تحليل المستندات الضارة -- الجزء 04 -- التدابير الدفاعية والخطوات التالية والختام

حتى الآن، غطينا مقدمة لنمذجة التهديدات واستخدام الأجهزة الافتراضية كبيئات لتحليل البرمجيات الضارة، وكيفية البدء في تحليل ملفات بي دي إف (PDF) ومايكروسوفت أوفيس في الأجزاء السابقة، وستساعدنا كل هذه المواضيع على تقديم دعم أفضل للآخرين كخط الدفاع الأول ضد المستندات المشبوهة.

لكن إذا دعمنا الجهات الفاعلة المعرضة للخطر، أي الجمهور المستهدف الأساسي لسلسلة المنشورات هذه فإننا نعلم أن هذا ليس سوى نصف القصة، وعلينا أيضًا التأكد من قدرتنا على تقديم مشورة استباقية جيدة للمستفيدين لدينا حتى نحافظ على حمايتهم جيدًا ضد المستندات الضارة قبل وصولها إلى أوساط تخزينهم. نأمل أنه ومع كل المحتوى الذي راجعناه ألا نتمكن فقط من فهم النصائح الكلاسيكية التي نقدمها للمستخدمين النهائيين بشكل أفضل وإنما أيضًا أن نقترح أيضًا تدبيرين إضافيين يمكن أن يكونا مفيدة للجهات الفاعلة المعرضة لخطر متزايد.

يعد الهدف الأول الذي نريد التركيز عليها هي أن إخبار النشطاء والصحفيين ووسائل الإعلام بأنه لا ينبغي عليهم فتح ملفات من مصادر غير معروفة **ليست**نصيحة مستدامة، لأنه كي يتمكنوا من مواصلة أنشطتهم يحتاج العديد من الأشخاص من هذه الفئات إلى فتح الملفات المرسلة إليهم والتي قد تشمل تهديدات مثل دعوات المؤتمرات الصحفية والوثائق المسربة وجداول أعمال الأحداث وما إلى ذلك. وبالتالي فإن النصيحة الأكثر ملائمة التي يمكننا تقديمها لهم هي معرفة المخاطر وبناء العمليات للسماح لهم بفتح الملفات بأكثر الطرق أمانًا.

لكن تشمل بعض التدابير الدفاعية ضد المستندات الضارة ما يلي:

بشكل عام

حلول مكافحة الفيروسات

تُعدّ العديد من المستندات الضارة المنشورة جزءًا من عمليات ضخمة موثّقة بنجاح ومضمّنة في قواعد بيانات الكشف عن الفيروسات، لكن يجب أن تراعي أن هذه التوصية لا تضمن اكتشاف الملفات الضارة المصممة خصيصًا لأهداف محددة. بالرغم من ذلك توفر طبقة من الأمان من المحبذ وجودها بالأخص إذا كانت تعمل مع العديد من الملفات غير الموثوقة. تذكر أن تختار بائعًا حسن السمعة وتفعيل ميزة الكشف في الوقت الفعلي إذا كانت متاحة وإبقاء قاعدة البيانات محدّثة.

استخدم البرامج القانونية والمحدثة

في كل عام تُكتشف المئات من الثغرات الأمنية الجديدة وتُضاف إلى العديد من البرامج المستخدمة يوميًا بما في ذلك قارئات ملفات مايكروسوفت أوفيس وبي دي إف (PDF) ويتم "تصحيح" الثغرات الأمنية المذكورة من خلال تحديثات البرامج، لذلك سيقلل تحديث جميع البرامج بشكل كبير من فرص استغلال شخص ما للثغرات المعروفة والموثقة لمهاجمة الهدف والنجاح. سيؤثر وجود برامج مقرصنة على قدرتها على اكتشاف تحديثات البرامج وتطبيقها مما يجعلها مشكلة أمنية، وسبب ذلك أنه من المستحسن وجود برنامج أصلي من منظور أمني حتى قبل التطرق إلى الاعتبارات القانونية.

مراجعة امتداد الملفات المشبوهة

تخدع بعض الحملات المستخدمين وتتسبب بقيامهم بفتح ملفات ضارة بمظهر مستندات ولكنها أنواع أخرى من الملفات مثل التطبيقات القابلة للتنفيذ أو ملفات zip. المضغوطة أو أنواع ملفات الحاويات الأخرى مثل iso. وما شابهها. عادةً ما تتضمن هذه الملفات رموزًا

مخصصة لتشبه مستندات مايكروسوفت وورد (MS Word) وملفات بي دي إف وما إلى ذلك. إن التحقق بعناية من الملفات التي نقوم بتنزيلها وفتحها سيمنحنا طبقة أخرى من الحماية عن طريق كشف عندما لا يكون نوع الملف نوع شائعًا أو متوقعًا.

استخدام قارئات "مستعارة"

تتمثل استراتيجية شائعة في فتح المستندات المشبوهة في بيئة بعيدة عن جهاز الكمبيوتر الخاص بك مجهزة بشكل أفضل لاكتشاف واحتواء أي تهديد محتمل، ومن الأمثلة الكلاسيكية على ذلك هو فتح الملفات باستخدام جوجل درايف (Google Drive) ويشمل ذلك المعاينات في جيميل (Gmail) لأن ذلك يسمح بفتح الملف فعليًا في خوادم جوجل وعرضه على أجهزة الكمبيوتر الخاصة بنا مما يجعل جوجل (أو أي منصة أخرى ذات قدرات مماثلة) هي الجهة الفاعلة التي عليها أن تقلق بشأن تهديدات محددة موجودة في المستندات المفتوحة. لكن الجانب السلبي لهذا النهج هو فقداننا لبعض إمكانيات الرؤية والتحليل لأننا لا نقوم بتنزيل الملفات ولكن سيكون هذا مفيدًا في الاستخدام اليومي.

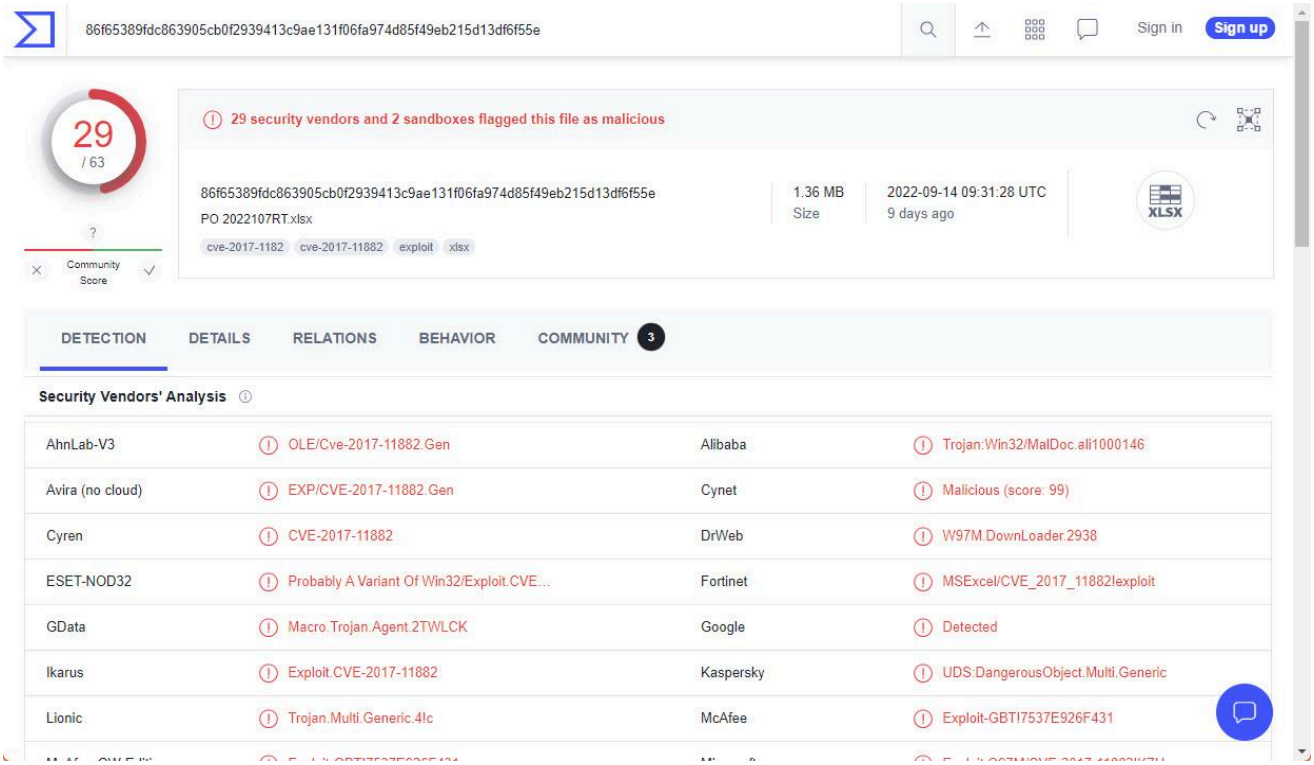
استخدم أدوات محددة مصممة لحالة الاستخدام هذه

هناك أدوات تستخدم مبدأ استخدام بيئة آمنة لفتح الملفات ولكن تُبسط العملية للمستخدم ثم تُنشئ نسخ آمنة تشمل فقط العناصر المرئية (على غرار طباعة المستند ثم مسح النتيجة وحفظها في ملف نهائي). إحدى الأدوات هي دينجزر زون (Dangerzone) التي هي عبارة عن برنامج يتلقى ملفًا مشبوهًا وينشئ نسخة آمنة لفتحها، والجانب السلبي الوحيد الملحوظ هو أن الأداة تتطلب تنزيل تبعيات حجمها كبير لذلك إذا كانت مساحة القرص الثابت و/أو سرعات التنزيل واستقرارها مشكلة فقد يكون إعداد هذه الأداة أكثر صعوبة. هناك أداة أخرى لتحقيق هذا الهدف هي منظف أقراص يو إس بي (USB) المسمى سيركلين (CIRCLean USB Sanitizer) من Circ.lu والذي يستخدم جهاز كمبيوتر منفصلٍ (يقترحون رازبيري باي (Raspberry Pi)) ومحركي أقراص يو إس بي. تضع في محرك الأقراص الأول النسخ المشبوهة من الملفات فيقوم البرنامج بإنشاء النسخ الآمنة وحفظها على محرك أقراص يو إس بي الثاني. تتمثل أبرز التحديات التي تواجه هذا النهج استخدام أجهزة مخصصة لتشغيل الملفات وإضافة خطوات مادية إضافية لنقل الملفات من وإلى محركات أقراص يو إس بي.

التحقق من شفرات تجزئة الملفات في منصات الكشف

هناك استراتيجية شائعة أخرى عندما تواجهك ملفات مشبوهة وهي فحصها في منصات مثل فايروس توتال (VirusTotal) لترى ما إذا كان الملف يعرف بأنه ضار، وسيساعدنا هذا على توفير الوقت في حالة كان الملف تهديدًا معروفًا وسيوفر لنا معلومات أكثر قيمة مثل نوع البرمجيات الضارة التي يحاول تنفيذها والرسائل الواردة من أعضاء المجتمع المرتبطين بالملف. من المهمة للغاية ملاحظة أن تحميل الملف إلى أدوات مثل فايروس توتال سيضع الملف في تصرف المجتمع ويكشف عن محتواه (الذي قد يحتوي على معلومات حساسة) وربما ينبه منشئي المستند إذا كانوا يراقبون هذا الملف. ولذلك يتمثل الحل البديل **في عدم** تحميل الملف ولكن التحقق من شفرة تجزئته. كان في الجزء الأول من هذه السلسلة إرشادات حول كيفية التحقق من شفرات التجزئة.

مثال على البحث عن شفرة تجزئة ملف واحد، أغسطس 2022.

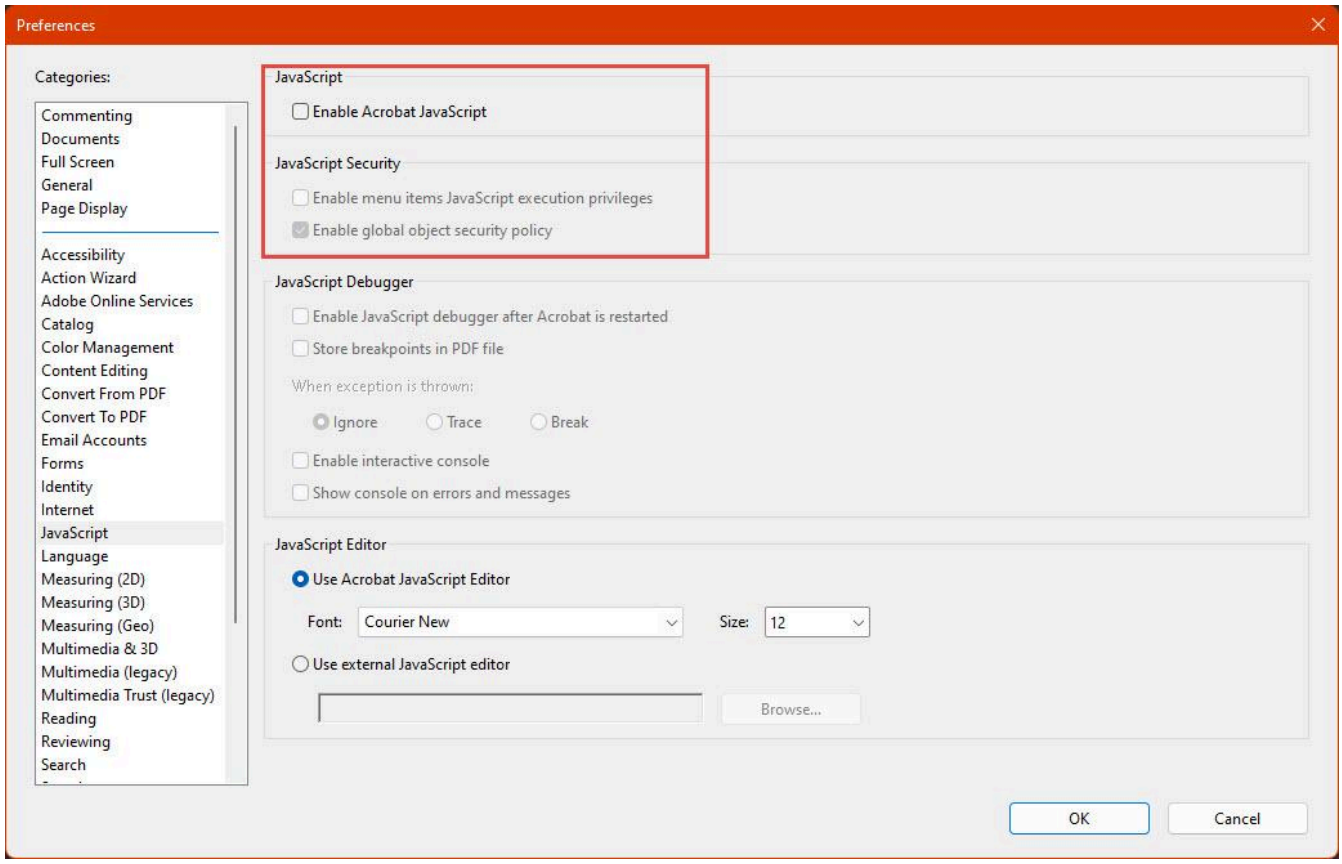


.

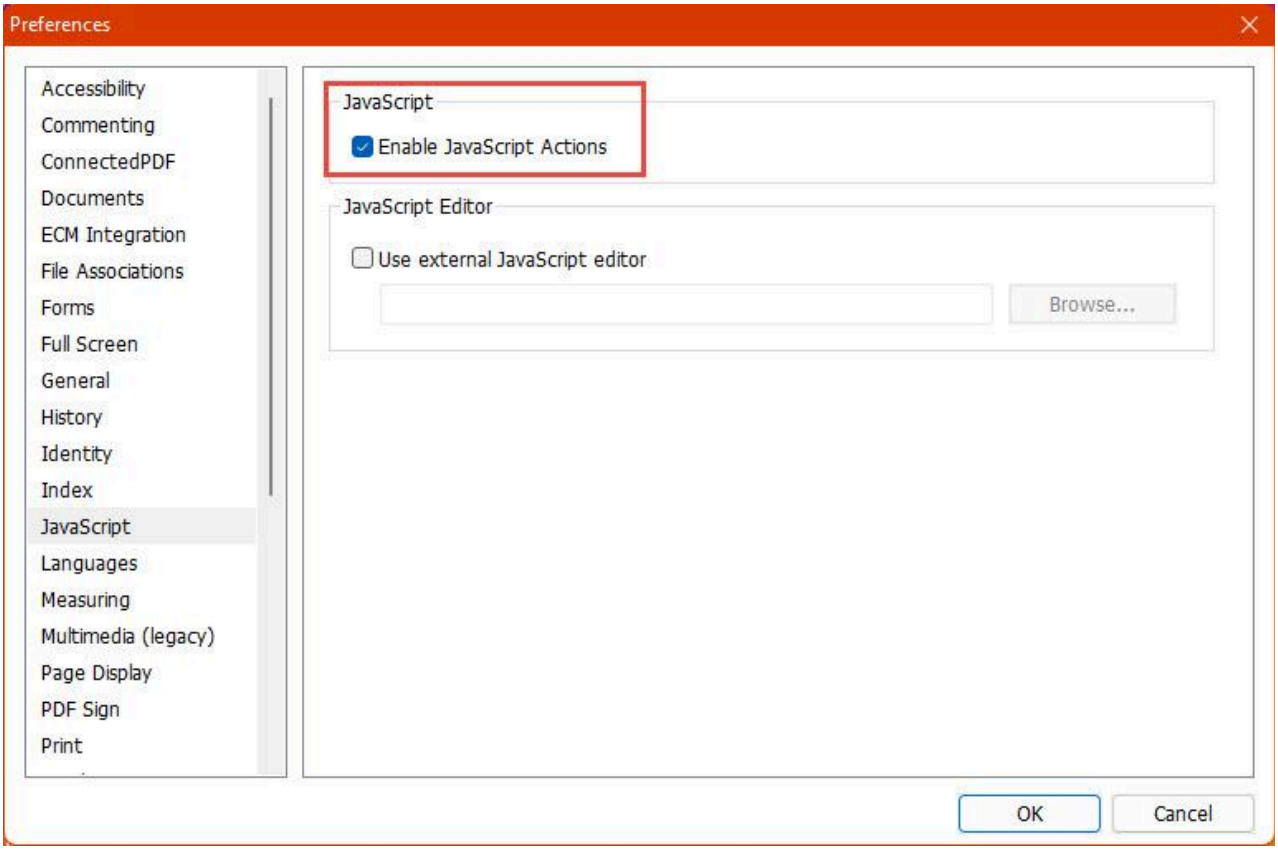
مثال على نتائج من فايروس توتال، أغسطس 2022.

خاص بملفات بي دي إف (PDF): تعطيل تنفيذ جافا سكريبت (Javascript) في القارئ (وإعدادات الأمان الأخرى)

حسب برنامج قارئ بي دي إف الخاص بك قد يكون تنفيذ تعليمات جافا سكريبت معطلًا بالفعل لكن يُنصح بالتحقق مرة أخرى في حالة كان من المتوقع أن تفتح ملفات مشبوهة. حسب المستعرض قد تكون هناك ميزات أمان أخرى يمكن تكوينها.



مثال قارئ أكروبات (Acrobat) (أغسطس 2022، القائمة تعديل -\> التفضيلات -\>جافا سكريبت)



}

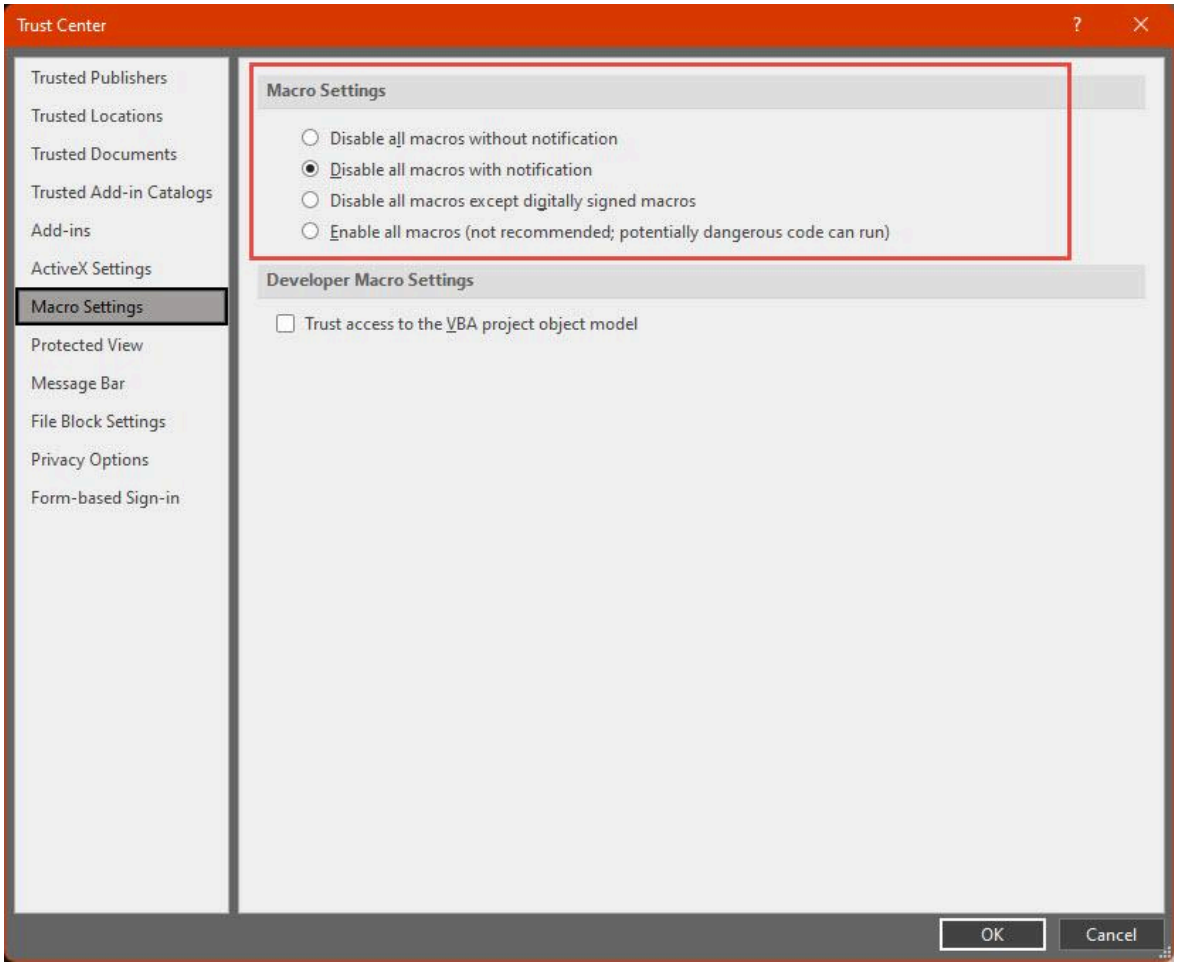
مثال لقارئ فوكسيت (أغسطس 2022، القائمة ملف-\>التفضيلات-\>جافا سكريبت)

خاص بملفات أوفيس: تقليل استخدام تعليمات الماكرو (macro) في الأنشطة المشروعة

حتى عندما يكون هناك العديد من حالات الاستخدام المقبولة وغير الضارة لتعليمات الماكرو من الممكن أن يؤدي استخدام المستندات التي تضمها بشكل متكرر والاعتياد على السماح بها إلى فتح الباب أمام تلقي مستند ضار وتمكين الماكرو فيه عن طريق الخطأ ويجب على المنظمات بالأخص أن تراعي هذه الحالة وتخطط وفقًا لذلك أو تزيل استخدام تعليمات الماكرو أو تجهيز العمليات تسمح باستخدامها لكن مع مراعاة كيفية التعامل مع الملفات غير الموثوقة.

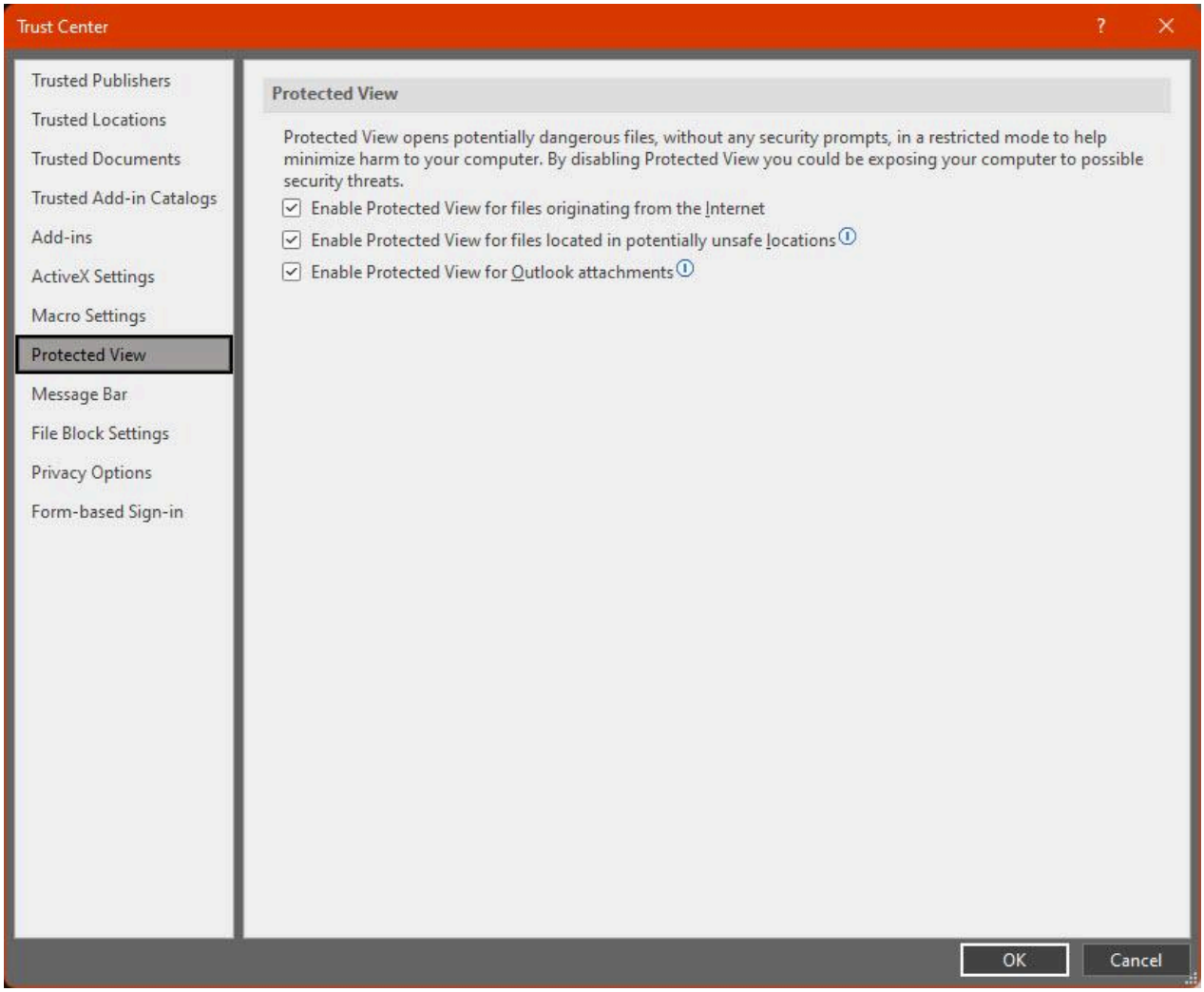
خاص بملفات أوفيس: تعطيل تعليمات الماكرو والتحقق من مركز التوثيق

تغيّرت مؤخرًا سياسات مايكروسوفت أوفيس المتعلقة بتعليمات الماكرو عدة مرات لذلك حسب وقت قراءتك لهذا القسم قد تكون تعليمات ماكرو مفعلة أو معطلة افتراضيًا في أوفيس وهناك أيضًا قواعد اعتمادًا على أصل الملفات وما إلى ذلك. وتتمثل إحدى طرق الحصول على رؤية وتحكم أكبر في التحقق من مركز التوثيق لرؤية سلوك التعامل وحدات الماكرو وضبطه مباشرة.

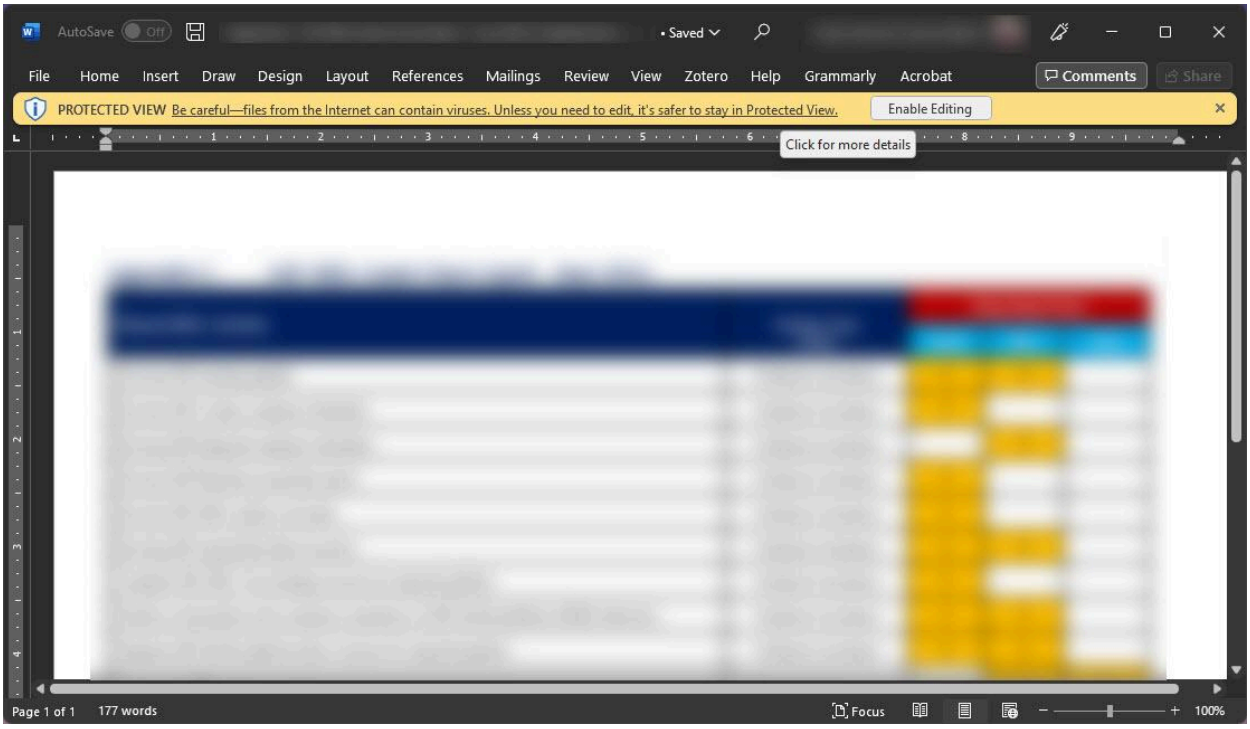


مركز التوثيق لبرنامج مايكروسوفت أوفيس (أغسطس 2022، القائمة ملف-\>خيارات-\>مركز التوثيق-\>إعدادات مركز التوثيق-\>إعدادات الماكرو)

إحدى الميزات الأخرى المثيرة للاهتمام في مايكروسوفت أوفيس هي طريقة العرض المحمية والتي حسب أصل الملف تقوم تفتحه في بيئة اختبار معزولة مع تقليل الامتيازات ووصولها إلى الكمبيوتر للعبث فيه بما يوفر طبقة ثقة إضافية. تتمثل إحدى المشكلات في هذا الوضع (وعلى غرار حظر تعليمات الماكرو) بوجود زر في شريط أعلى المستند يسمح للمستخدم بتعطيل ميزة العرض المحمي مما يتيح مرة أخرى للهجمات في حال خدع منشئ المستند المستخدم لتعطيل هذه الحماية.



إعدادات العرض المحمي (أغسطس 2022، القائمة ملف-\>خيارات- \>مركز التوثيق-\>إعدادات مركز التوثيق-\>العرض المحمي)



طريقة العرض المحمي لمستند مايكروسوفت وورد (أغسطس 2022)

الخطوات التالية

في البداية عند تلقي ملف مشبوه سيكون لديك المهارات اللازمة لإجراء تحليل أولي لمعرفة أي مشاكل أمنية واضحة ويمكن أن تشمل السيناريوهات المحتملة ما يلي:

1. إذا بدا أن الملف لا يحتوي على أي شيء ضار فيمكننا خفض مستوى الاشتباه في الملف.
   - إذا كان الهدف يعاني بأي حال من الأحوال من مستوى خطر مرتفع فقد نرغب في التحقق مرة أخرى مع زملاء آخرين أو مجموعات أكثر تخصصًا.
2. إذا كان الملف يبدو ضارًا يمكن أن نحاول فحصه على منصات مثل فايروس توتال باستخدام شفرة تجزئته، وإذا كانت عينة برمجية ضارة معروفة يمكننا العثور على الكثير من المعلومات الأكثر تفصيلًا التي ستكون مفيدة لفهم طبيعة التهديد وحجم الحملة وما إلى ذلك.
3. إذا كان من السهل اكتشاف التهديدات الواردة في الملف وفهمها ولكن لا يعرفها المجتمع فيجب أن نكون قادرين على إعطاء بعض الأفكار حول التفاصيل عند البحث أكثر أو طلب المساعدة.
4. إذا كانت العناصر الواردة في الملف تبدو متقدمة أو يصعب فهمها أو حتى يصعب تصنيفها على أنها تهديدات وشفرة تجزئة الملف غير معروفة للمنصات العامة، فمن الجدير التواصل مع منظمات أكثر تخصصًا يمكنها إلقاء نظرة أفضل على الملفات بحثًا عن تهديدات غير واضحة.

ننصح أيضًا بشكل عام بما يلي:

- تجنب تنفيذ أي تعليمات برمجية مشبوهة ما لم تفهم المخاطر وتتخذ الاحتياطات ذات الصلة وهي أمور لا يغطيها هذا القسم.

- ابحث أكثر عن أي تفاصيل تجدها ولا تعرف ماهيتها. علمًا أن هناك الكثير من الأوامر والطرق المختلفة لتحقيق الأشياء باستخدام التعليمات البرمجية ومن غير المستدام معرفتها جميعها لذلك من الطبيعي والمتوقع مراجعة الوثائق التي تبحث عن تعليمات أو خصائص محددة لتحسين فهم تعليمات الماكرو أو الكائنات الأخرى غير المعروفة.

يجب مراعاة أن تحليل المستندات والبرمجيات الضارة بشكل عام هي مهنة كاملة تتطلب عادة سنوات من الخبرة للتعامل مع الحالات الأكثر تقدمًا. لكننا نؤكد أن هذا القسم هو مقدمة إلى قسم خاص من تحليل البرمجيات الضارة نأمل أن يشجع القارئ على معرفة المزيد واكتساب المزيد من المهارات في هذا المجال. لكن نظرًا للمخاطر المرتبطة بتشغيل العناصر الضارة دون استخدام العمليات والاعتبارات الأمنية المناسبة، لا نشجع القراء على استخدام عمليات أو أدوات تحليل إلى سير العمل المقدم دون معرفة مناسبة بتلك العمليات والأدوات وبالأخص تلك التي تنطوي على تنفيذ البرمجيات الضارة (أو التحليل الديناميكي).

يخضع هذا القسم لمراجعة مستمرة، ولأي أسئلة أو ملاحظات يرجى التواصل مع cguerra@internews.org