الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1235

(2022/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

مكافحة الرسائل الاقتحامية – الأمن السيبراني

تكنولوجيات مكافحة انتحال صفة الموقع الإلكتروني لمنظمات الاتصالات

التوصية ITU-T X.1235

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1-X.199
التوصيل البيني للأنظمة المفتوحة	X.200-X.299
التشغيل البيني للشبكات	X.300-X.399
أنظمة معالجة الرسائل	X.400-X.499
الدليل	X.500-X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600-X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.600-X.699
الأمن	X.800-X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850-X.899
المعالجة الموزعة المفتوحة	X.900-X.999
آمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000-X.1029
آمن الشبكة	X.1030-X.1049
إدارة الأمن	X.1050-X.1069
الخصائص البيومترية	X.1080-X.1099
تطبيقات وخدمات آمنة (1)	
آمن البث المتعدد	X.1100-X.1109
آمن الشبكة المحلية	X.1110-X.1119
آمن الخدمات المتنقلة	X.1120-X.1139
آمن الويب (1)	X.1140-X.1149
بروتوكولات الأمن (1)	X.1150-X.1159
الأمن بين جهتين نظيرتين	X.1160-X.1169
آمن معرفات الهوية عبر الشبكات	X.1170-X.1179
آمن التلفزيون القائم على بروتوكول الإنترنت	X.1180-X.1199
آمن الفضاء السيبراني	
الأمن السيبراني	X.1200-X.1229
مكافحة الرسائل الاقتحامية	**X.1230-X.1249**
إدارة الهوية	X.1250-X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300-X.1309
آمن شبكات المحاسيس واسعة الانتشار	X.1310-X.1319
آمن شبكة الكهرباء الذكية	X.1330-X.1339
البريد المعتمد	X.1340-X.1349
آمن إنترنت الأشياء (IoT)	X.1350-X.1369
آمن أنظمة النقل الذكية (ITS)	X.1370-X.1399
آمن سجل الحسابات الموزع (DLT)	X.1400-X.1429
آمن التطبيقات (2)	X.1450-X.1459
آمن شبكة الويب (2)	X.1470-X.1489
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500-X.1519
تبادل مواطن الضعف/الحالة	X.1520-X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540-X.1549
تبادل السياسات	X.1550-X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560-X.1569
تعرف الهوية والاكتشاف	X.1570-X.1579
التبادل المضمون	X.1580-X.1589
الدفاع السيبراني	X.1590-X.1599
آمن الحوسبة السحابية	
نظرة عامة على آمن الحوسبة السحابية	X.1600-X.1601
تصميم آمن الحوسبة السحابية	X.1602-X.1639
أفضل الممارسات ومبادئ توجيهية بشأن آمن الحوسبة السحابية	X.1640-X.1659
تنفيذ آمن الحوسبة السحابية	X.1660-X.1679
آمن أشكال أخرى للحوسبة السحابية	X.1680-X.1699
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار آمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم آمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات آمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
آمن البيانات	
آمن البيانات الضخمة	X.1759–X.1750
حماية البيانات	X.1789–X.1770
آمن الاتصالات المتنقلة الدولية–2020	X.1819–X.1800

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1235

تكنولوجيات مكافحة انتحال صفة الموقع الإلكتروني لمنظمات الاتصالات

ملخص

يشكل انتحال صفة موقع إلكتروني تهديداً كبيراً لمنظمات الاتصالات، ولا سيما شركات التشغيل. ويوصى مشغلو الاتصالات باعتماد تكنولوجيات مكافحة انتحال صفة موقع إلكتروني لحماية عملائهم وصون سمعتهم وإيراداتهم. وتحلل التوصية ITU-T X.1235 التدابير الرئيسية لانتحال صفة موقع إلكتروني وتوصي بتكنولوجيات لتحديد المواقع الإلكترونية ذات الصفة المنتحَلة، ويمكن اعتبار هذه التدابير مبادئ توجيهية لحماية المواقع الإلكترونية من انتحال صفتها بالنسبة إلى منظمات الاتصالات. ويمكن تنفيذ نهج مماثل ضد انتحال صفة أي موقع إلكتروني، بما في ذلك المواقع الإلكترونية للمصارف، وشركات التأمين، ومحلات الإنترنت وغيرها.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1235	2022-01-07	17	11.1002/1000/14797

مصطلحات أساسية

التدابير المضادة، انتحال صفة موقع إلكتروني.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع/ حقوق ملكية برمجيات يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية الرجوع إلى قواعد البيانات المناسبة لدى قطاع تقييس الاتصالات المتاحة في الموقع الإلكتروني للقطاع في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مقدمة

أدى انتحال صفة موقع إلكتروني دوراً رئيسياً في الاحتيال عبر الإنترنت في السنوات الأخيرة. ويختار المحتالون عادة مواقع إلكترونية لمنظمات أو شركات معروفة لجمع بيانات اعتماد الزوار أو نشر برمجيات خبيثة. ويؤدي ذلك إلى خسارة مالية للزوار ومشغلي الاتصالات على السواء وإلى إهدار سمعة مشغلي الاتصالات.

ونظراً لأن المواقع الإلكترونية لمشغلي الاتصالات أصبحت من أهم البوابات الإلكترونية لعملائهم كي يستعلموا عن جميع أنواع الخدمات ويشتركوا فيها، فقد لوحظ في جميع أنحاء العالم أن المحتالين يحاولون على الدوام تزييف المواقع الإلكترونية لمشغلي الاتصالات بغية غش العملاء. وتجري هذه التوصية تحليلاً شاملاً لانتحال صفة المواقع الإلكترونية وتوصي بسلسلة من التدابير المضادة المنظمة.

التوصية ITU-T X.1235

تكنولوجيات مكافحة انتحال صفة الموقع الإلكتروني لمنظمات الاتصالات

1 مجال التطبيق

توصي هذه التوصية بالتكنولوجيات اللازمة لمنظمات الاتصالات للتعرف على انتحال صفة موقع إلكتروني في الوقت المناسب وحماية مواقعها الإلكترونية من التلاعب. وبعد تحليل منهجي لتدابير انتحال الصفة وسماتها، توصي بأفضل الممارسات في تطبيق التكنولوجيات على جانب الشبكة بمساعدة التكنولوجيات من جانب المستعمل لمكافحة انتحال صفة موقع إلكتروني.

ولا يجوز اعتبار الامتثال لهذه التوصية دليلاً يتيح الادعاء بالامتثال لأي قانون، أو لائحة، أو سياسة على المستوى الوطني أو الإقليمي. ولا تكفل الوسائل التقنية، والتنظيمية، والإجرائية الموصوفة في هذه التوصية بأي حال من الأحوال تشكيل أي مستوى من الأمن الذي يمكن أن يُرسى على أساس التوافق مع أي قوانين، أو لوائح، أو سياسات وطنية أو إقليمية.

ويمكن تنفيذ نهج مماثل ضد انتحال صفة أي موقع إلكتروني، بما في ذلك المواقع الإلكترونية للمصارف، وشركات التأمين، ومحلات الإنترنت وغيرها.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

لا توجد.

3 التعاريف

1.3 مصطلحات معرَّفة في مصادر أخرى

لا توجد.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 الشبكة العصبية التلافيفية: خوارزمية تعلم عميق تأخذ صورة المدخلات، وتسند أهمية لجوانب/كائنات مختلفة في الصورة ويمكنها تمييز أحدها عن الأخرى.

2.2.3 شبكات الذاكرة الطويلة للبيانات قصيرة الأجل: نمط من الشبكات العصبية المتكررة القادرة على تعلم الاعتماد على ترتيب معين في مشاكل التنبؤ بالتتابع.

3.2.3 الشبكة العصبية المتكررة: صنف من الشبكات العصبية يسمح باستعمال المخرجات السابقة كمدخلات مزودة بحالات محجوبة.

4.2.3 تحويل السمة غير المتغيرة مع المقاييس (SIFT): هو خوارزمية كشف سمة في رؤية الحاسوب لكشف ووصف السمات المحلية في الصور، وهي تتألف من معرّف وصفي لا يتغير مع الترجمات والدورانات وتحويلات المقايسة في ميدان الصورة، ويظل

متماسكاً أمام تحولات المنظور وتغيرات الإضاءة المعتدلة. وقد ثبت تجريبياً أن معرف الهوية الوصفي لتحويل السمة غير المتغيرة مع المقاييس (SIFT) مفيد جداً من الناحية العملية لمطابقة الصور والتعرف على الكائنات في ظروف العالم الحقيقي.

5.2.3 السمات المتماسكة المسرَّعة: كاشف السمة المحلية ومعرفها الوصفي في رؤية الحاسوب للكشف عن السمات المحلية للصور ووصفها وهو أسرع عدة مرات من تحويل السمة غير المتغيرة مع المقاييس (SIFT) وهو أكثر تماسكاً ضد تحويلات الصور المختلفة مقارنة بتحويل السمة غير المتغيرة مع المقاييس.

6.2.3 موقع إلكتروني ذو صفة منتحَلة: موقع إلكتروني مُنشأ بانتحال صفة موقع إلكتروني آخر (انظر الفقرة 8.2.3).

7.2.3 آلة متجه الدعم: نموذج تعلم الآلة الخاضع للإشراف الذي يحل مشاكل التصنيف في مجموعتين بمجموعات معينة من بيانات التدريب الموسومة لكل فئة، تستطيع تصنيف مجموعات جديدة.

8.2.3 انتحال صفة موقع إلكتروني: هو مجموعة من السلوكيات الخبيثة لتقليد موقع إلكتروني معروف جيداً للعموم أو لمجموعة من الناس؛ ثم يُستعمل الموقع الإلكتروني المزيف لاستغلال ثقة الزوار من أجل تحقيق أهداف خبيثة/غير قانونية، مثل الاحتيال وانتهاك الخصوصيات، وما إلى ذلك.

4 الاختصارات والأسماء المختصرة

تستعمل هذه التوصية الاختصارات والأسماء المختصرة التالية:

AI الذكاء الاصطناعي *(Artificial Intelligence)*

DNS خدمة أسماء الميادين *(Domain Name Service)*

GUI السطح البيني البياني للمستعمل *(Graphical User Interface)*

LSTM الذاكرة الطويلة للبيانات قصيرة الأجل *(Long Short-Term Memory)*

OCR التعرف البصري على الحروف *(Optical Character Recognition)*

PII المعلومات المحدِّدة لهوية شخص *(Personally Identifiable Information)*

QR الرد السريع *(Quick Response)*

SIFT تحويل السمة غير المتغيرة مع المقاييس *(Scale-Invariant Feature Transform)*

SURF السمات المتماسكة المسرَّعة *(Speeded Up Robust Features)*

SVM آلة متجه الدعم *(Support Vector Machine)*

URL محدد موقع الموارد الموحد *(Uniform Resource Locator)*

5 الاصطلاحات

تستعمل هذه التوصية الاصطلاحات التالية:

وتشير كلمة "**يُوصَى**" إلى متطلَّب يُوصى به لكنه ليس ملزِماً إلزاماً مطلَقاً. وبالتالي لا يستلزم إعلانُ المطابقة تحقُّقَ هذا المتطلَّب.

وكلمة "**يجوز**" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به.

وفي متن هذه التوصية، تظهر في بعض الأحيان كلمة "**يمكن**". وفي هذه الحالة يكون تأويلها بمعنى فعل "**يستطيع**" وتصريفاته.

6 تحليل انتحال صفة موقع إلكتروني

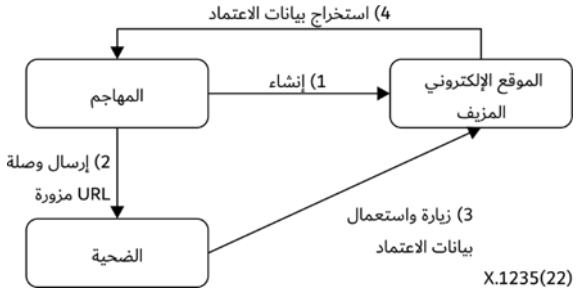
انتحال صفة موقع إلكتروني هو مجموعة من السلوكيات الخبيثة لتقليد موقع إلكتروني معروف للعموم أو لمجموعة من الناس. وتقوم المواقع الإلكترونية ذات الصفة المنتحَلة بجمع بيانات اعتماد الزوار أو نشر البرمجيات الضارة لتحقيق أهداف خبيثة/غير قانونية، مثل الاحتيال وانتهاك الخصوصيات، وما إلى ذلك.

ويمكن أن يتسبب انتحال صفة موقع إلكتروني في أضرار جسيمة بعدة طرق. فقد يكبد مثلاً العملاء والمشغلين معاً خسائر مالية ويلحق الضرر بسمعة المشغلين، وما إلى ذلك. علاوة على ذلك، تمكن إساءة استعمال معلومات المستعمل المتسربة لفترة طويلة حتى في حال اختفاء الموقع الإلكتروني ذي الصفة المنتحَلة. ولذلك، من المهم لمنظمات الاتصالات، خاصة شركات التشغيل، أن تعتمد تكنولوجيات مفيدة لمكافحة انتحال صفة المواقع الإلكترونية.

1.6 سيناريو انتحال صفة موقع إلكتروني

ومن السيناريوهات النمطية لإنشاء موقع إلكتروني ذي صفة منتحَلة لتحقيق هدف غير سليم ثلاث مراحل على النحو المبين في الشكل 6-1.

- **المرحلة الأولى**: إنشاء موقع إلكتروني
  - الخطوة الأولى: إنشاء وتشغيل موقع إلكتروني ذي صفة منتحَلة يماثل بعض المواقع الإلكترونية المعروفة أو يشابهها.
- **المرحلة الثانية**: نشر وصلة محدِّد موقع الموارد الموحَّد (URL)
  - الخطوة الثانية: يُنشر الموقع الإلكتروني ذو الصفة المنتحَلة بأساليب مختلفة مثل البريد الإلكتروني وخدمة الرسائل القصيرة وخدمات المراسلة الفورية، وما إلى ذلك.
- **المرحلة الثالثة**: جمع بيانات الاعتماد أو نشر البرمجيات الضارة
  - الخطوة الثالثة: خداع الزائرين لإدخال بيانات الاعتماد أو تنزيل برمجيات ضارة. وبمجرد نفاذ الضحايا إلى موقع إلكتروني ذي صفة منتحَلة، قد يعتقدون خطأً أن الموقع الإلكتروني هو الموقع الحقيقي ويسجلون دخولهم ببيانات اعتمادهم أو يقومون بتنزيل برمجيات ضارة.
  - الخطوة الرابعة: تُستخرج بيانات اعتماد الزائرين، ويجري الاستعداد لاحتيال أو أي نشاط خبيث آخر.



الشكل 6-1 – المراحل الأربعة لاستعمال موقع إلكتروني ذي صفة منتحَلة لجمع بيانات اعتماد المستعمل

2.6 خصائص انتحال صفة المواقع الإلكترونية

1.2.6 خصائص المواقع الإلكترونية ذات الصفة المنتحَلة

تستعمل المواقع الإلكترونية ذات الصفة المنتحَلة تقنيات متماثلة لخداع الزوار كي يعتقدوا أنهم يزورون مواقع حقيقية. ولها عدة خصائص مشتركة:

- التشابه المرئي: قد يكون الموقع الإلكتروني ذو الصفة المنتحَلة نسخة كاملة من الموقع الحقيقي، بما في ذلك محتواه المرئي ومنطقه التفاعلي.
- استعارة العناصر المرئية: قد يستعير الموقع الإلكتروني ذو الصفة المنتحَلة بعض العناصر المرئية المهمة من الموقع الإلكتروني الحقيقي.
- الوصل مع مواقع إلكترونية معروفة جيداً: قد يتضمن الموقع الإلكتروني ذو الصفة المنتحَلة وصلات إلى مواقع إلكترونية معروفة لتقليد موقع إلكتروني شريك معتمَد أو موقع إلكتروني ذي صلة أو نسخة مختلفة من الموقع الإلكتروني.
- اسم ميدان مشابه: من شأن اسم الميدان لموقع إلكتروني ذي صفة منتحَلة أن يشابه إلى حد كبير اسم الميدان للموقع الإلكتروني الحقيقي.
- اسم ميدان ملتبس: يستعمل المهاجمون أحياناً خدمات تقصير عناوين URL أو شفرات الرد السريع (QR) لحجب الاسم الحقيقي للميدان في موقع إلكتروني على أساس التشارك في وصلة.
- اسم ميدان مكرر: قد تُحجز مجموعة من أسماء الميادين لموقع إلكتروني ذي صفة منتحَلة ولإطالة عمر الموقع الإلكتروني ذي الصفة المنتحَلة، يُتناوب على نشر العديد منها لمرة واحدة.
- تمويه شفرة المصدر: قد تُموه شفرة مصدر موقع إلكتروني ذي صفة منتحَلة لإرباك برامج الفحص الأمني.
- مدخلات بيانات الاعتماد: قد تغري المواقع الإلكترونية ذات الصفة المنتحَلة الزائرين لإدخال بيانات الاعتماد.
- إعادة التوجيه إلى موقع إلكتروني معروف: قد يقوم موقع إلكتروني ذو صفة منتحَلة بإعادة التوجيه إلى مواقع إلكترونية معروفة (مثل google.com) خلال وقت الخمول لتجنب الفحص التلقائي للاحتيال عبر الإنترنت.
- شريط العناوين المزور: قد تصمَم بعض المواقع الإلكترونية ذات الصفة المنتحَلة لمتصفحات الويب المتنقلة على وجه التحديد. ويمكن لهذا الموقع الإلكتروني أن يضع نسخة مزيفة من شريط عنوان المتصفح المتنقل في أعلى شاشة الهاتف المتنقل وأن يثبِّت النسخة في مكانها عن طريق إساءة استعمال ميزة السطح البيني البياني للمستعمل (GUI) في متصفح الهاتف المتنقل.

2.2.6 خصائص الأنشطة ذات الصلة

يمكن القيام بالعديد من الأنشطة لإغراء أو خداع الأشخاص بغية حملهم على زيارة المواقع الإلكترونية ذات الصفة المنتحَلة والتفاعل معها. ويمكن أن تكون خصائص أو تكتيكات هذه الأنشطة واحدة أو أكثر من تلك المذكورة فيما يلي:

- نشر رسائل لإعلام أكبر عدد ممكن من الناس بوجود موقع إلكتروني ذي صفة منتحَلة.
- الاستيلاء على خدمة في خدمة أسماء الميادين (DNS) أو إفسادها بحيث يعاد توجيه أي زيارات للموقع الإلكتروني الأصلي إلى الموقع الإلكتروني ذي الصفة المنتحَلة.
- استعمال فوائد (من قبيل قسيمة وهدايا وما إلى ذلك) لإغراء المستعملين بالنقر على وصلات مزيفة في الموقع الإلكتروني.
- تثبيت برمجية خبيثة على هاتف الضحية للاستعاضة عن الطلب الحقيقي لموقع إلكتروني بطلب مزيف.
- الاتصال مع المستعملين بتقليد خدمة العملاء وتزويدهم بوصلات مزيفة إلى مواقع إلكترونية.

3.6 العواقب

يمكن أن يكون للموقع الإلكتروني ذي الصفة المنتحَلة تأثيرات سلبية كثيرة على المستعملين ومالكي المواقع الإلكترونية وترد أدناه العواقب المحتملة:

- خسارة ممتلكات للمستعملين: يُحتمل تسرب بيانات اعتماد المستعمل والمعلومات المحددة لهوية الشخص (PII). ويمكن للمحتالين استعمال هذه المعلومات لمواصلة عمليات احتيال أخرى. ويمكن خداع المستعملين لحملهم على تنزيل

برمجيات طروادة وشفرات التنقيب عن العملات المجفَّرة والبرمجيات الضارة الأخرى. ويمكن التحكم في مطاريف المستعمل لسرقة الحسابات المالية ونشر الرسائل الاقتحامية وإصابة المستعملين الآخرين بالعدوى. وستؤدي هذه الأنشطة إلى استنفاد شحنة البطارية أو تعطل المطاريف وستوقع أيضاً خسائر مالية مباشرة وفادحة.

- خسارة ممتلكات للمشغلين: من شأن المعاملات العادية بين المستعملين والمشغلين أن تضيع بل وتُكبح على المدى الطويل.
- إهدار السمعة: من شأن سمعة المواقع الإلكترونية الحقيقية وحتى ثقة الجمهور في المشغِّل أن تتضرر وأن يؤدي ذلك أيضاً إلى عدد كبير من شكاوى العملاء وتقييم سلبي طويل الأجل.

7 التدابير المضادة

يمكن تقسيم التدابير المضادة لانتحال صفة موقع إلكتروني إلى جانبين: تعرُّف الهوية والحماية. فيميز الجانب الأول المواقع الإلكترونية ذات الصفة المنتحَلة عن المواقع الإلكترونية الأخرى؛ انظر الفقرة 1.7. ويحمي الجانب الثاني المستعملين من النفاذ إلى المواقع الإلكترونية ذات الصفة المنتحَلة المعروفة أو الانخداع بها؛ انظر الفقرة 2.7.

ولا ضرورة لمنظمة اتصالات أن تستعمل جميع التكنولوجيات الموصى بها في هذه الفقرة في الوقت نفسه. وبمراعاة البيانات المحصَّلة والبيئة التشريعية ومتطلبات المشتركين وما إلى ذلك، ينبغي لمنظمة اتصالات أن تعتمد التكنولوجيات المناسبة بمرونة، على النحو الموضح في هذه الفقرة.

1.7 تعرُّف الهوية

وفقاً لخصائص المواقع الإلكترونية ذات الصفة المنتحَلة الموضحة في الفقرة 1.2.6، يوصى بالنظر في التدابير المضادة التالية:

1.1.7 مقارنة أسماء الميادين المتشابهة

يوصى بأن يحتفظ المشغلون بقائمة بأسماء ميادين المواقع الإلكترونية المعروفة المعرَّضة لانتحال الصفة. فإذا كان اسم ميدان مشابهاً جداً (وليس مطابقاً) لاسم ميدان وارد في القائمة، قد يكون اسم ميدان لموقع إلكتروني ذي صفة منتحَلة. وإذا كان اسم الميدان مختصَراً بواسطة خدمة اختصار عنوان URL، فينبغي تحويله ثانيةً إلى عنوان URL الأصلي قبل المقارنة.

وهناك أساليب كثيرة لحساب التشابه بين اسمي ميدانين، بما في ذلك تعديل المسافة وتشابه Jaccard وأطول تتابع فرعي مشترك وتحويل التشابه المرئي وغير ذلك.

- **أسلوب تعديل المسافة:** في اسمي الميدان A وB، يحسب هذا الأسلوب العدد الأدنى من التعديلات المطلوبة للتحويل من A إلى B. وكلما قصرت مسافة التعديل، زاد التشابه.
- **أسلوب تشابه Jaccard:** يصار إلى تقسيم مقاس تقاطع مجموعتين من حروف اسم الميدان على مقاس اتحادهما. وكلما زادت النسبة، زاد التشابه.
- **أسلوب أطول تتابع فرعي مشترك:** يتمثل في حساب طول أطول تتابع فرعي مشترك لاسمي ميدانين. وكلما زاد الطول، زاد التشابه.

  ملاحظة – أطول تتابع فرعي مشترك: يعني التتابع الأطول المشترك لتتابعين معيّنين، بشرط ألا تشغل عناصر التتابع الفرعي مواقع متتالية ضمن التتابعات الأصلية. ويجب أن يكون التتابع الفرعي المشترك تتابعاً تصاعدياً تماماً لمؤشري التتابعين المعيّنين. فمثلاً، إذا كان كل من "abcde" و"akcve" تتابعين معينين، فإن "ace" هي التتابع الفرعي الأطول في التتابعين.
- **أسلوب تحويل التشابه المرئي:** تبدَّل حروف متشابهة بصرياً قبل المقارنة. فعلى سبيل المثال، يمكن تبديل "0" و"o" أحدهما بالآخر؛ ويمكن تبديل "1" و"i" أحدهما بالآخر، وما إلى ذلك. فمثلاً، يمكن تحويل اسم الميدان "z00.com" إلى "zoo.com". ويمكن لهذا الأسلوب أن يعزز أداء التشابه. وفي ظروف معينة يمكن لتحويل التشابه المرئي أن يخفض الأداء، ولذلك يستدعي الحذر إجراء مقارنة التشابه قبل وبعد التحويل.

2.1.7 كشف الشعار الرسمي

يوصى بمقارنة الصور أو العناصر المرئية الأخرى في موقع إلكتروني غير معروف بالشعارات الرسمية. وتشمل الشعارات الرسمية، على سبيل المثال لا الحصر، العلامة المميزة والتصاميم الإعلانية وغيرها من العناصر الأيقونية للشركة أو المنظمة. ويشمل أسلوب كشف الشعارات الرسمية الخطوات التالية:

- قبل الكشف، ينبغي جمع الشعارات الرسمية وتخزينها في قاعدة بيانات للشعارات.
- ويصار إلى تنزيل العناصر المرئية لصفحة ويب مجهولة أو لقطة شاشة، ومقارنتها بالشعارات الموجودة في قاعدة بيانات الشعارات. ويمكن حساب التشابه بين الصورتين بواصفين شائعين هما تحويل السمة غير المتغيرة مع المقاييس (SIFT) والسمات المتماسكة المسرَّعة (SURF).
- وفي حال تم تمويه شفرة مصدر كشف صفحة الويب، قد يصعب تنزيل العناصر المرئية. ويمكن بعد ذلك استعمال نوع من أنواع إطار اختبار أتمتة تطبيقات الويب القائم على المتصفح لالتقاط لقطة شاشة لصفحة الويب. وقبل مقارنة الشعارات، يمكن اقتصاص الشعارات من لقطة الشاشة باستعمال نموذج كشف الشعار القائم على الذكاء الاصطناعي. ويمكن تدريب نموذج كشف الشعار هذا القائم على الذكاء الاصطناعي بشكل جيد باستعمال بعض قواعد بيانات الشعارات مفتوحة المصدر.

3.1.7 كشف تمويه الشفرة

يمكن أن تموِّه المواقع الإلكترونية ذات الصفة المنتحَلة الشفرة الخبيثة أو شفرة انتحال الصفة لتصعِّب تحليلها. وتختلف الشفرة المموَهة كثيراً عن الشفرة العادية. وتكثر أساليب كشف الشفرة المموَهة، ومنها المصنِّفات القائمة على الشبكة العصبية التلافيفية والمتكررة، وما إلى ذلك.

- يمكن للمصنفات القائمة على الشبكة العصبية التلافيفية أن تستخرج تلقائياً سمات تتابع n-gram لشفرة المصدر العادية المموَهة. وn-gram هو تتابع متلاصق لكلمات عددها n من شفرة مصدر معينة. ويمكن تحديد عدد الكلمات على أنه 5 أو أكثر لالتقاط السمات التمييزية للتصنيف تماماً.
- وتعتمد المصنِّفات القائمة على الشبكة العصبية المتكررة بشكل أساسي على شبكات الذاكرة الطويلة للبيانات قصيرة الأجل (LSTM) أو شبكات المحولات. وتعامل هذه المصنفات شفرة المصدر على أنها تتابع من الحروف، وتحدد تلقائياً أنماط التتابع بين الشفرة العادية والشفرة المموهة، ثم تحدد ما إذا كانت شفرة مموهة.

4.1.7 كشف مدخلات بيانات الاعتماد

توجد مدخلات بيانات الاعتماد عادة في شكل "استمارات المدخلات" في شفرة مصدر صفحات الويب. ويوجد عادة نعت "كلمة المرور" في شفرة مصدر استمارة الدخل (فهذا النعت يضمن عدم عرض محتوى كلمة المرور عند قيام المستعمل بإدخالها). ويمكن تحديد موقع معلومات النعوت هذه بسرعة باستعمال التعبيرات العادية أو أدوات تحليل صفحة الويب. وفي حال تمويه شفرة مصدر الموقع الإلكتروني، يمكن استعمال أسلوب التعرف البصري على الحروف (OCR) لكشف مدخلات الاعتماد في لقطات شاشة الموقع الإلكتروني. وسيحدد أسلوب التعرف البصري على الحروف المجالات النصية في لقطة شاشة صفحة الويب أولاً ثم يحول المجالات النصية إلى نصوص. فإذا احتوت النصوص المحولة على بعض الكلمات الرئيسية مثل "كلمة المرور"، تُكشَف مدخلات الاعتماد في صفحة الويب.

5.1.7 خدمة أمنية من طرف ثالث

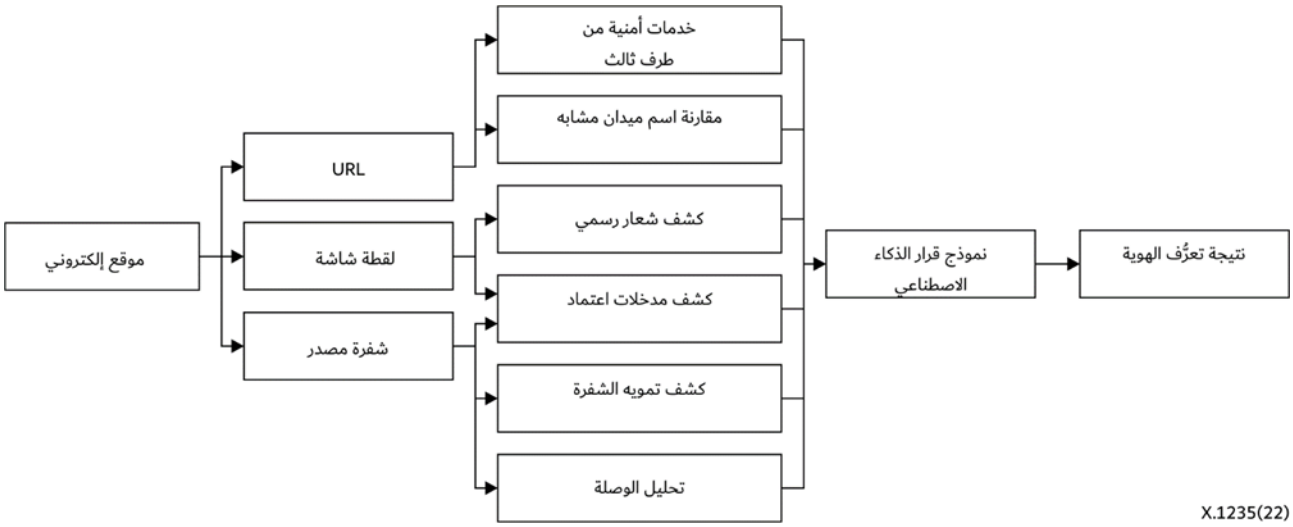
يوصى بأن يستعمل المشغلون الخدمات الأمنية التي يقدمها باعة الخدمات الأمنية الآخرون للحصول على نعوت وإحصاءات موقع إلكتروني، بما في ذلك حركة الموقع الإلكتروني وسمعته وما يخصه من الإضافات المساعدة وتسجيل اسم الميدان والشهادة وغير ذلك من المعلومات الأمنية. ويمكن استعمال هذه المعلومة كمعلومة إضافية لتحديد موقع إلكتروني ذي صفة منتحَلة.

6.1.7 تحليل الوصلة

يمكن للموقع الإلكتروني ذي الصفة المنتحَلة نسخ الوصلات التشعبية في الموقع الإلكتروني الرسمي لإعادة استعمال العناصر المرئية للموقع الإلكتروني الرسمي في صفحاته الإلكترونية ذات الصفة المنتحَلة. ويمكن كشف هذا السلوك بتحليل الوصلة. ويجمع تحليل الوصلة وصلات العناصر المرئية في الموقع الإلكتروني الرسمي ويقارنها مع الوصلات الموجودة في الموقع الإلكتروني المراد كشفه. فإذا احتوى الموقعان على نفس الوصلات التشعبية، أو على العديد منها، يحتمَل أن يكون الموقع الإلكتروني ذا صفة منتحَلة.

7.1.7 تعرُّف الهوية النهائي استناداً إلى درجة السمعة

يوصى بأن يستعمل المشغلون نموذج قرار بشأن الذكاء الاصطناعي (AI) لتجميع كل نتائج التحليل أو الكشف للتدابير المضادة الموصى بها أعلاه واتخاذ قرار شامل بشأن ما إذا كان الموقع الإلكتروني موقعاً إلكترونياً ذا صفة منتحَلة أم لا. وفي نموذج القرار بشأن الذكاء الاصطناعي، تحدَّد ترجيح كل تدبير مضاد تلقائياً بعد مرحلة التدريب.



الشكل 7-1 – تعرُّف الهوية النهائي استناداً إلى درجة السمعة

على النحو الموضح في الشكل 7-1، يجري تحليل الموقع الإلكتروني استناداً إلى عنوان URL الخاص به، ولقطات الشاشة الخاصة به، وشفرة مصدره. وبالنسبة إلى عنوان URL لصفحة الويب، تُحسب درجة تشابه أسماء الميادين ويُتحقق من نتيجة خدمات أمن الطرف الثالث. وبالنسبة إلى لقطات الشاشة، تُكشف الشعارات الرسمية ومدخلات الاعتماد وتُحلَل. وبالنسبة لشفرة المصدر، تُكتشف مدخلات الاعتماد ويجري تحليل الوصلة. ولتحديد ما إذا كان الموقع الإلكتروني ذا صفة منتحَلة، ينبغي أن يأخذ نموذج قرار الذكاء الاصطناعي في الاعتبار جميع هذه الجوانب.

ولتدريب نموذج قرار الذكاء الاصطناعي هذا، ينبغي جمع جميع المواقع الإلكترونية الرسمية المطلوب حمايتها والمواقع الإلكترونية المعروفة ذات الصفة المنتحَلة وغيرها من المواقع الإلكترونية العادية كعينات. وتسنَد درجات تقييم إلى جميع العينات (أي المواقع الإلكترونية التي جُمعت) قياساً بالتدابير المضادة الموصى بها أعلاه على النحو المبين في الشكل 7-1 وسيكون لكل عينة متجه درجة تقييم. ويمكن استعمال جميع متجهات درجات التقييم وأنماطها (ذات الصفة المنتحَلة أو غير المنتحَلة) لجميع العينات كبيانات تدريبية لتدريب مصنِّف لتشكيل نموذج قرار الذكاء الاصطناعي. ويمكن أن تكون المصنِّفات مصنفات قائمة على آلة متجه الدعم (SVM) أو قائمة على الشبكة العصبية العميقة.

ومن المفيد أن تقوم الجهات المستعرضة البشرية بمراجعة المواقع الإلكترونية ذات الصفة المنتحَلة التي تعرَّف عليها نموذج قرار الذكاء الاصطناعي لتجنب سوء التعرف.

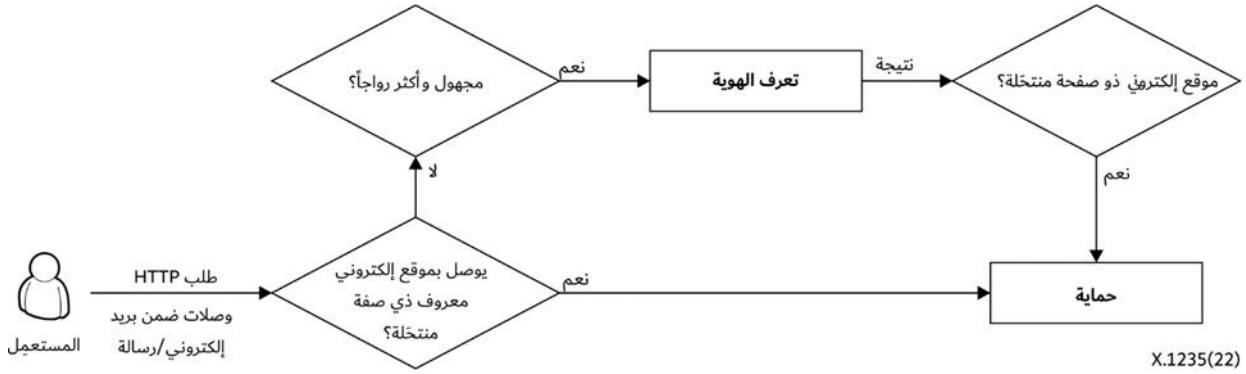
2.7 الحماية

يوصى بأن يحمي المشغِّل المستعملين باعتماد التدابير المضادة التالية بإذن من المستعملين:

- تحذير المستعملين: بمجرد زيارة مستعمل لموقع إلكتروني معروف ذي صفة منتحَلة، يوصى بأن يحجز المشغل الطلب، ويعيد توجيهه إلى صفحة تحذير للتنبيه بخطر انتحال صفة، ويطلب منه تأكيد الطلب.
- إنشاء قائمة حظر: يوصى المشغل بإنشاء قائمة حظر للمواقع الإلكترونية ذات الصفة المنتحَلة لمقاطعة جميع الطلبات الواردة في قائمة الحظر. ويمكن أن تعمل قائمة الحظر في المسيِّرات في شبكات المشغل أو في مخدمات نظام أسماء الميادين الخاصة بالمشغل أو في كيانات الشبكة المناسبة الأخرى.
- منع الانتشار: يوصى المشغل بحظر الرسائل المدسوسة التي تتضمن الوصلة إلى المواقع الإلكترونية ذات الصفة المنتحلة.
- إرشاد المستعملين لحماية أنفسهم من المواقع الإلكترونية التي يُشتبه بانتحالها لصفة: تذكير المستعملين دورياً بمخاطر وسمات المواقع الإلكترونية ذات الصفة المنتحَلة وإعلامهم بأفضل الممارسات في تجنب استعمال هذه المواقع. وتشمل أفضل الممارسات الموصى بها ما يلي:
  - عدم النقر على الوصلات الغريبة في البريد الإلكتروني أو الرسائل.
  - التبصر بعناية في معلومات اسم الميدان في شريط العنوان ومقارنتها مع الموقع الإلكتروني الرسمي.
  - استعمال الوظيفة الأمنية لمتصفحات الويب للتحقق من أصالة موقع إلكتروني ما.
- حماية المستعمل من خلال اكتشاف أسماء الميادين المتجددة لنفس المواقع الإلكترونية ذات الصفة المنتحَلة: يمكن استعمال مجموعة من أسماء الميادين في موقع إلكتروني ذي صفة منتحَلة للتنبؤ بأسماء الميادين المتجددة الأخرى في الموقع الإلكتروني. وإذا التزم محتوى المواقع الإلكترونية في إطار أسماء الميادين المتجددة الحديثة بمحتوى المواقع الإلكترونية المعروفة ذات الصفة المنتحَلة، يمكن التعامل معها على أنها نفس المواقع الإلكترونية ذات الصفة المنتحَلة مباشرةً، واتخاذ إجراءات الحماية الموصى بها أعلاه.

8 الآلية

يوصى بآلية منهجية لمكافحة الموقع الإلكتروني ذي الصفة المنتحَلة بالجمع بين جميع التدابير المضادة الموضحة في الفقرة 7.



الشكل 8-1 – آلية مكافحة المواقع الإلكترونية ذات الصفة المنتحَلة

1) يمكن أن تأتي عناوين URL، على النحو المبين في الشكل 8-1، من طلبات المستعمل لعناوين HTTP أو من رسائل البريد الإلكتروني أو الرسائل الآنية (المرسَلة من الطرف الثالث أو من مستعملين مخولين).

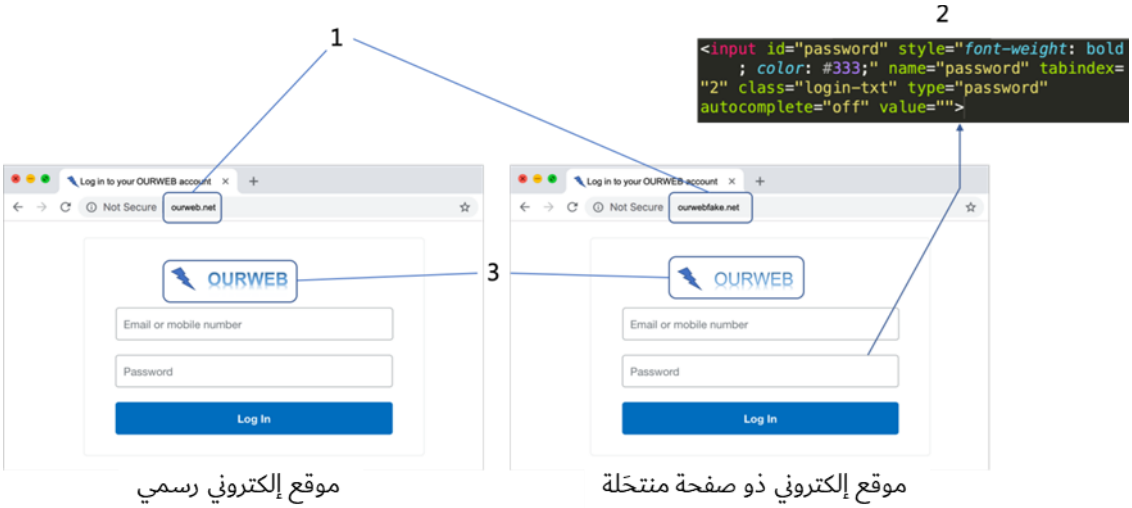
2) إذا أشار عنوان URL إلى موقع إلكتروني معروف، ينبغي اتخاذ تدابير الحماية المضادة للتعامل مع الطلب أو الرسالة.

3) إذا أشار عنوان URL إلى موقع إلكتروني مجهول، ينبغي اتخاذ تدابير تعرف الهوية المضادة من أجل تحديد نمط الموقع الإلكتروني.

4) إذا أشارت نتيجة تدابير تعرف الهوية المضادة إلى موقع إلكتروني ذي صفة منتحَلة، ينبغي اتخاذ تدابير وقائية مضادة لحماية المستعمل من النفاذ إلى الموقع الإلكتروني.

التذييل I
مثال على آلية مكافحة المواقع الإلكترونية ذات الصفة المنتحَلة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)



الشكل I-1 – مثال على موقع إلكتروني وموقع إلكتروني ذي صفة منتحَلة

لنفترض أن هناك موقع إلكتروني معروف يدعى "OURWEB" اسم ميدانه "ourweb.net". ويحاول دخيل إنشاء موقع إلكتروني ذي صفة منتحَلة اسم ميدانه "ourwebfake.net". ولنفترض أن المشغِّل يجهل اسم ميدان الموقع الإلكتروني ذي الصفة المنتحَلة، وحينما يطلب الكثير من المستعملين الموقع الإلكتروني ذي الصفة المنتحَلة، يصبح هذا الموقع الإلكتروني موقعاً إلكترونياً مجهولاً ورائجاً. عندئذ ينبغي التعامل مع الموقع الإلكتروني بتدابير التعرّف المضادة. وعلى النحو المبين في الشكل I.1، هناك ثلاثة تدابير مضادة للتعرف على ذي الصفة المنتحَلة.

1) يتشابه اسما ميدان الموقعين الإلكترونيين. ويُفترض أن درجة تقييم التشابه تساوي 0,8، وهو ما يقابل نسبة الحروف المشتركة.

2) يوجد دخل بيانات اعتماد، في الموقع الإلكتروني ذي الصفة المنتحَلة، يمكن التعرف عليه من شفرة المصدر. ودرجة تقييم دخل الاعتماد هي 1.

3) شعار الموقع الإلكتروني ذي الصفة المنتحَلة يشابه شعار الموقع الإلكتروني الرسمي. لنفترض أن درجة تقييم التشابه تساوي 0,9 وهي نسبة معرفات الهوية الوصفية المرئية المشتركة مثل معرف SIFT الوصفي.

4) لنفترض أن درجات تقييم التدابير المضادة الأخرى صفرٌ.

عندئذ يمكننا تشكيل متجه درجة تقييم [0.8,0.9,0,1,0,0]. وأول قيمة في المتجه هي درجة تقييم تشابه اسمي الميدان. والقيمة الثانية هي درجة تقييم التشابه في الشعار. وأما درجة التقييم الرابعة فهي درجة تقييم مدخلات الاعتماد. ويمكن أن يكون هذا المتجه دخلاً في مصنف آلة متجه الدعم (SVM) للحصول على النتيجة. وإذا بينت النتيجة موقعاً إلكترونياً ذا صفة منتحَلة، يصار إلى التعامل معه بتدابير وقائية مضادة لحماية المستعملين من النفاذ إلى الموقع الإلكتروني. فعلى سبيل المثال، تنبغي إضافة اسم ميدان الموقع الإلكتروني إلى قائمة الحظر في مسيِّرات شبكة المشغلين.

التذييل II
أمثلة على التدابير التقنية

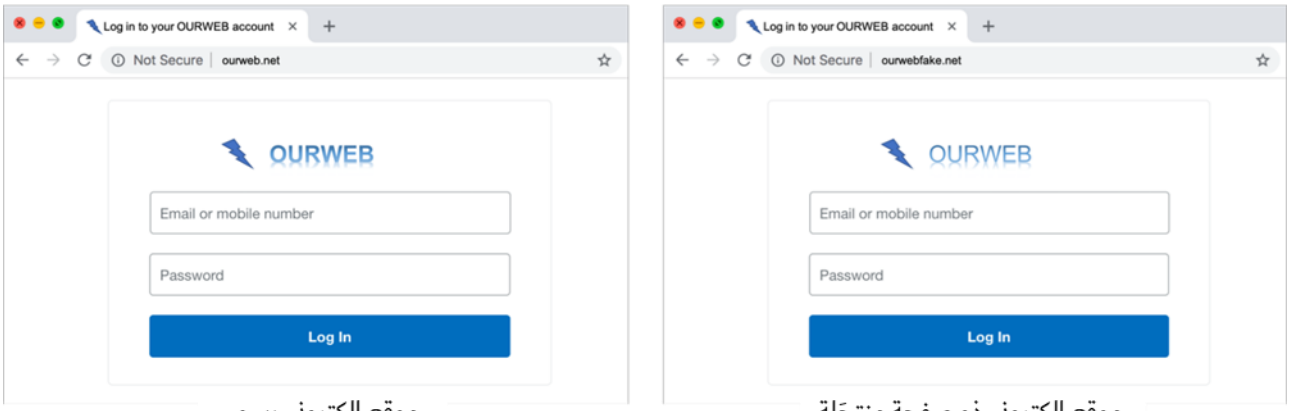
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

المثال 1.II: مقارنة أسماء الميادين المتشابهة

لنفترض أن اسم الميدان الرسمي هو "abc123.cn". ويستعمل الموقع الإلكتروني ذو الصفة المنتحَلة اسم "abc123cn.org" كاسم ميدان. وبحساب تشابه Jaccard (يقسَّم مقاس تقاطع مجموعتين من حروف اسم الميدان على مقاس اتحادهما) بين اسمي الميدانين، نحصل على درجة التشابه 8/11 = 0,73.

المثال 2.II: كشف الشعار الرسمي

على النحو المبين في الشكل 1.II، يظهر الموقع الإلكتروني الرسمي OURWEB على اليسار، ويُبين الموقع الإلكتروني المقابل ذو الصفة المنتحَلة على اليمين. لنفترض أن الشعار الرسمي لموقع OURWEB قد أضيف إلى قاعدة بيانات الشعارات. ويتشابه شعار الموقع الإلكتروني ذي الصفة المنتحَلة إلى حد كبير مع الشعار الرسمي لموقع OURWEB. وباستعمال خوارزمية مقارنة التشابه، يمكن تحديد درجة تشابه (0,9، على سبيل المثال).



الشكل 1.II – الموقع الإلكتروني ذو الصفة المنتحَلة مع الشعار الرسمي

المثال 3.II: كشف تمويه الشفرة

تستعمل بعض المواقع الإلكترونية لغة JavaScript لإنتاج محتوى ويب دينامياً، وتستعمل خدمة التمويه المتاحة عبر الإنترنت (مثل https://obfuscator.io/) لتجفير شفرة JavaScript.

على النحو الموضح في الشكل 2.II، تختلف الشفرة المموهة كثيراً عن الشفرة العادية. ويمكن استعمال نموذج تصنيف نص قائم على الذكاء الاصطناعي للتنبؤ بما إذا كانت الشفرة مموهة. وتقدم الخوارزمية قيمة احتمال التنبؤ لشفرة المصدر (0,7 مثلاً).

الشكل 2.II – أمثلة على التمويه لشفرة JavaScript

المثال 4.II: كشف مدخلات الاعتماد

على النحو الموضح في الشكل 1.II، يخدع الموقع الإلكتروني ذو الصفة المنتحَلة المستعملين لحملهم على إدخال بيانات الاعتماد. ويمكن حساب درجة تقييم الموقع الإلكتروني بالتحقق مما إذا كانت هناك استمارة على الصفحة لإدخال بيانات الاعتماد. وإذا كانت هناك استمارة لإدخال بيانات الاعتماد، تُسنّد درجة 1 إلى الموقع، وإلا تُسنّد إليه درجة 0.

المثال 5.II: خدمة الأمن من طرف ثالث

يمكن لخدمات الاستعلام عبر محدد موقع الموارد الموحد (URL) المتاحة على الإنترنت من بائعي الخدمات الأمنية (مثل https://www.urlvoid.com/) أن تساعد في تحديد ما إذا كان الموقع الإلكتروني موقعاً إلكترونياً ذا صفة منتحَلة. وإذا صُنف الموقع الإلكتروني المكتشف على أنه موقع إلكتروني ذو صفة منتحَلة، فإن درجة التقييم تساوي 1، وإلا فإنها تساوي 0.

المثال 6.II: تحليل الوصلة

في الشكل 1.I، قد يشير الشعار إلى موارد الموقع الإلكتروني الرسمي OURWEB. ويمكن أن يحدد تحليل الوصلة أن مورد الصورة من موقعنا، ourweb.net، (ليس موقعنا المزيف، ourwebfake.net). وفي حال وجود وصلات إلى موارد الصور الرسمية في الموقع الإلكتروني، يمكن إسناد درجة التقييم 1، وإلا يمكن إسناد درجة التقييم 0.

المثال 7.II: تجميع النتائج

تجمَّع درجات تقييم الأساليب المختلفة للمواقع الإلكترونية ذات الصفة المنتحَلة في متجه. ويرد في الجدول 1.II مثال على إسناد درجات تقييم إلى موقع إلكتروني. ويشكل العمود الثاني من الجدول متجه درجة التقييم. ويمكن إدخال هذا المتجه في المصنِّف لتحديد ما إذا كان الموقع الإلكتروني موقعاً إلكترونياً ذا صفة منتحَلة.

الجدول 1.II – مثال على إسناد درجات تقييم إلى موقع إلكتروني

أساليب تعرف الهوية	درجة التقييم
مقارنة تشابه اسم الميدان	0,8
كشف الشعار الرسمي	0,9
كشف تمويه الشفرة	0,7
كشف مدخلات الاعتماد	1
خدمة الأمن من طرف ثالث	0
تحليل الوصلة	1

الجدول 2.II – التقابل بين أساليب تعرف الهوية
وخصائص المواقع الإلكترونية ذات الصفة المنتحَلة

أساليب تعرف الهوية	الخصائص
مقارنة تشابه اسم الميدان	تشابه اسم الميدان
كشف الشعار الرسمي	تشابه مرئي استعارة عناصر مرئية
كشف تمويه الشفرة	تمويه شفرة المصدر
كشف مدخلات الاعتماد	مدخلات الاعتماد
خدمة الأمن من طرف ثالث	
تحليل الوصلة	التوصيل بمواقع إلكترونية معروفة جيداً

بيبليوغرافيا

[b-ITU-T X.1126] Recommendation ITU-T X.1126 (2017), *Guidelines on mitigating the negative effects of infected terminals in mobile networks*.

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-SVM] Nature biotechnology, 2006, 24(12) 1565-1567*: What is a support vector machine?*

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2022