروتوكول الإنترنت عن طريق وضع أقواس مربعة حول جميع النقاط أو على الأقل الأخيرة، ومن الناحية العملية يكفي على الأغلب وضعها حول النقطة الأخيرة ولهذا السبب قمنا بتطبيق ذلك في هذا الدليل. لذلك بدلًا من `internews.org` نكتب `internews[.]org` وبدلًا من `127.0.0.1` ، نكتب `127.0.0[.]1`.

تُعدّ الآثار الموجودة في الفقرة السابقة والعديد من تلك الموجودة في هذا الدليل ليست خبيثة وبالتالي يمكن إزالة الأقواس المربعة، ولكن من الممارسات الشائعة أن تقوم ببساطة بتطبيق ذلك عليها.

ستقوم العديد من الأدوات والخدمات (حيث يمكنك إدخال النطاقات وعناوين بروتوكول إنترنت بما فيها فايروس توتال) بإزالة الأقواس المربعة تلقائيًا، لذلك لا يتعين عليك القيام بذلك قبل البحث عن شيء ما.

السؤال 7.1. لماذا لا تحتاج إلى إزالة الضرر من أسماء الملفات؟ (انظر الملحق للحصول على الإجابة.)

شفرات التجزئة

دالة التجزئة المشفرة هي خوارزمية رياضية تأخذ بيانات ذات حجم عشوائي (على سبيل المثال، كلمة مرور أو محتويات ملف) وتحولها إلى عدد ثابت من البايتات: **"قيمة التجزئة"** أو **"شفرة التجزئة"** فقط. وعندما التعامل مع عينات البرمجيات الضارة تعتبر شفرات التجزئة مريحة للغاية لأسباب عديدة.

أولها الأمان: حيث لا تريد مشاركة البرمجيات الضارة بطريقة يمكن أن تتسبب بتشغيلها عن طريق الخطأ ويمكن أن تتسبب بضرر، وتُعدّ مشاركة شفرة تجزئة أكثر أمانًا.

والأمر الثاني هو الحجم: حيث تُعدّ شفرة التجزئة صغيرة وبالتالي يمكنك مشاركتها في رسالة بريد إلكتروني أو رسالة سيغنال (Signal) أو على وسائل التواصل الاجتماعي دون الحاجة إلى إرفاق الملف الأصلي.

يتمثل السبب الثالث في أن شفرة التجزئة هي بمثابة "بصمة" عينة مما يجعل من السهل العثور على نسخ أخرى في مجموعة من عينات البرمجيات الضارة، وبالتالي يمكن أن يكون هذا مفيدًا جدًا. في بعض الأحيان، لا تريد أن تكشف للعلن المزيد من المعلومات حول العينة أكثر مما مكشوفا بالفعل. عندما تقول أنك رأيت مرفق بريد إلكتروني ضار يضم شفرة تجزئة معينة، يمكن للأشخاص التحقق من مجموعة المرفقات أو مستودعات عينات البرمجيات الضارة مثل فايروس توتال ومعرفة ما إذا كانوا قد شاهدوا نفس الملف.

عندما يرسل ممثل ضار العديد من ملفات البرمجيات الضارة في حملة ما يكون من السهل عليه تعديل كل منها بطريقة صغيرة بحيث تكون التجزئة مختلفة تمامًا، ولكن في الممارسة العملية لا يفعلون ذلك في كثير من الأحيان ولذلك لا تزال شفرة التجزئة طريقة جيدة لمساعدة الناس على تحديد أنهم يرون ملفات البرمجيات الضارة ذاتها في حملة من الهجمات.

من المهم ملاحظة أن اسم الملف ليس جزءًا من البيانات المجزأة ولذلك إذا قمت بإعادة تسمية ملف فلن تتغير شفرة التجزئة، ولكن إذا قمت بتغيير بايت واحد في ملف فستتغير.

تتمتع شفرات التجزئة بالخصائص التالية:

- يمكن حساب شفرة التجزئة بسرعة حتى بالنسبةللمدخلات الكبيرةجدًا.
- بالنظر إلى قيمة شفرة التجزئة من المستحيل عمليًا حساب البيانات الأصلية.
- بالنظر إلى بعض البيانات التي تسمح لك بحساب قيمة شفرة التجزئة، من المستحيل عمليًا العثور على بيانات أخرى تتمتع بقيمة شفرة التجزئة ذاتها.
- تؤدي حتى أصغر التغييرات في البيانات إلى توليد قيمة شفرة تجزئة مختلفة تمامًا.

كما توجد أنواع شفرات تجزئة أخرى تؤدي دورًا في التحليل الذكي للتهديدات لا تشترك بهذه الخاصية الأخيرة، وتسمى شفرات تجزئة قريبة، ومن الأمثلة عليها SSDEEP على فايروس توتال التي هي مثال على "تجزئة قريبة".

في الممارسة العملية، هناك ثلاث دالات شفرات تجزئة ذات صلة هي: md5 وsha1 وsha256. الدالتان الأولى والثانية هما أقدم وليستا مثاليتين ومن غير المرجح أن يؤثرا على عملك، ولكن عند اختيار دالة تجزئة يوصى باختيار sha256.

تتكون شفرة تجزئة sha256 من 32 بايت (أو 256 بت ومن هنا جاء اسمها) وتكتب بشكل 64 حرفًا باستخدام الأرقام من 0 إلى 9 والحروف من a إلى f، وبسبب الخصائص المذكورة أعلاه، لا أهمية لأحرف شفرة التجزئة بحد ذاتها لأنها مجرد سلسلة من الحروف في بحثك.

السؤال 7.2. لا يمكنك أن "تعكس هندسة" شفرة التجزئة كي تصل إلى البيانات الأصلية بحكم الخاصية الثانية أعلاه، لكن إذا وجدت شفرة تجزئة وليس لديك أي فكرة عنها فيمكنك دائمًا تجربة حظك باستخدام محرك بحث. ما هي البيانات الأصلية التي نتجت عنها شفرة التجزئة التالية؟

```
md5:d41d8cd98f00b204e9800998ecf8427e
sha1:da39a3ee5e6b4b0d3255bfef95601890afd80709
sha256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

(تستخدم النقطتان بشكل شائع للإشارة إلى نوع شفرة التجزئة، ولكن كما يتضح لشفرات التجزئة الثلاث أيضًا أطوال مختلفة.)

التمرين 7.3 في نسخة ريمنوكس لديك قم بإنشاء ملف نصي وأدخل نص "`hello world`" (دون علامات اقتباس أو فاصل أسطر) واحفظ الملف بتسميته `test.txt`.

1 ثم استخدم أمر `sha256sum` لحساب شفرة تجزئة sha256 للملف، ودوّن قيمة شفرة التجزئة.

استخدم `md5sum` و`sha1sum` لحساب شفرات تجزئة md5 وsha1 أيضًا.

2 الآن أعد تسمية الملف إلى `newtest.txt` باستخدام الأمر `mv` ، ثم قم بحساب شفرة تجزئة sha256 للملف الجديد وتأكد أنها مماثلة.

3 الآن افتح الملف الجديد للتحرير، وحول "h" إلى "H" (حرف صغير إلى كبير)، ثم احفظه واحسب شفرة تجزئة sha256 الجديدة وتأكد من أنه مختلف ولا علاقة له بشفرة التجزئة الأصلية.

4 انتقل إلى مالوير بازار (Malware Bazaar) وتأكد من القيام بذلك في متصفح داخل ريمنوكس، ثم ابحث عن قاعدة بيانات البرمجيات الضارة الخاصة فيه وانقر على أي ملف. قم بتنزيل العينة وفك حزمها (تذكر أنه من الشائع وضع البرمجيات الضارة في ملف مضغوط محمي بكلمة مرور هي "infected").

عادةً ما يمكن فك حزم الملفات المضغوطة باستخدام أمر unzip ولكن قد تواجه خطأ، وفي حال حصل ذلك ثبّت أمر 7z عن طريق تشغيل

```
sudo apt-get install p7zip-full،
```

وثم قم بفك حزم الملف عن طريق تشغيل

```
[7z x [file
```

ثم احسب شفرة تجزئة sha256 لعينة البرمجيات الضارة.

إذا اتبعت الخطوات بشكل صحيح فستلاحظ أن شفرة التجزئة نفسها اسم الملف. وهذا أمر شائع جدًا في قواعد بيانات البرمجيات الضارة.

استخدام فايروس توتال

بعد الاطلاع على هذه المعلومات الأساسية دعونا نلقي نظرة على فايروس توتال حيث يمكننا مقارنة النطاقات وعناوين بروتوكول إنترنت وعناوين مواقع الويب من ملفاتك مع تلك التي تم تحميلها من قبل محللي التهديدات في جميع أنحاء العالم.

قبل استخدام فايروس توتال يجب أن تفهم كيفية عمل الموقع، حيث إن وظائفه الرئيسية مجانية ولا تتطلب التسجيل حتى. وسيسمح لك إنشاء حساب مجاني ببعض الخيارات الإضافية لكننا لن نستخدمها في هذا الدليل.

يوفر فايروس توتال أيضًا حسابات مدفوعة، مما يسهل البحث في مجموعة ملفاته الضخمة عن خصائص معينة مثل الاسم وتنزيل الملفات، وتأتي أهمية هذا الأمر من افتراض أن المتطفلين، وبالأخص الأكثر مكرًا بينهم، يملكون حسابات مدفوعة ويستخدمونها للبحث عن الملفات ذات الصلة بأهدافهم. لذا كن حذرًا بشأن تحميل الملفات إلى فايروس توتال: وقم فقط بتحميل الملفات التي تشعر بالراحة حيال نشرها علنًا.

عمليات التحقق من الملفات وتحميلها

هناك سببان وراء رغبتك في تحميل ملف: أولهما هو التحقق من سياقه ومعرفة المزيد عنه مثل ما إذا كان خبيثًا، والنطاقات التي تتصل بها عند تشغيلها وما إلى ذلك؟

والثاني هو مشاركتها مع مجال الأمن، حيث إن معظم شركات الأمن عملاء لدى فايروس توتال ويعد تحميل ملف طريقة بسيطة لمشاركة الملف معهم جميعًا. ويمكن أن يساعدهم ذلك في اكتشاف الهجوم المحدد الذي تواجهه ومنعه من التأثير على الآخرين.

تجدر الإشارة هنا إلى أن معظم شركات الأمن ترى ملايين عينات البرمجيات الضارة يوميًا ومعظم عمليات المسح وإضافة الكشف تحدث تلقائيًا بالكامل، وهو أمر لا بأس به في كثير من الأحيان ولكن إذا كنت تريد منهم إيلاء اهتمام وثيق بالملف لسبب ما فتأكد من التواصل معهم مباشرة.

عند التحقق من ملف على فايروس توتال، اتبع الخطوات الأربع التالية:

1. احسب شفرة تجزئة sha256 للملف كما هو موضح أعلاه، وتحقق منها على فايروس توتال. وفي حال كانت موجودة، ستعلم أن الملف قد سبق تحميله بالفعل.
2. أما في حال لم تعثر عليه عليك أن تقرر ما إذا كنت تريد تحميل الملف، فحتى لو كان الملف ضارًا قد يكون قد تم تصميمه خصيصًا للهدف وبالتالي يشمل على بعض المعلومات الشخصية. في حالة كان الملف مستهدف سيؤدي تحميله إلى فايروس توتال إلى الكشف عن حقيقة أنه تم فتحه ويجري تحليله، ولا بأس أيضًا أن تقرر عدم تحميل الملف لأنك لست متأكدًا.

3. إذا كنت ترغب في تحميله ففكر فيما إذا كان اسم الملف شيئًا ترغب في مشاركته، وفي حال لم ترغب بذلك أو إذا لم تكن متأكدًا، أعد تسمية الملف ليصبح `[sha256].[extension]`: وأبق الملحق الأصلي مثل (.exe، .docx وما إلى ذلك) ولكن أعد تسمية الجزء قبل النقطة إلى شفرة تجزئة sha256. هذه ممارسة جيدة (رأينا ذلك مع مالوير بازار أعلاه) ولكن لا يدل على أي شيء عن الملف.
4. قم بتحميل الملف باستخدام واجهة الويب الخاصة بفايروس توتال، وتأكد من تحميل الملف نفسه فقط وليس مجلدًا كاملًا أو ملفًا مضغوطًا يحتوي عليه.

علامة تبويب الكشف

في الأقسام التالية سنستخدم العينة 971c5b5396ee37827635badea90d26d395b08d17cbe9e8027dc87b120f8bc0a2[21]، وهو ملف .exe ضار يستخدم في الهجمات المستهدفة من قبل جهة تهديد مرتبطة بإيران تسمى إيه ب تي 42 (APT42). سبقت الإشارة إليها في تقرير ماشن من قبل شركة الأمن مانديانت (Mandiant) (التي تملكها الآن شركة غوغل (Google)).

تُظهر فايروس توتال عنوانًا يحتوي على العديد من "علامات التبويب" أسفله، ويتضمن العنوان شفرة تجزئة sha256 وحجم الملف ومتى تم تحليله آخر مرة.

في الأسفل، تسمى علامة التبويب الأولى "الكشف"، وتعرض نتائج المسح من العشرات من محركات مكافحة الفيروسات. ويستخدم محرك الكلمات عمدًا هنا حيث عادة ما ينظر هذا الجزء من المنتج فقط إلى الملف نفسه بدلًا إلى ما يفعله.

لاحظ أن معدلات الكشف المنخفضة شائعة جدًا، وبالأخص للملفات الجديدة ويجب أيضًا مراعاة أن عدد عمليات الكشف مؤشر حول مدى معرفة مجتمع الأمان بالملف وليس مدى نجاح منتج معين في إيقاف التهديد في موقف حقيقي.[22]

تعني النتائج الإيجابية الخاطئة الملفات غير الضارة أو السليمة التي دل اكتشاف على أنها برمجيات ضارة بشكل غير صحيح وهو أمر يحدث ولكنه نادر. وفي الممارسة العملية أي شيء يتجاوز عدة اكتشافات يشير إلى أن الملف ضار.

نصيحة: إذا كان الملف قد تم مسحه آخر مرة منذ بعض الوقت فيمكنك النقر فوق السهم المنحني في الزاوية العلوية اليسرى لمسح الملف مرة أخرى وعادة ما يتحسّن الكشف بمرور الوقت، مما يمنحك صورة أكثر دقة.

[21] مثال على الإشارة إلى ملف من خلال شفرة تجزئته.

[22] يرجع سبب هذا إلى استخدام فايروس توتال محرك ملفات مبسّط وليس كامل المنتج. يمكنك مقارنة ذلك بحارس أمن لم يكن ليتعرف على لص بناءً على مظهره ولكن كان من الممكن أن يمنعه من سرقة شيء ما بالفعل.

أخيرًا هناك أمران يتعلقان بالمحركات، حيث بعضها في الواقع هو نفسه (على سبيل المثال، استحوذت شركة أفاست على إيه في جي (AVG) منذ بعض الوقت وكانت المنتجات هي نفسها منذ فترة طويلة) وتدرج بشكل منفصل فقط لأن العلامات التجارية لا تزال موجودة. ويمكن عادة تجاهل أسماء الكشف: فهي غالبًا ما تكون عامة وعندما لا تكون عامة عادة ما تكون خاطئة.

وثانيًا لاحظ أنه إذا قمت بتسجيل الدخول إلى فايروس توتال فسترى بعض قواعد الكشف مدرجة فوق نتائج مكافحة الفيروسات، وهذه قواعد كشف أخرى وعلى عكس أسماء الكشف عن الفيروسات يمكن أن تكون مفيدة في فهم نوع البرمجيات الضارة هذه.

علامة تبويب التفاصيل

تعرض علامة التبويب تفاصيل معلومات أكبر حول ملف، مثل شفرات التجزئة المختلفة: sha256 وmd5 وما إلى ذلك. ملفنا هو ملف قابل للتنفيذ على ويندوز (Windows) (سترى نوع الملف مدرجًا)، وبالنسبة لأنواع الملفات الأخرى، تختلف المعلومات هنا، فعلى سبيل المثال بالنسبة لملفات آندرويد (Android) تُعرض الأذونات المطلوبة وهو أمر يمكن أن يكون مفيدًا للغاية.

تُخبرك علامة تبويب "التفاصيل" بموعد إرسال شفرة التجزئة لأول مرة إلى فايروس توتال وهو مؤشر جيد، وتخبرك بموعد إنشاء الملف ومتى شوهد لأول مرة ولكن ليست هذه التفاصيل دقيقة بشكل خاص لذلك لا توليها الكثير من الاهتمام.

ستلاحظ أيضًا أسماء مختلفة تم بموجبها إرسال الملفات، وفي بعض الأحيان يساعدك هذا على فهم كيفية استخدام الملف كما هو موضح في التمرين التالي.

السؤال 7.4. يتلقى الشخص الذي تدعمه ملفًا ضارًا يسمى `tax_information.docx` ، وتشتبه في أن أحد المتطفلين يستهدفه على وجه التحديد بحملة تم تصميمها لتبدو وكأنها من مكتب الضرائب المحلي. في فايروس توتال، ستجد أن الملف نفسه قد تم إرساله أيضًا باسمي package_receipt.docx وbirthday_gift.docx. كيف يمكن أن تساعدك هذه المعلومات؟ (انظر الملحق للعثور على الإجابة.)

علامة تبويب "العلاقات"

تعرض علامة تبويب "العلاقات" الصلة بين الملف الذي قمت بتحميله ومؤشرات الاختراق الأخرى في فايروس توتال، مثل عناوين مواقع الويب والنطاقات وعناوين بروتوكول إنترنت التي تم الاتصال بها عند تشغيل الملف في بيئة اختبار معزولة (سنتحدث عن ذلك بتفصيل أكبر في فصل لاحق) بالإضافة إلى الملفات التي تم تنزيلها من الإنترنت أو إنشاؤها مباشرة عند تنفيذ الملف.

يمكنك النقر على هذه الكائنات لمعرفة المزيد عنها وربما العثور على روابط تهديدات أخرى وهذا ما يسمى تتبع المحور، وسنناقش هذا لاحقًا في الدليل.

التمرين 7.5 يبرز نطاق `update-driversonline[.]bid` بين تلك المرتبطة بهذا الملف (ما زلنا نتحدث عن 971c5b5396ee37827635badea90d26d395b08d17cbe9e8027dc87b120f8bc0a2). هناك العديد من الأسباب للشك بأنه خبيث وبعض الأسباب للاعتقاد بأنه ليس خبيثًا، فما هي الأسباب التي تعرفها؟

يمكن أن تحتوي علامة التبويب "العلاقات" أيضًا على سياقات أخرى، مثل عناوين مواقع الويب التي تم تنزيل هذا الملف منها أو الأرشيفات (مثل zip) التي تحتويها، ويمكن أن تكون جميع هذه المعلومات مفيدة في فهم التهديد.

علامات تبويب السلوك والمجتمع

تناقش علامة تبويب "السلوك" ما يفعله الملف، وبالنسبة إلى الملف التنفيذي لويندوز يمكن أن يكون هذا مفيدًا حقًا. ولكن بالنسبة لمحلل مبتدئ يمكن أن تكون المعلومات هنا مربكة للغاية. دون أي إدراك إضافي لما تفعله الملفات (التي يمكنك على سبيل المثال أن تستخدم بيئة اختبار معزولة لاختبارها وهو أمر ستتم تغطيته في الفصل 10)، عليك أن تحذر من استخلاص الاستنتاجات بناءً على علامة التبويب هذه فقط.

تحتوي علامة تبويب "المجتمع" على تعليقات حول الملف، حيث تكون العديد من التعليقات مولدة تلقائيًا وتظهر المزيد من نتائج بيئة الاختبار المعزولة. تضاف بعض التعليقات من قبل البشر وهي مفيدة جدًا، وإذا كنت ترغب بذلك يمكنك إنشاء حساب مجاني على فايروس توتال وعرض سياق الملف وربما حتى إضافة اقتراح أن يتصل بك شخص ما في حال كان يعرف المزيد عنه. ولكن في هذه الحالة يجب أن تراعي أنه متاح للعامة بما في ذلك المتطفلين، لذلك لا تقم بإضافة أي شيء يمكن ربطه بك بصفتك شخصًا إذا كنت تعتبر أنه من غير الآمن القيام بذلك.

أنواع الملفات الأخرى

يمكن لفايروس توتال التعامل مع العديد من أنواع الملفات المختلفة، ويمكن أن تختلف علامات التبويب ومحتواها إلى حد ما اعتمادًا على نوع الملف.

تحقق من علامات تبويب فايروس توتال لأجل الأمثلة الثلاثة التالية وأمض بضع دقائق كي تتعرفعليها:

مستند وورد (Word) ضار: 2382d4957569aed12896aa8ca2cc9d2698217e53c9ab5d52799e4ea0920aa9b9

ملف حزمة أندرويد (APK): 86acaac2a95d0b7ebf60e56bca3ce400ef2f9080dbc463d6b408314c265cb523

ملف ماك أو إس (macOS) قابل للتنفيذ: 483b2f45a06516439b1dbfedda52f135a4ccdeafd91192e64250305644e5ff48

السؤال 7.6. في الأمثلة أعلاه، ابحث في علامات التبويب وحاول الإجابة على الأسئلة التالية:

1. هل يتصل مستند وورد بأي نطاقات مشبوهة؟ إذا لم يكن يحاول ذلك، فهل هناك أي اتصالات مشبوهة بطرق أخرى؟
2. هل يطلب ملف آندرويد إذن الاستماع إلى الميكروفون؟
3. دون استخدام محرك بحث آخر غير فايروس توتال، هل يمكنك العثور على تقرير حول الملف التنفيذي لنظام ماك أو إس؟ (انظر الملحق للعثور على الإجابة.)

أسماء المضيفين والنطاقات

الآن ابحث على فايروس توتال عن نطاق `update-driversonline[.]bid` الذي رأيناه في عينتنا الأصلية، ويمكنك أيضًا الانتقال إلى تلك العينة على فايروس توتال والنقر على ذلك الرابط في علامة التبويب "العلاقات".

سترى أن فايروس توتال يشمل أيضًا الكثير من المعلومات حول أسماء النطاقات، وتبدو علامة تبويب "الكشف" مألوفة. لكن اكتشاف النطاقات أقل صعوبة من اكتشاف الملفات، ولا يوجد دائمًا تمييز واضح بين النطاقات "الجيدة" و"السيئة" (تذكر أنواع النطاقات الأربعة التي ناقشناها في هذا

الفصل في القسم الخاص بالمفاهيم المهمة للتحليل الذكي للتهديدات)، ولكن ينطبق المبدأ ذاته هنا أيضًا فكلما زاد اكتشافات أنها ضارة كلما زاد احتمال أن تكون ضارة بالفعل.

تحتوي علامة تبويب "التفاصيل" على مزيد من المعلومات حول النطاق، بما في ذلك معلومات هو إز (whois) والتي تخبرك متى تم تسجيله وأحيانًا من قام بتسجيله. سترى أن علاماتي تبويب المجتمع والعلاقات مألوفة والثانية مفيدة بشكل خاص، ويمكنك استخدامها لتتبع المحور وأيضًا العثور على نطاقات فرعية.

السؤال 7.7. اتصل بالنطاق ثلاث ملفات من بينها عينتنا الأصلية. هل تعتقد أن الملفات الثلاثة مرتبطة؟ لماذا تعتقد ذلك؟ (انظر الملحق للعثور على الإجابة.)

عناوين بروتوكول الإنترنت

يشمل فايروس توتال أيضًا على معلومات حول عناوين بروتوكول إنترنت، وتعد علامة تبويب "العلاقات" هنا مفيدة للغاية فهي تُظهر أن سجل نطاقات A يُشير إلى عنوان بروتوكول إنترنت. ويمكن أن يكون هذا مفيدًا حقًا عند محاولة العثور على نطاقات أخرى مرتبطة بنطاق معين.

السؤال 7.8. استخدم إدخال فايروس توتال للعنوان `update-driversonline[.]bid` وألق نظرة على عناوين بروتوكول إنترنت ذات الصلة. هل يمكنك العثور على نطاقات أخرى تعتقد أنها استخدمت في نفس الحملة؟ (انظر الملحق للعثور على الإجابة.)

عناوين مواقع الويب

أخيرًا يحتوي فايروس توتال أيضًا على صفحات على عناوين مواقع الويب لكنها نادرًا ما تضيف الكثير إلى ما يظهر في صفحات النطاق أو اسم المضيف المقابلة، ونظرًا لأن عناوين مواقع الويب غالبًا ما تكون فريدة من نوعها فإن إضافتها إلى فايروس توتال يمكن أن يوفر معلومات للخصم حول قيامك بتحليلها، وبالتالي من الأفضل البحث عن اسم المضيف فقط.

دائمًا ما يكون التحقق من اسم المضيف أو اسم النطاق أمرًا مستحسنًا، حيث يقوم فايروس توتال بمسح أسماء النطاقات بنشاط لذلك لا داعي للقلق بشأن "تحميل" نطاق جديد. الحالة الوحيدة التي قد ترغب فيها في توخي الحذر بعض الشيء هي إذا كان لديك اسم مضيف محدد للغاية، مثل `long].domain` والذي قد يكون فريدًا لهذا الهدف المحدد، رغم أن هذا أمر نادر الحدوث.

تتبع التهديدات

يُعدُّ تتبع التهديدات نشاطًا استباقيًا حيث تقوم بتتبع التهديدات بدلًا من تحليل التهديدات الموجودة، وفي بعض الأحيان يتضمن تتبع التهديدات البحث عن تهديدات تستهدف منظمة أو مجتمعًا معينًا دون أي تركيز محدد، على سبيل المثال، من خلال البحث عن نطاقات مسجلة حديثًا تستخدم اسم مؤسستك مما قد يعني أن الجهة الفاعلة في التهديد تسجلها لاستخدامها في حملة تصيد احتيالي.

في كثير من الأحيان، ينطلق تتبع التهديدات من تهديد موجود مثل ملف ضار، ثم البحث عن الأدوات ذات الصلة (ملفات أخرى أو نطاقات وما إلى ذلك) كي تحصل على صورة أفضل للتهديد والفاعل الذي يقف وراءه.

تُعدّ فايروس توتال أداة رائعة لتتبع التهديدات، وفي القسم السابق قمنا بذلك قليلًا من خلال البحث عن الملفات والنطاقات ذات الصلة، وتُعدّ حسابات فايروس توتال المدفوعة رائعة حقًا في تحقيق هذا الغرض لأنها تفتح المزيد

من الإمكانيات لتتبع التهديدات. ويمكنك تتبع المحور للتحقيق في المؤشرات الإضافية التي تجدها وأيضًا استخدام قواعد "YARA "، وهي طريقة للبحث عن الملفات في مجموعة كبيرة مفيدة بشكل خاص عند البحث عن البرمجيات الضارة ذات الصلة.

قد يفاجئك مقدار ما يمكنك تحقيقه باستخدام أدوات مجانية عبر الإنترنت دون معرفة كيفية عكس هندسة البرمجيات الضارة[23] أو كيفية كتابة قواعد YARA، ولكن هناك تحذيران مهمان:

الأول هو أن نكون حذرين من الاستنتاجات الجريئة، حيث من الخادع أن تشعر بالحماس [24] عند ربط بعض البرمجيات الضارة بممثل معروف خاصة عندما يكون ممثلًا متقدمًا مرتبطًا ببعض الحكومات، وفي بعض الأحيان تكون هذه الروابط موجودة بالفعل وفي كثير من الأحيان لا تكون موجودة. على سبيل المثال، قد يكون لدى كلا الفاعلين بنية تحتية مشتركة مع طرف ثالث أو كانت هناك محاولة متعمدة لتضليل الباحثين. والاحتمال الآخر هو أن النطاقات التي يستخدمها كلا التهديدين انتهت بالتوجيه إلى حفرة إعادة توجيه (سنتحدث عن حفرة إعادة التوجيه فيما يلي).

أما التحذير الثاني هو عدم نسيان هدف تحقيقك، فليس عليك البحث عن تهديدات مماثلة لكل تهديد تحقق فيه، حيث إذا لم يقم الشخص الذي أبلغ عن الحدث بفتح المرفق الضار أو لم يكن المرفق يستهدفه أو يستهدف منظمته على وجه التحديد، فلا بأس من إغلاق التحقيق والتركيز على أشياء أخرى.

التهديدات المستهدفة وغير المستهدفة

تُقسّم التهديدات الرقمية مثل البرمجيات الضارة والتصيد الاحتيالي تقليديًا إلى تهديدات مستهدفة وغير مستهدفة. حيث في السيناريو الأول يستهدف التهديد مستخدمًا فرديًا أو منظمة فردية أو ربما عددًا صغيرًا جدًا منهم، أما في السيناريو الثاني من الممكن أن يتلقى أي مستخدم التهديد وتأمل الجهات الفاعلة المسؤولة عنه أن يقع ذلك المستخدم ضحية له.

يكمن التحدي في حقيقة أنه من الناحية العملية لا تزال العديد من التهديدات غير المستهدفة تبدو مستهدفة إلى حد ما، لأنه أولًا من الشائع جدًا أن تستهدف حملة غير مستهدفة بلدًا أو منطقة معينة فقط مما يسمح للفاعل المسؤول عنها بكتابة الرسائل باللغة المحلية وإضافة السياق المحلي الذي يجعل من الأسهل تصديقها.

ثانيًا غالبًا ما يستخدم الممثل الضار البيانات من العديد من حسابات البريد الإلكتروني المخترقة عند إرسال رسائل بريد إلكتروني ضارة، وبهذه الطريقة يمكنهم جعل رسالة البريد الإلكتروني تبدو وكأنها رد على شيء أرسلته سابقًا أو كأنها جاءت من إحدى جهات الاتصال لديك. من شأن ذلك أن يجعل البريد الإلكتروني يبدو مستهدفًا للغاية حتى عندما لا يكون كذلك فالجهات الفاعلة قادرة على إرسال عدد كبير من رسائل البريد الإلكتروني تلقائيًا مع إمكانية أن تبدو كل منها مخصصة تمامًا للمستلم.

وأخيرًا وجدت الجهات الفاعلة في مجال التهديد، لا سيما تلك التي تشارك في الجرائم الإلكترونية مزيجًا بين التهديدات المستهدفة وغير المستهدفة حيث يؤدي التهديد غير المستهدف إلى حساب مخترق غالبًا داخل مؤسسة كبيرة. ثم يتم بيع الوصول إلى هذا الحساب إلى جهة فاعلة أخرى التي تستخدم الوصول بطريقة أكثر استهدافًا، على سبيل المثال عن طريق نشر برمجية الفدية في جميع أنحاء الشبكة، وبالرغم من أن التهديد الثاني كان مستهدفًا للغاية إلا أن التهديد الأصلي لم يكن مستهدفًا.

تُعدّ الغالبية العظمى من التهديدات الرقمية غير مستهدفة وهذا صحيح حتى بالنسبة للتهديدات ضد أولئك الذين يواجهون أيضًا تهديدات مستهدفة للغاية.

[23] الهندسة العكسية هي عملية تشمل التعرف على ما يفعله برنامج ما في الغالب ما يكون برمجية ضارة، بالاستناد إلى الرمز المكون من وحدات البايت **المجمّع**.

[24] لا بأس بأن تتحمس لهذه الأمور حتى لو كانت التهديدات خطيرة وتؤثر على أشخاص حقيقيين بطرق خطيرة في كثير من الأحيان،
لكن لا تدع رغبتك في مساعدة الناس والمجموعات تكون مدفوعة بالتهديدات التي تثيرك أكثر لأن الغالبية العظمى من التهديدات عادية جدًا.

السؤال 7.9. يخاطب البريد الإلكتروني الذي يحتوي على مرفق ضار المستلم وهو موظف في إحدى منظمات المجتمع المدني باستخدام اسمه واسم عائلته ويظهر وكأنه من موظف آخر في المنظمة. هل يمكنك تحديد سبب لكون هذا تهديدًا آليًا وغير مستهدف؟ (انظر الملحق للعثور على الإجابة.)

حفرة إعادة التوجيه

يتحكم في معظم البرمجيات الضارة خادم أو مجموعة من الخوادم يتحكم بها ممثل التهديد، ويسمى هذا الخادم أو مجموعة الخوادم بمجموعة القيادة والتحكم (يشار إليها غالبًا باسم C&C أو C2 بالإنجليزية). حيث تتطلب معظم البرمجيات الضارة اتصالًا بالإنترنت حتى تتمكن من تلقي الطلبات من مجموعة القيادة والتحكم. تُخبر البرمجيات الضارة جهازك بالاتصال بنطاق واحد أو أكثر يشير إلى عنوان بروتوكول إنترنت لخادم القيادة والتحكم، وتسمح الإشارة إلى نطاق بدلًا من عنوان بروتوكول إنترنت للجهات الفاعلة بالتبديل إلى خادم مختلف إذا أصبح الخادم الأصلي غير متاح لها.

لإيقاف عملية القيادة والتحكم والبرمجيات الضارة التي تتحكم بها، قد تعرض وكالة إنفاذ القانون أو شركة أمان دليلًا لمسجل النطاق يؤكد أن النطاق قد تم استخدامه لأغراض ضارة وإقناع المسجل بالسماح لهم بالاستحواذ على النطاق. قد يقومون بعد ذلك بتوجيه النطاق إلى خادم يتحكمون فيه (غالبًا ما يسمى ذلك **"بإعادة توجيه النطاق إلى حفرة"**)، ويعني ذلك أنه في كل مرة تحاول فيها البرمجية الضارة الاتصال بخادم القيادة والتحكم خاصتها تتصل بدلًا من ذلك بنطاق حفرة إعادة التوجيه مما يمنح المشغلين معلومات متعمّقة حول التهديد. وفي بعض الأحيان يمكن لوكالة أو شركة إنفاذ القانون بعد ذلك إرسال أوامر لتحييد البرمجيات الضارة إذا طورت فهمًا كافيًا لكيفية عمل القيادة والتحكم فيها.

تستخدم بعض البرمجيات الضارة خوارزمية توليد النطاق لإنشاء نطاقات جديدة على أساس يومي على الأرجح، وتجعل خطوة التمويه هذه من الصعب على المحلل تحديد أن العديد من عينات البرمجيات الضارة تشير إلى خادم القيادة والتحكم ذاته لأنه لا يستطيع العثور بسهولة على نطاقات تعرّف الهوية. تقوم الجهات الفاعلة في مجال البرمجيات الضارة بتسجيل هذه النطاقات الجديدة طوال استمرار حملتها ولا داعي للقلق كثيرًا بشأن عمليات الاستحواذ على النطاق أو حظر النطاق من قبل منتجات الأمان. في كثير من الحالات، يمكن "فك شفرة" خوارزمية توليد النطاق مما يسمح للباحثين بالتنبؤ بالنطاقات التي سيتم استخدامها وتسجيلها بشكل استباقي وتوجيهها إلى حفرة إعادة التوجيه.

عند التحقيق في نطاق خبيث، من المهم أن تراعي أن النطاق الذي تراه قد تم توجيهه إلى حفرة إعادة التوجيه. كما يجب مراعاة أنه لا توجد قائمة عامة بعناوين بروتوكول إنترنت حفر إعادة التوجيه، وإذا كانت موجودة سيقوم مؤلفو البرمجيات الضارة ببساطة بإيقاف اتصال البرمجيات الضارة بأي عنوان بروتوكول إنترنت في تلك القائمة، وليس من الواضح دائمًا متى يكون عنوان بروتوكول إنترنت هو حفرة إعادة توجيه فعلية. غالبًا ما يمكن أن يكون وجود العديد من النطاقات من حملات تبدو غير ذات صلة ولكن تشير إلى عنوان بروتوكول إنترنت ذاته وذلك دليل كبير على أنه حفرة إعادة التوجيه، وفي حالة الشك يمكنك إدخال عنوان بروتوكول الإنترنت في محرك بحث أو تحقق من علامة التبويب "المجتمع" في فايروس توتال أو يمكنك أن تسأل.

السؤال 7.10. يُعد استخدام حفرة إعادة التوجيه لإرسال الأوامر لتحييد عدوى البرمجيات الضارة أمرًا مثيرًا للجدل إلى حد ما. هل يمكنك التفكير بأسباب ذلك؟ (انظر الملحق للعثور على الإجابة.)

أدوات أخرى

تُعدُّ فايروس توتال هي أداة رائعة لتحليل التهديدات والتتبع ولكنها ليست الوحيدة. لعل أكثر الأدوات فائدة للجميع هي محركات البحث، وسواء كنت تفضل غوغل أم أحد البدائل الرائعة العديدة فقد يفاجئك مقدار ما يمكنك العثور عليه غالبًا من خلال البحث عن اسم نطاق أو عنوان بروتوكول إنترنت أو شفرة تجزئة ملف أو أي أثر أخرى.

ينطبق الشيء نفسه على وسائل التواصل الاجتماعي ولا سيما تويتر (Twitter)، على الرغم من أنه في وقت كتابة هذا التقرير (أوائل ديسمبر/كانون الأول 2022)، غادر العديد من الباحثين الأمنيين تويتر وانتقلوا إلى ماستودون (Mastodon). كانت مشاركة مؤشرات الاختراق شائعة جدًا على تويتر وقد تصبح شائعة على ماستودون. وتتمثل الميزة الكبيرة للعثور مؤشر اختراق على وسائل التواصل الاجتماعي في أنه يمكنك الرد على الشخص الذي نشرها وطرح الأسئلة أو إضافة تعليقاتك الخاصة.