الحلول الفنية الحالية لمكافحة الرسائل الإلكترونية الاقتحامية

مقدمة:

الرسائل الإلكترونية الاقتحامية هي أكثر الرسائل الاقتحامية شيوعاً، ويتم حالياً مكافحتها من خلال حلول متنوعة على الصعيد الفني لمكافحة الرسائل الاقتحامية. إن الحلول الرئيسية لمكافحة الرسائل الإلكترونية الاقتحامية مستمدة من المنتجات المتخصصة التي تطرح لهذا الغرض والممارسات المقدمة في هذه الوثيقة.

مرشحات البريد الإلكتروني:

يمكن تصنيف المرشحات الحالية لفرز البريد الإلكتروني على أنها مرشحات آلية وغير آلية. وقد صممت المرشحات غير الآلية للعمل من خلال الإعدادات اليدوية لمكافحة الرسائل الاقتحامية، وهي ليست قادرة على التعلم الذاتي للأنماط المختلفة من الرسائل الاقتحامية، كما أنه لا يمكنها تطوير نفسها لتمييز الخواص المتجددة للرسائل الإلكترونية الاقتحامية. وبالمقابل، تعتبر مرشحات الفرز الآلية ذكية وقادرة على التعلم من الأنماط المختلفة للرسائل الاقتحامية ومن ثم مكافحتها. ومن هنا، فهي مصممة للإستجابة للخواص المتطورة والمتجددة للرسائل الإلكترونية الاقتحامية. وفيما يلي الأنواع الرئيسية الحالية لمرشحات الرسائل الإلكترونية:

- **مرشحات القوائم السوداء / القوائم البيضاء**

تُصنَّف مرشحات القوائم البيضاء / القوائم السوداء بأنها مرشحات فرز غير آلية. إن مرشحات القوائم السوداء مبنية على قائمة (قائمة سوداء) من العناوين البريدية الإلكترونية التي تعتبر مصدراً للرسائل الإلكترونية الاقتحامية. وعليه، فإن الرسائل الإلكترونية المرسلة من هذه العناوين تفرز من قبل نظام الترشيح. ومن الناحية الأخرى، فإن مرشحات القوائم البيضاء مبنية على (قائمة بيضاء) من العناوين البريدية الإلكترونية والتي تعتبر مصادر للرسائل المشروعة. وبالتالي تسمح المرشحات فقط بمرور الرسائل الإلكترونية الواردة من تلك العناوين، أما الأخرى فتفرز من قبل نظام الترشيح. وجميع القوائم البيضاء والسوداء يمكن تهيأتها يدوياً أو توضع للتهيئة الأوتوماتيكية . في التهيئة اليدوية، تتم إضافة مرسلي الرسائل المدرجين سواءً على القوائم البيضاء أو على السوداء من خلال إضافة عناوينهم الإلكترونية إلى القائمة المعينة. أما في التهيئية الأوتوماتيكية، فيضاف مرسلو الرسائل الإلكترونية إلى القائمة السوداء أو البيضاء أتوماتيكياً إذا كانت عناوينهم مطابقة لخوص معينة .

المزايا: تعتبر مرشحات القوائم السوداء أو البيضاء للرسائل الإلكترونية بسيطة وسريعة وسهلة التطبيق.

المحددات: السلبية الرئيسية لمرشحات القوائم السوداء أو القوائم البيضاء الخاصة بالرسائل الإلكترونية هي أنه يمكن التحايل عليها بالتغيير المخادع في عنوان البريد الإلكتروني للمرسل.

- **مرشحات البريد الإلكتروني الاستكشافية**

تصنف مرشحات البريد الإلكتروني الاستكشافية (Heuristics) على أنها مرشحات غير آلية تعمل بناءً على قوانين مسبقة التعريف. وهذه القوانين يمكن أن تطبق على ترويسة الرسالة لإلكترونية (Header) وعلى متن الرسالة (Body). إن القوانين المطبقة على الترويسات تحدد خصائص معينة للرسائل الإلكترونية الاقتحامية في ترويساتها مثل الأنماط التي قد تعرف من خلالها العناوين والتواريخ والمواضيع غير الصحيحة للبريد الإلكتروني. وبالإضافة إلى ذلك، يمكن تعديل هذه القوانين لتشمل حقول أخرى في ترويسة الرسالة. أما القوانين المطبقة على متن الرسالة الإلكترونية فتتعرف على مقاطع من الرسائل الإلكترونية الاقتحامية من خلال تعبيرات منتظمة. وهذه تعبيرات المنتظمة يمكن تعديلها لتشمل التعبيرات التي تدور حولها كلمات الرسائل الإلكترونية الاقتحامية. وتعطى الرسائل الإلكترونية نقاطاً بناءً على عدد القوانين التي تتطابق معها، فإذا حصلت الرسالة الإلكترونية على نقاط أعلى من النقاط المحددة مسبقاً، فإنها ستصنف على أنها رسالة إلكترونية اقتحامية وتفرز بواسطة نظام الترشيح.

المزايا: تعتبر مرشحات البريد الإلكتروني الاستكشافية بسيطة وعالية الدقة من حيث قوانين التعبيرات المنتظمة ومن حيث سرعة التنفيذ القصوى.

المحددات: لا تمتلك مرشحات البريد الإلكتروني الاستكشافية إمكانات فرز ذكية (لا تتكيف مع الخواص المتطورة والمتجددة للرسائل الإلكترونية الاقتحامية)، وتحتاج إلى تدخل مدير النظام لتحديث مجموعات القوانين أو لتحميلها بشكل منتظم، كما أنها قد تولد معدلات عالية من الإيجابيات الزائفة مع ازدياد حساسيتها لمعايير وتعابيرمعينة.

- **مرشحات الرسائل الإلكترونية لنصوص HTML المخفية**

تعتبر مرشحات الرسائل الإلكترونية المحتوية على نصوص (HTML) مخفية من ضمن مرشحات الفرز غير الآلية. وهي مبنية على مرشحات الرسائل الإلكترونية الاستكشافية Heuristic. وتقوم بعملية مسح الرسائل الإلكترونية لمعرفة فيما إذا كانت الرسائل الإلكترونية تحتوي على أي كود نشط مخفي مكتوب بلغة HTML. إن العديد من برامج البريد الإلكتروني تدعم إنشاء وعرض الرسائل بصغية HTML، وقد يتضمن المحتوى المكتوب بلغة HTML في الرسائل الإلكترونية وصلات لاستعادة محتوى موجود على الشبكة العنكبوتية، مثل صور أو مواقع إلكترونية تحتوي على مضمون اقتحامي، وعلى نصوص برمجية ورموز تدل المقتحمين على أن الرسالة الإلكترونية قد تمت قراءتها وأن حساب الرسائل الإلكترونية نشطاً، وعلى رموز برمجية تستخدم لتحميل دودات خبيثة و/أو نصوص برمجية معينة لتنفيذ كودات خبيثة. وحيث أن العديد من مرشحات الرسائل الإلكترونية تصنف الرسائل الإلكترونية بناءً على المحتوى، فإن المقتحمين يميلون إلى استعمال مثل هذه الأساليب لتجنب هذه المرشحات. إن مرشح الرسائل الإلكترونية المحتوية على نصوص HTML مخفية يمنع استلام وعرض الرسائل الإلكترونية التي تحتوي على كود HTML خبيث. وبذلك، فإن مرشحات الرسائل الإلكترونية ذات النصوص المنشطة المخفية HTML تحمي أجهزة المستخدم من المحتوى الخبيث الذي قد يكون مخفياً في الرسائل الإلكترونية الاقتحامية وفي الرسائل المشروعة. ويمكن كذلك لمرشحات حماية حاسبات المستخدمين أن تحمي أجهزتهم كي لا تصبح مصدراً للفيروسات دون علمهم بذلك.

المزايا: تعتبر مرشحات الرسائل الإلكترونية ذات النصوص HTML المنشطة المخفية فعالة جداً في منع استلام أو عرض الرسائل الإلكترونية التي تحتوي على نصوص HTML منشطة مخفية أو رموز برمجة ويب مثل نصوص جافا. وعليه، فإن هذه المرشحات تحمي أجهزة المستقبل من المحتويات الاقتحامية وكذلك من المحتويات الأخرى التي قد تعتبر خبيثة. إن العديد من برامج خوادم البريد الإلكتروني توفر خياراً لتعطيل عرض الرسائل الإلكترونية التي تأتي بصيغة HTML.

المحددات: قد تمنع مرشحات الرسائل الإلكترونية المحتوية على نصوص HTML مخفية استلام أو عرض الرسائل الإلكترونية الصحيحة مثل الرسائل الإلكترونية القادمة على شكل نشرات إخبارية لأن العديد من الرسائل الإلكترونية التي تحمل نشرات إخبارية ترسل بحيث يتم عرضها بصيغة HTML، أو قد تحتوي على روابط لأستعادة صور من الشبكة العنكبوتية.

- **مرشحات تواقيع الرسائل الإلكترونية – Signatures mail Filters**

تصنف مرشحات تواقيع الرسائل الإلكترونية كمرشحات غير آلية. وهذه المرشحات تم تطويرها بناءً على المفاهيم الرياضية لما يعرف بوظائف الدمج العشوائي (Hash Functions). وهذه الوظائف مصممة بحيث تكون مقاومة جداً للتصادم وبحيث تقدم مخرجات واضحة لمدخلاتها. وتحافظ مرشحات تواقيع الرسائل الإلكترونية على قائمة (قاعدة بيانات) من القيم العشوائية للرسائل الإلكترونية الاقتحامية المعروفة. يعمل نظام ترشيح تواقيع الرسائل الإلكترونية كالتالي: توليد قيم عشوائية للرسالة الإلكترونية الواردة ومقارنته بالقيم العشوائية المعروفة للرسائل الإلكترونية الاقتحامية، وعند مطابقتها بشكل ناجح، فإن الرسالة الإلكترونية تصنف على أنها رسالة اقتحامية ويتم منعها من المرور، ولكن ليس بمقدور نظام الترشيح التعرف على القيم العشوائية الأخرى للرسائل الإلكترونية الاقتحامية الجديدة، حيث يجب إدخال قائمة الدمج العشوائي للرسائل الإلكترونية الاقتحامية في نظام الترشيح. يستلم نظام الترشيح قوائم الدمج العشوائي المحدثة للرسائل الإلكترونية الاقتحامية من خادم توزيع التواقيع. ويتطلب الاتصال بخادم توزيع التواقيع وتخزين قائمة القيم العشوائية تدابير أمنية مشددة.

المزايا: بناءً على المقاومة الشديدة التي تبديها وظائف الدمج العشوائي ضد التصادم، تولد مرشحات تواقيع الرسائل الإلكترونية معدلات منخفضة من الإيجابيات الزائفة.

المحددات: ليس لمرشحات تواقيع الرسائل الإلكترونية أية إمكانات فرز ذكية (لا تستطيع تحديد القيم العشوائية الخاصة بالرسائل الإلكترونية الاقتحامية الجديدة)، وتوجب تدخل مدير النظام لتحديث قائمة الدمج العشوائي للرسائل الإلكترونية الاقتحامية، أو البحث عن القائمة وجلبها بشكل منتظم من خادم توزيع التواقيع، وفشل آلية الترشيح في التعرف على الرسائل الإلكترونية المعروفة سابقاً عندما يتم تعديلها، حيث إن تعديل الرسائل الإلكترونية الاقتحامية المعروفة مسبقاً يولد قيم عشوائية مختلفة عما تعود عليه نظام الترشيح، وبالتالي يمكن للرسالة الإلكترونية الاقتحامية المعدلة اختراق ذلك نظام.

- **مرشحات بيسيان(Bayesian) للرسائل الإلكترونية**

تصنف مرشحات بيسيان على أنها مرشحات فرز آلية، وهي المرشحات الآلية الوحيدة المطبقة في الوقت الحاضر. وهذه المرشحات قائمة على حساب الاحتمالات لمجموعة من الرموز. وتعرف الرموز هنا بأنها كلمات مأخوذة من اللغة الطبيعية الموجودة في مضمون الرسالة الإلكترونية. وتعطى الرموز نقاطاً احتمالية بناءً على سجلات ظهورها السابق في الرسائل

الإلكترونية الاقتحامية. ويستطيع مستخدمو الرسائل الإلكترونية تعديل المرشحات لتصنيف (ترشيح) الرسائل الإلكترونية المستلمة حسب متطلباتهم. وعليه، فإن مرشحات بيسيان للرسائل الإلكترونية يمكن أن يتم تعديلها بشكل مختلف من قبل المستخدمين المختلفين، الذين يستطيعون أيضاً تعديل قوانينهم بناءً على المعلومات الواردة من المستخدمين، بحيث يتم ترميز الرسائل الإلكترونية الواردة عند استلامها، ويتم بعد ذلك مطابقة كل رمز مع سجله المعروف بغرض حساب الاحتمالات. ثم يتم دمج جميع الاحتمالات بناءً على قانون بيس الرياضي. وتشير الاحتمالية العالية إلى إمكانية كبيرة لكون الرسالة الإلكترونية رسالة اقتحامية. وبناءً على مجموع قيمة الاحتمالات، يتم ترشيح الرسائل الإلكترونية الاقتحامية. إن أنظمة بيسيان لترشيح الرسائل الإلكترونية تلائم بشكل كبير جانب برنامج البريد الإلكتروني أكثر مما تلائم جانب الخادم، وذلك بسبب وجود خاصية تعديل المرشح. إن إعداد أنظمة ترشيح بيسيان على جانب الخادم فقط من شأنه منع مستخدمي الرسائل الإلكترونية من الاستفادة من خاصية تعديل المرشح إلا إذا سمح بها على الخادم.

المزايا: لمرشحات بيسيان المستخدمة للرسائل الإلكترونية قدرات ترشيح ذكية (هي مرشحات آلية) فضلاً عن قدرات الترشيح الواسعة القائمة على تحليل المضمون (المحتوى). وهذه المرشحات تمكن المستخدمين من تعديلها بناءً على نوع الرسائل الاقتحامية التي يستلمونها. بالاضافةإلى ذلك، تعتبر مرشحات بيسيان المستخدمة في الرسائل الإلكترونية عالية الدقة.

المحددات: تصاغ الرموز في مرشحات بيسيان للرسائل الإلكترونية من كلمات مفردة. وبالتالي فإن الكلمات المركبة قد تستطيع اختراق نظام الكشف. كما تفتقر هذه المرشحات إلى القدرة على تحليل الكلمات المتتابعة والتي تشكل مقاطع اقتحامية شائعة في مضامين الرسائل الإلكترونية، مثل مقطع special offer والذي يعني عرض خاص، لأن كل كلمة تحلل بشكل منفصل. وغالباً ما تتم ملاحظة كلمات متتابعة أو كلمات مركبة في الرسائل الإلكترونية الاقتحامية. إن الإخفاق في التعرف على مثل هذه الكلمات يحد من القدرة على اكتشاف مثل هذه الانواع من الرسائل الإلكترونية الاقتحامية عندما تقوم آلية الترشيح بوظيفتها. غير أنه تتوفر حالياً بعض الخوارزميات algorithms التي تساعد في تحليل تبديل ترتيب الكلمات المفردة والكلمات المتتابعة والكلمات التي تظهر بعيدة عن بعضها البعض.

- **مرشحات تحليل حركة مرور الرسائل الإلكترونية**

تُصنف مرشحات تحليل حركة مرور الرسائل الإلكترونية على أنها مرشحات غير آلية تستخدم ملفات التسجيل الخاصة بخادم برتوكول لتحويل البريد الإلكتروني (SMTP) للكشف عن الحالات الشاذة في حركة مرور الرسائل الإلكترونية. تتصف حركة مرور الرسائل الإلكترونية الاقتحامية بصفات معينة: مثل عملية وصولها (فيما إذا كانت رسالة أعيد إرسالها)، وحجمها، وعدد المستقبلين لكل رسالة (عندما يفيض البريد الإلكتروني بالرسائل) وكونها عامة أو محلية مؤقته بين المستقبلين. وبناءً على الحالات الشاذة في حركة مرور الرسائل الإلكترونية يتم الكشف عن الرسائل الإلكترونية الاقتحامية وترشيحها.

المزايا: تعتبر مرشحات تحليل حركة مرور الرسائل الإلكترونية معقدة نوعاً ما، ولكن تبدو آلية الترشيح التي تستخدمها سريعة وموسعة بالمقارنة مع التحليل الفعلي لمحتويات الرسائل الإلكترونية لأنها تحلل فقط سجلات بروتوكول تحويل الرسائل الإلكترونية البسيطة SMTP.

المحددات: ليس لمرشحات تحليل حركة مرور الرسائل الإلكترونية قدرات فرز ذكية (أي أنها لا تتكيف مع الخصائص الجديدة والمتطورة للرسائل الاقتحامية). وبناءً على الوضع الراهن، لا تستطيع هذه المرشحات تحديد الخاصية الأكثر ملائمة لنوع محدد من الرسائل الإلكترونية من بين الخصائص المطبقة على حركة مرور الرسائل الإلكترونية.

التحقق من المصدر

إن التحقق من مصدر الرسالة الإلكترونية أو مرسلها يزيد من موثوقية الرسائل الإلكترونية المستلمة ويضع الرسائل غير المعروفة تحت شبهة كونها اقتحامية. هناك صفة عامة بين مرسلي الرسائل الإلكترونية الاقتحامية وهي أنهم يزورون هوياتهم لجعل عملية تتبع مصدر الرسائل الإلكترونية الاقتحامية صعبة. وبالإضافة إلى استخدام اساساليب متقدمة مثل تزوير ترويسة البريد الإلكتروني واستخدام اتصالات الوكيل (proxy) المفتوحة والحواسيب المسيطر عليها والمستخدمة كحاضنة لانطلاق الرسائل الاقتحامية zombie ، فإن مرسلي الرسائل الإلكترونية الاقتحامية يستخدمون أساليب متقدمة لتزوير ترويسات الرسائل الإلكترونية. وبناءً على ذلك ، يتم استخدام أسليب مختلفة لتوثيق مصدر الرسائل الإلكترونية. وفيما يلي النماذج الرئيسية الرئيسية المستخدمة حالياً في المنتجات والممارسات الخاصة بهذه الصناعة.

إطار سياسة المرسل/ إطار هوية المرسل

إن إطار سياسة المرسل (SPF) أو إطار هوية المرسل هو امتداد لبرتوكول تحويل الرسائل الإلكترونية البسيطة (SMTP) يهدف إلى تمكين القيام بتوثيق مصدر الرسالة الإلكترونية. وهذا الإطار يسمح لخوادم الرسائل الإلكترونية بتحديد العناوين المزيفة في حقل " ِمن أو المرسل" في ترويسة الرسالة الإلكترونية وذلك من خلال حماية "مسار الإعادة". إن عملية تزوير حقل " ِمن أو المرسل" في ترويسة الرسالة الإلكترونية ممارسة شائعة يقوم بها مرسلو الرسائل الإلكترونية الاقتحامية لتجنب كشف هوياتهم الحقيقية عند إرسالهم رسائلهم الإلكترونية الاقتحامية التي تحمل أسماء المرسلين المعروفة. وهذا يتم باستخدام القصور الموجود في التنفيذ العادي لمواصفات برتوكول تحويل الرسائل الإلكترونية البسيطة (SMTP). تسمح مواصفات هذا البرتوكول لخوادم الرسائل الإلكترونية بإرسال الرسائل الإلكترونية بدون الإفصاح المؤكد عن هوية المرسل. لقد عالج إطار عمل نظام المرسل (SPF) أو هوية المرسل هذا القصور وذلك بالسماح لمالكي أسماء النطاقات (DNS) باستخدام سجلات على نظام اسم النطاق (DNS) (سجل النص) لتحديد خوادم الرسائل الإلكترونية لأسماء نطاقاتهم المسموح لها ببث الرسائل الإلكترونية، وخاصة السجلات التي تحتوي على عناوين بروتوكولات الانترنت الخاصة بخوادم الرسائل الإلكترونية النظامية وأسماء نطاقاتهم المماثلة والتي يتم تحديدها في " مسار الإعادة".

يستطيع مرسلو الرسائل الإلكترونية الاقتحامية تزوير حقل " ِمن أو المرسل"، ولكن ليس بمقدورهم تزوير حقل "مسار الإعادة" لأنه مؤمن من قبل بروتوكول إطار عمل نظام المرسل SPF. وهكذا، يكون بإمكان خوادم مستلمي الرسائل الإلكترونية الاستفسار من خادم على نظام اسم النطاق (DNS) عن موقع خادم مصدر الرسالة ومقارنة كل من "مسار الإعادة" وعنوان بروتوكول الإنترنت المحدد لخادم مصدر الرسالة الإلكترونية مع تلك المسجلة في سجل على نظام اسم النطاق (DNS). وينجم عن ذلك مرور الرسالة إذا صحت المطابقة، أو ينجم فشل المرور إذا فشلت المطابقة. وهكذا فإن خوادم الرسائل الإلكترونية التي تفشل في عملية التحقق من "إطارعمل نظام المرسل أو هوية المرسل تعتبر مصادر للرسائل الاقتحامية ويتم حجبها. وهناك مصدراً آخر للحيل التي يمارسها مرسلوا الرسائل الاقتحامية في حالة عدم استخدام بروتوكول SPF/هوية المرسل، فهم قد يقوموا بتزويير حقل "مسار الإعادة" ووضع عناوين أشخاص آخرين بحيث يضايقونهم بالرسائل الإلكترونية المرتدة أو الإجابة على رسائل لم تصدر عنهم ورسائل تدل على أخطاء. غير أن استخدام بروتوكول SPF/هوية المرسل لن يسمح بحدوث مثل هذه المشاكل أساساً.

إن تسمية بروتوكول SPF/هوية المرسل بهذا الإسم جاءت بناءً على الآلية التشغيلية التي يقوم بها. فهو يضع القوانين للرسائل الإلكترونية الصادرة من موقع الإنترنت . ومع أن هوية المصدر تعمل بشكل مماثل لإطار سياسة المرسل أو هوية المرسل إلا أنها تعتبر بروتوكولاً مختلفاً لأن كل منهما مختلف من حيث التطبيق. ان إطار سياسة المرسل أو هوية المرسل مختلفان من حيث كيفية التحقق من الصحة ومن ناحية طبقة نظام البريد الإلكتروني الذي يتعاملان معها.

المزايا: يضع بروتوكول سياسة المرسل SPF/هوية المرسل نظاماً فعالاً للتحقق من صحة خوادم مصادر الرسائل الإلكترونية، وذلك بإدخال تحسينات على بروتوكول تحويل الرسائل الإلكترونية البسيطة (SMTP). وبالتالي، يتم حجب الأجهزة المسيطر عليها لتصبح مصدراً للرسائل الاقتحامية والمرحلات المفتوحة واتصالات الوكيل المفتوحة. إن حجب الرسائل الإلكترونية هي خاصية خوادم الرسائل الإلكترونية التي تنفذ بروتوكول سياسة المرسل SPF/هوية المرسل. وبالتالي فهي لا تحتاج إلى تجهيز برامج أو أجهزة إضافية. ويوفر بروتوكول سياسة المرسل SPF/هوية المرسل كذلك وسيلة آمنة لمكافحة الرسائل الاقتحامية، وذلك من خلال عدم استلام (حجب) الرسائل من الخوادم التي ترسل رسائل إلكترونية اقتحامية في المقام الأول. من الممكن استخدام بروتوكول سياسة المرسل SPF/هوية المرسل كأسلوب للترشيح لمرحلة ما قبل إرسال الرسائل.

المحددات: مع أن بروتوكول سياسة المرسل SPF/هوية المرسل قد تم تنفيذه واستخدامه من قبل العديد من متبادلي الرسائل الإلكترونية، إلا أنه ما زال مسودة إنترنت(RFC) موجودة على طلب إبداء الملاحظات. وعليه ، فإن بروتوكول سياسة المرسل SPF/هوية المرسل غير ملزم للخوادم لكي تقوم باتباعه. وقد يرغب بعض مستخدمي الرسائل الإلكترونية في تحديد عناوين مختلفة لإعادة إرسال رسائلهم الإلكترونية. وحسب الوضع، القائم فإن هذا غير ممكن عند استخدام بروتوكول سياسة المرسل SPF/هوية المرسل لإنه يربط بشدة بين الجهة المرسلة و حقل "مسار الإعادة".

قد يعتبر "نظام هوية المرسل" الرسائل الإلكترونية المحولة كرسائل اقتحامية إذا كان عنوان برتوكول الإنترنت المحول غير مطابق لأسم النطاق لمنشيء الرسالة. وحيث أن هوية المرسل تتناقض بعض الشيء مع المواصفات الحالية فقد تم عمل التوصيات لوقف العمل بها كمسودة إنترنت إلى أن يتم ايجاد حل لهذا التناقض. وعلى أية حال فهي ما زالت تحت الدراسة حتى الآن وموجودة على طلب إبداء الملاحظات على المقاييس الموضوعة، وهي مطبقة على العديد من المنتجات.

- **البريد الإلكتروني المعرف بمتاح النطاق**

البريد الإلكتروني المعرف بمفتاح النطاق DKIM يسمح بتوثيف مصدر الرسالة الإلكترونية بشكل مستقل عن بروتوكول تحويل الرسائل الالكترونية البسيطة (SMTP)، ويسمح بتتبع مصادر الرسائل الإلكترونية المزورة وذلك بالتحقق من

الموقع المرسل للرسالة الإلكترونية والتحقق من سلامة الرسالة. وهذا يتم تحقيقه من خلال التواقيع الرقمية والتي هي وظيفة مشهورة لشيفرة المفتاح العام Public key Cryptography. سيكون لكل نطاق مفتاحان (عام وخاص) للتوقيع، ويقوم بعملية التوقيع خادم البريد الإلكتروني للمرسل (MTA) مستخدماً المفتاح الخاص للنطاق المرسل. ويحتاج كل من خادم البريد المرسل وخادم البريد المستقبل إلى تطبيق (KDIM). هذا علما بأن البريد الإلكتروني المعرف بمفتاح النطاق DKIM يحتاج بأن يكون لكل نطاق سجل لنظام تسمية النطاق (DNS) بحيث يقوم هذا السجل بنشر المفتاح العام للنطاق إضافة إلى الخواص الأخرى، ويتطلب أيضاً أن تقوم خوادم البريد بالحفاظ على سرية المفتاح الخاص لهذه النطاقات. أما الآلية التي تعمل بها في كالتالي: يقوم خادم البريد المرسل بتوقيع محتوى الرسالة الصادرة رقمياً باستعمال SHA-1 وذلك كإحدى وظائف الدمج العشوائي وباستعمال RSA كخوارزمية تشفير، ويربط التوقيع (توقيع مفتاح النطاق) بترويسة الرسالة الالكترونية، ثم يقوم خادم البريد المرسل بإرسال الرسالة الإلكترونية، وعند استلام الرسالة الإلكترونية، يقوم خادم البريد المستقبل باستخلاص اسم النطاق من حقل الترويسة "مِن / المرسل" ويطلب من خادم نظام تسمية النطاق لموقع المرسل استرجاع مفتاحه العام. وإذا لم يتم العثور على المفتاح العام، يستطيع خادم مستقبل الرسالة الإلكترونية الحكم بأن مصدر الرسالة الإلكترونية مزوراً وأن الرسالة اقتحامية، وعليه يتم التخلص منها. وعلى أية حال، عندما يتم الإسترجاع الناجح للمفتاح العام، فإن خادم مستقبل الرسالة الإلكترونية يستطيع التحقق من التوقيع الرقمي. وعند نجاح التحقق من الصحة، فإن خادم مستقبل الرسالة الإلكترونية سيثق بمصدر الرسالة على أنه خادم رسائل إلكترونية شرعي. وعند الإخفاق في التحقق من الصحة، فإن خادم مستلم الرسالة الإلكترونية قد يعتبر مصدرها اقتحاميا ويتخلص منها. كما أن نجاح عملية التحقق من الصحة ستضمن عدم المساس بمحتوى الرسالة الإلكترونية .

الفوائد: تعتبر أسلوب البريد الإلكتروني المعرف بمفتاح النطاق DKIM خطة توثيق فعالة للتحقق من شرعية مصدر الرسائل الإلكترونية وضمان صحة الرسالة. ويعد استخدام KDIM في التخلص من الرسائل الإلكترونية من ضمن الخواص الموجودة في خوادم البريد. وهكذا، فإن خوادم البريد لا تحتاج إلى إعدادات برمجية أو أجهزة أضافية لمكافحة الرسائل الاقتحامية. ويوفر KDIM أيضا وسيلة آمنة لمكافحة الرسائل الاقتحامية وذلك بالتخلص منها في المقام الاول. وبهذه الطريقة يمكن اسخدامه كأسلوب ترشيح لما قبل الإرسال. وتقوم مواصفات KDIM على نظام الترويسة الاختياري لطلب الإيضاح ٢٨٢٢ (RFC2822) وعلى سجلات نظام تسمية النطاق. ولذلك فهي متطابقة مع بروتوكولات البريد الإلكتروني القائمة حالياً.

المحددات: لا يشتمل أسلوب البريد الإلكتروني المعرف بمفتاح النطاق DKIM على ترويسة الرسالة الإلكترونية في توقيع مفتاح النطاق، ولذلك فإن تزوير "مسار الإعادة" لا يمكن الكشف عنه. ونتيجة لذلك فإن مرسلو الرسائل الاقتحامية قد يقوموا بتزوير حقل مسار الإعادة ووضع عناوين أشخاص آخرين حتى يتمكنوا من ازعاجهم بالرسائل المرتدة والإجابات غير المطلوبة ورسائل الأخطاء. بالإضافة لذلك، فإن تقنية المفاتيح العامة (PKI) هي تقنية باهظة الثمن، وعليه، فاستخدام هذا الإسلوب قد لا يكون مجدياً من حيث التكلفة.

التحدي والاستجابة

تقوم أنظمة التحدي والاستجابة على التفاعل بين الإنسان والنظام لتحديد فيما إذا كانت الرسالة من الرسائل الإلكترونية الاقتحامية. وتقوم هذه الانظمة بالتحقق من أن مرسل الرسالة الإلكترونية هو إنسان وليس نظام آلي معد لإرسال رسائل اقتحامية (Spamboot). تعمل هذه الأنظمة على خادم البريد لاعتراض الرسائل الواردة والتي يشتبه أنها اقتحامية. ومن ثم ترسل هذه الأنظمة تحدياً إلى المرسل لكي يرد عليها. إن المبدأ الذي تنضوي عليه هذه الأنظمة هو أن مرسلي الرسائل الاقتحامية لن يقوموا بالرد لأنهم يرسلون رسائل جماعية بالجملة، كما أن مرسلي الرسائل الاقتحامية لن يستلموا تحدياً إذا زوروعناوينهم الإلكترونية. وانطلاقاً من هذا المبدأ، يتم تصنيف الرسائل الإلكترونية على أنها اقتحامية ويتم ترشيحها والتخلص منها إذا لم تتم الاستجابة للتحدي. يتم تبادل التحديات والاستجابات على شكل رسائل إلكترونية .

الفوائد: إن أنظمة التحدي والاستجابة فعالة جداً في مكافحة الرسائل الإلكترونية الاقتحامية إذا أرسلت من مصادر خاصة بإرسال الرسائل الاقتحامية bots أو من قبل هوية مزورة.

المحددات: لا تمتلك أنظمة التحدي والاستجابة إمكانات ترشيح ذكية (لا تستجيب للسمات الحديثة والمتطورة للرسائل الاقتحامية) بالإضافة إلى ذلك، تعتبر غير مناسبة لمستخدمي الرسائل الإلكترونية لأنه يتوجب عليهم الاستجابة إلى التحديات لبعض الرسائل الإلكترونية المرسلة.

البحث العكسي في نظام أسماء النطاقات (rDNS)

قد يساعد البحث العكسي في نظام أسماء النطاقات (DNS) في تحديد الرسائل الإلكترونية الاقتحامية وحجب الرسائل الواردة من خوادم الرسائل التي ترسل رسائل إلكترونية اقتحامية. يقوم البحث في أسماء النطاقات بوظيفة عكسية في نظام تسمية النطاقات. وبشكل أساسي، يحدد نظام أسماء النطاقات عنوان أو عناوين بروتوكولات الانترنت المرتبطة باسم

مضيف معين والذي يعرف بـ"تمرير البحث عن نظام تسمية النطاق Forward DNS Lookup". وتقوم سجلات نظام rDNS بتحديد الأسماء المضيفة المرتبطة بعناوين بروتوكول إنترنت معين وهو ما يعرف بـ "البحث العكسي في نظام أسماء النطاقات (DNS)"[1]. وأيضاً، تقوم السجلات بإدراج خوادم الرسائل الإلكترونية لكل نطاق. وبناءً على هذه المفاهيم الأساسية، تقوم عوامل بث الرسائل الإلكترونية بالبحث العكسي في نظام تسمية النطاق للكشف عن الرسائل الإلكترونية الاقتحامية من خلال التأكد مما يلي:

١. إذا كانت نتائج إعادة إرسال البحث في نظام تسمية النطاق مطابقة للبحث العكسي في نظام تسمية النطاق من حيث اسم الموقع وعنوان بروتوكول الإنترنت المدخلين في خادم مصدر الرسالة الإلكترونية، ويعرف هذا الاسلوب ب "التأكيد العكسي لاسم النطاق FCrDNS)". وبهذه الطريقة يتم التحقق من أن هناك مستوى من العلاقة الشرعية بين مالك الموقع وبين مالك عنوان بروتوكول الإنترنت. وهذا الربط كاف فقط لمعرفة أن خوادم مصادر الرسائل الإلكترونية هي غير مسيطر عليها وغير مستخدمة كحاضنات مصدرة للفيروسات وأن المواقع المصدرية غير مزورة، وهي طرق شائعة يستخدمها مرسلو الرسائل الاقتحامية.

٢. أسماء النطاقات لخوادم البريد المصدرية في سجلات rDNS للتحقق من احتمالية كونها قادمة من مستخدمين من شبكة هاتفية، أو من عناوين معينة بشكل ديناميكي، أو من مستخدمي إنترنت يعملون من بيوتهم باستعمال النطاق العريض. يفترض أن تكون مصادر معظم الرسائل الإلكترونية الاقتحامية صادرة من خوادم بريد مجهزة ضمن الفئات المذكورة.

إن إجراء البحث العكسي في نظام أسماء النطاقات هو خاصية قياسية تقريباً في خوادم البريد. عادة ما تكون (MTA's) مصممة للقيام بنوعين من التدقيقات ومن ثم تحجب الرسائل الإلكترونية القادمة من خوادم البريد المصدرية تبعاً لذلك.

المزايا: يعتبر الكشف عن الرسائل الإلكترونية الاقتحامية باستخدام البحث العكسي في نظام أسماء النطاقات سريعاً ومثالياً. ويتم حجب الرسائل الإلكترونية كأحد خواص خوادم البريد لوكلاء نقل البريد (MTA's). وهكذا، فإنها لا تحتاج إلى تجهيز برامج أو أجهزة إضافية، كما أنها توفر وسيلة آمنة لمكافحة الرسائل الإلكترونية الاقتحامية وذلك من خلال عدم استلام (حجب) الرسائل الإلكترونية القادمة من خوادم تصدر الرسائل الاقتحامية. لقد أثبت أسلوب "البحث العكسي عن نظام أسماء النطاقات" فعالية في حجب الأجهزة المسيطر عليها والمستخدمة كحاضنات للرسائل الاقتحامية والفيروسات، وبالإمكان استخدام هذا الأسلوب كمرشح لما قبل إرسال الرسائل الإلكترونية. لقد أوصت منظمة التعاون الاقتصادي والتنمية OECD باستخدامه لمكافحة الرسائل الاقتحامية في ورشة عملها المتعلقة بالرسائل الاقتحامية.

المحددات: المراجعات التي يجريها وكلاء نقل البريد MTA محدودة كما هو موضح في في الأسلوب أعلاه. وبالتالي لا يتم حجب الاساليب المتقدمة في إرسال الرسائل الاقتحامية والرسائل الإلكترونية الاقتحامية. ومن المعوقات الرئيسية لنجاح هذا الاسلوب هو إمكانية التحايل على بروتوكول الإنترنت. ومع أن هذا التحايل معقد وغير مجدي من حيث التكلفة بالنسبة لمرسلي الرسائل الإلكترونية الاقتحامية، إلا أنه من المحتمل أن يستخدم مرسلو الرسائل الإلكترونية التحايل على بروتوكول الإنترنت لتزييف عناوين بروتوكول الإنترنت المرسلة. بالإضافة إلى ذلك، إن الأساليب المشروحة غير موحدة التنفيذ من قبل بروتوكولات الرسائل الإلكترونية علماً بأن القيام بالبحث العكسي في نظام أسماء النطاقات هو خاصية قياسية موحدة في خوادم البريد في الوقت الحاضر. ونتيجة لذلك ليس من الضروري تطبيقها من قبل جميع عوامل بث الرسائل الإلكترونية. زد على ذلك أن عمليات البحث العكسي في نظام أسماء النطاقات قد لا يكون الغرض منها التعامل مع مشكلة الرسائل الإلكترونية الاقتحامية على وجه التحديد، بل تستخدم كتطبيق لمكافحة الرسائل الإلكترونية الاقتحامية. وكذلك قد تولد عمليات البحث في نظام أسماء النطاقات متسوى عال من الايجابيات الزائفة، حيث أن بعض مديري الأنظمة المتمرسين قد لا يقومو بإعداد سجلات نظام أسماء النطاقات العكسي. يقوم بعض مدراء الأنظمة بتعيين نطاقات متعددة لنفس عنوان بروتوكول الانترنت الأمر الذي يعتبر شرعي وهو أيضاً مستخدم على نطاق واسع.

القوائم السوداء على نظام اسم النطاق (DNSBLs)

القوائم السوداء (Black List) على على نظام اسم النطاق (DNS) هي سجلات تحتوي بشكل رئيس على عناوين بروتوكولات الإنترنت وأسماء النطاق القرينة لها لخوادم البريد التي تعتبر مصدراً للرسائل الاقتحامية على الإنترنت. تُنشر القوائم السوداء (Black List) على على نظام اسم النطاق (DNS) وصيغتها مبنية على صيغة سجل على نظام اسم النطاق (DNS). وعند استلام الرسائل الإلكترونية من خادم البريد، فإن خادم البريد المستلم يطلب من خادم على نظام اسم النطاق (DNS) الذي يحتوي على القائمة السوداء لتحديد عنوان بروتوكول خادم الإنترنت الذي هو مصدر الرسائل الإلكترونية. يقوم خادم نظام اسم النطاق بالبحث في القائمة السوداء لنظام اسم النطاق عن اسم النطاق المتماثل مع عنوان بروتوكول الإنترنت المطلوب. وإذا وجد اسم النطاق يستجيب خادم على نظام اسم النطاق (DNS) وبذلك يعتبر خادم مصدر الرسالة

[1] يمكن أن يكون هناد عنوان بروتوكول إنترنت واحد مطبق على عدة أسماء مضيفةلأغرض التسكين الافتراضية. كما يمكن أن يكون هناك عدة بروتوكولات إنترنت مطبقة على اسم مضيف واحد لأغراض تحمل الأخطاء وموازنة الأحمال.

الإلكترونية مصدراً معروفاً للرسائل الإلكترونية الاقتحامية. وإذا لم يتم العثور على اسم النطاق، فإن خادم على نظام اسم النطاق (DNS) يستجيب ويرد بإعطاء قيمة اسم النطاق يرمز لها (NXDOMAIN) وتعني أن النطاق غير موجود. وبناءً على ذلك فإن خادم استقبال الرسائل الإلكترونية يقوم باتخاذ قرار بخصوص الرسائل الإلكترونية الاقتحامية ويحجب الرسائل القادمة من خادم مصدر الرسائل. لقد أثبتت القوائم السوداء (Black List) لعلى نظام اسم النطاق (DNS) أنها فعالة في حجب الرسائل الاقتحامية من مرحلات البريد المفتوحة واتصالات البريد المفتوحة ومن مرسلي الرسائل الاقتحامية المعروفين وما شابه ذلك. هناك قوائم سوداء لعلى نظام اسم النطاق (DNS) معروفة ومتوفرة ومحددة لعمل قائمة بالمرحلات المفتوحة واتصالات الوكيل المفتوحة التي يمكن استخدامها من قبل خوادم بريد قبل قبولها استلام الرسائل من خوادم غير معوروفة.

المزايا: يعتبر الكشف عن الرسائل الإلكترونية الاقتحامية باستخدم القائمة السوداء لعلى نظام اسم النطاق (DNS) سريع ومثالي. ويتم حجب الرسائل الإلكترونية كأحد خواص خوادم البريد لوكلاء نقل البريد (MTA's). وهكذا، فإنه لا يحتاج إلى تجهيز برامج أو أجهزة إضافية. كما يوفر وسيلة آمنه لمكافحة الرسائل الإلكترونية الاقتحامية بعدم استقبال (حجب) الرسائل الإلكترونية القادمة من خوادم تقوم بإرسال الرسائل الاقتحامية. لقد أثبت هذا الاسلوب فعالية في حجب الاجهزة المسيطر عليها وأصبحت حاضناً ومصدراً للرسائل الاقتحامية والفيروسات والتي تستعمل كخوادم لإرسال الرسائل الإلكترونية الاقتحامية. وهذا الاسلوب يستخدم كاسلوب ترشيح لما قبل إرسال الرسائل.

المحددات: يعتبر نوع الفحص الدي يقوم به أسلوب القائمة السوداء لعلى نظام اسم النطاق (DNS) بدائياً عند مقارنته بأساليب إرسال الرسائل الاقتحامية المتقدمة. وقد يلتف مرسلو الرسائل الإلكترونية الاقتحامية حوله لنشر وسائلهم الإلكترونية الاقتحامية من خلال تجهير خوادم رسائل إلكترونية (من الأجهزة الحاضنة المسيطر عليها) لتتوسط الاتصال بين خادم الرسائل الإلكترونية الاقتحامية وبين خادم مستقبل الرسائل الإلكترونية. بالإضافة إلى ذلك، من الصعب رصد وإدراج عناوين بروتوكلات الانترنت الديناميكية في كل مرة، وأيضاً بإمكان مرسلي الرسائل الاقتحامية تجهيز خوادم جديدة لإرسال الرسائل الإلكترونية الاقتحامية. ومن المعوقات الرئيسة لنجاح هذا الاسلوب هو إمكانية التحايل على بروتوكول الإنترنت. ومع أن هذا التحايل معقد وغير مجدي من حيث التكلفة بالنسبة لمرسلي الرسائل الإلكترونية الاقتحامية، إلا أنه من المحتمل أن يستخدم مرسلو الرسائل الإلكترونية التحايل على بروتوكول الإنترنت لتزييف عناوين بروتوكول الإنترنت المرسلة. إن القوائم السوداء (Black List) لعلى نظام اسم النطاق (DNS) ليست ذاتية التعلم، وسجلاتها بحاجة للتحديث اليدوي والقيام بإدخالات جديدة من قبل شخص مصرح له القيام بذلك. وقد يعتبر اختيار قائمة سوداء موثوق بها لعلى نظام اسم النطاق (DNS) تحدياً في بعض الحالات، لأن هناك قوائم سوداء عديدة لعلى نظام اسم النطاق (DNS) متوفرة لدى العامة وتعتبر جديرة بالثقة. وقد ينشر مرسلو الرسائل الإلكترونية الاقتحامية قوائم سوداء مزيفة لخداع خوادم البريد. إن التحقق من مشروعية ناشر القوائم السوداء (Black List) لعلى نظام اسم النطاق (DNS) يتطلب آليات توثيق معقدة. بالإضافة إلى ذلك، إن خادم على نظام اسم النطاق (DNS) وقائمته السوداء تتطلبان مستويات عالية من الإجراءات الأمنية لتجنب هذه الهجمات والمناورة والتزييف.

البحث في أسماء المواقع (URL)

قد يساعد البحث في أسماء المواقع (URL) على تحديد الرسائل الإلكترونية التي تحتوي على روابط مواقع على الشبكة العنكبوتية تستخدم من قبل مرسلي الرسائل الاقتحامية لوضع محتويات لم يطلبها المستخدمون. وكمحاولة لتجاوز مرشحات الرسائل الإلكترونية، يقوم مرسلو الرسائل الافتحامية باستضافة موقع على الشبكة العنكبوتية يضعون عليه محتويات غير مرغوبة. وبعد ذلك يقومون بتوزيع عناوين المواقع من خلال الرسائل الإلكترونية الاقتحامية. من الناحية النموذجية، يقوم مزود الخدمة بنشر قائمة لأسماء المواقع الموجودة على الشبكة والتي تحتوي على محتوى اقتحامي. وعند استلام رسالة إلكترونية تحتوي على اسم موقع محدد (URL) فإن نظام مكافحة الرسائل الاقتحامية سيستخلص اسم الموقع ويقوم بالإستفسار باستخدام نسخة من قائمة الفحص الموجودة على الشبكة أو الفحص باستخدام النسخة المحلية لتحديد مصدر عنوان الموقع ومعرفة فيما إذا كان مصدر الموقع المحدد يشير إلى موقع ذي طبيعة اقتحامية. ويتم حجب الرسالة الإلكترونية إذا ثبت مطابقة نطاق اسم الموقع مع نطاق آخر مدرج في القائمة.

المزايا: يعتبر أسلوب البحث في أسماء المواقع فعالاً في حجب الرسائل الإلكترونية التي قد تحتوي على روابط تشير إلى مواقع إلكترونية ذات طبيعة اقتحامية. وفي الوقت الحاضر، فهذه هي الآلية الوحيدة للتحقق من شرعية الروابط الواردة ضمن الرسائل الإلكترونية.

المحددات: يقتصر أسلوب البحث في أسماء المواقع على تحديد الرسائل الإلكترونية التي تحتوي على روابط تشير إلى مواقع إلكترونية ذات طبيعة اقتحامية، ولا يركز هذا الأسلوب على الأنواع الأخرى للرسائل الإلكترونية الاقتحامية. وهو لا يستطيع أن يتعلم بذاته القوائم التي تحتوي على مواقع إلكترونية ذات طبيعة اقتحامية. وبالتالي فهو بحاجة للتحديث اليدوي بإدخالات جديدة من قبل شخص مصرح له القيام بذلك. وإذا لم يتم الكشف عنها من قبل شخص ما أو تم نشرها في القائمة، فإنه يتعذر الكشف عن الرابط ذو الطبيعة الاقتحامية الموجود على الشبكة . إن اختيار مزود خدمة موثوق به يقوم

بنشر القائمة قد يعتبر تحدياً في بعض الحالات، حيث قد يقوم مرسلو الرسائل الاقتحامية بنشر قوائم سوداء مزيفة لخداع عمليات البحث. بالإضافة إلى ذلك، فإن التحقق من الناشر قد يتطلب آليات توثيق معقدة، ولا يغني ذلك عن القول بأن هذه الطريقة قد تولد بعض الإيجابيات الزائفة من خلال حجب رسائل إلكترونية تحذر من زيارة مواقع إلكترونية خطرة.

رفض قوائم جري (Grey) الإلكترونية

تتضمن هذه الطريقة آلية تقوم بإعادة الرسائل الإلكترونية التي يتم استلامها من خوادم رسائل إلكترونية غير معروفة. والإفتراض الذي تقوم عليه هذه الآلية مبني على مواصفات طلب إبداء الملاحظات والتي مفادها أن خادم الرسائل الإلكترونية الشرعية سيحاول الاتصال فيما بعد لتوصيل الرسائل الإلكترونية التي تم رفضها. وفي المقابل، ليس من المتوقع أن تقوم خوادم الرسائل الاقتحامية بإعادة إرسال رسائلها المعادة لأنها تبث رسائل إلكترونية جماعية. وعلى أية حال، فإن معظم خوادم الرسائل الإلكترونية الاقتحامية التي تحاول إعادة بث الرسائل الإلكترونية المعادة مدرجة في القوائم السوداء (Black List) المشهورة والمرتبطة بعلى نظام اسم النطاق (DNS). من الناحية النموذجية، يسجل الخادم الذي يستقبل الرسائل الإلكترونية عنوان بروتوكول الإنترنت لخادم مصدر الرسائل الإلكترونية، وعنوان مرسل الرسالة الإلكترونية وعنوان مستلمها. ويقوم وكيل بث الرسائل الإلكترونية بفحص السجل الموجود في قاعدة البيانات الداخلية. وفي حالة عدم العثور على السجل، فإن خادم مستقبل الرسائل الإلكترونية يرفض الرسائل الواردة. وبعد ذلك، ينتظر خادم مستقبل الرسائل الإلكترونية لفترة من الوقت لكي يقوم خادم مصدر الرسالة الإلكترونية بإعادة الرسائل المرفوضة. وعند انقضاء المدة دون استلام الرسائل المرفوضة فإن مستلم الرسالة قد يعتبر خادم مصدر الرسالة على أنه مصدر اقتحامي. وعلى أية حال، جميع الرسائل الإلكترونية غير المعروفة يتم رفضها في جميع الحالات في المقام الاول. وعادة، لا تقوم الحواسيب المسيطر عليها zombie الحاضنة للرسائل الإلكترونية الاقتحامية أو خوادم الرسائل الاقتحامية بمحاولة إعادة إرسال الرسائل الإلكترونية المرفوضة. ومن هنا، وجد هذا الأسلوب فعالا في حجب خوادم الرسائل الاقتحامية.

المزايا: تعتبر طريقة الكشف عن الرسائل الإلكترونية الاقتحامية باستخدام قوائم جري(Grey) سريعة وبسيطة ومثالية. ويستخدم المواصفات القياسية لبروتوكولات البريد الإلكتروني. ويتم حجب الرسائل الإلكترونية كأحد خواص خوادم البريد لوكلاء نقل البريد (MTA's). وهكذا، فإنه لا يحتاج إلى تجهيز برامج أو أجهزة إضافية. ويوفر وسيلة آمنه لمكافحة الرسائل الإلكترونية الاقتحامية من خلال الرفض الأولي لاستلام الرسائل القادمة من خوادم ترسل رسائل إلكترونية اقتحامية. وقد اثبت هذا الاسلوب فعالية في رفض التعامل مع الأجهزة التي تعتبر مقرات حاضنة zombie مصدرة للفايروسات المستخدمة في خوادم إرسال رسائل إلكترونية اقتحامية. ويمكن استخدام هذا الأسلوب كطريقة ترشيح ما قبل إرسال الرسائل الإلكترونية.

المحددات: تعتبر قوائم جري (Grey) لرفض الرسائل الإلكترونية حلاً شاملاً لمكافحة الرسائل الإلكترونية الاقتحامية. وعلى الرغم من فعاليتها، فإن بأمكانها أن تسبب ازعاجات رئيسية وتأخير للرسائل الإلكترونية التي تتطلب رداً فورياً. ومثال ذلك المواقع الإلكترونية التي تحتاج إلى استجابات سريعة من المستخدم من خلال الرسائل الإلكترونية لإكمال عمليات تسجيلهم على الشبكة. وهذا الأسلوب قد يعيق المستخدمين من إكمال عمليات تسجيلهم لبعض الوقت. وثمة إزعاج آخر جوهري قد يحدث إذا كانت فترة الإنتظار المعطاه للرسائل الإلكترونية المعادة لا تتم متابعتها أو التعرف عليها من خادم مصدر الرسائل الإلكترونية. وفي هذه الحالة سترسل الرسالة الإلكترونية بعد انقضاء المدة. وهكذا، لن تصل الرسالة الإلكترونية إلى المستلم، وبالتالي، فإن خادم مستقبل الرسالة الإلكترونية قد يعتبرخادم مصدر الرسالة مصدراً اقتحامياً ويقوم بحجبه.

عناوين الرسائل الإلكترونية القابلة للتخلص منها DEA

عناوين الرسائل الإلكترونية القابلة للتخلص هي بشكل أساسي خدمة يقدمها مزودو خدمة عناوين الرسائل الإلكترونية القابلة للتخلص. وعناوين الرسائل الإلكترونية القابلة للتخلص فعالة في السيطرة على الرسائل الاقتحامية. وفيما يلي المبدأ الذي تقوم عليه هذه العناوين: بإمكان المستخدم الحصول على عدد من عناوين الرسائل الإلكترونية المؤقتة المرتبطة بواحد أو أكثر من عناوين المراسلة الإلكترونية الأصلية. ومن ناحية نموذجية، فإن المستخدم يستطيع الحصول على عناوين رسائل إلكترونية قابلة للتخلص لمجموعة من عناوين المراسلة الأصلية الإلكترونية، أو الحصول على عناوين رسائل إلكترونية قابلة للتخلص وذلك لكل عنوان من عناوين المراسلة الأصلية. مثال:
(SingleContactName@User.DEAServiceProviderName.Com). يقوم المستخدم بتعميم عناوين الرسائل الإلكترونية القابلة للتخلص وفي نفس الوقت يحافظ على سرية العناوين الأصلية. تقوم عناوين الرسائل الإلكترونية القابلة للتخلص بإعادة إرسال الرسائل الإلكترونية القادمة إلى قائمة العناوين الأصلية. وفي حالة الهجوم على عناوين الرسائل الإلكترونية القابلة للتخلص من قبل الرسائل الإلكترونية الاقتحامية، أو عندما لا يصبح المستخدم مهتماً في استلام رسائل إلكترونية من ضمن عناوين الرسائل الإلكترونية القابلة للتخلص، فيمكنه إلغاءها. وإذا وضعت عناوين الرسائل الإلكترونية

القابلة للتخلص على أساس فردي لكل عنوان من العناوين الأصلية، يستطيع المستخدم أيضاً الكشف عن مصدر الرسائل الاقتحامية والإبلاغ عن محاولة سوء استخدام من النوع الإقتحامي. وبالإضافة إلى ذلك، إذا رغب المستخدم في تغيير عناوين الرسائل الإلكترونية القابلة للتخلص المتعلقة بعنوان مراسلة حقيقي وشرعي، فإنه يحتاج فقط لتحديث عنوان المراسلة جنباً إلى جنب مع عناوين الرسائل الإلكترونية القابلة للتخلص الجديدة.

المزايا: استخدام آلية عناوين الرسائل الإلكترونية القابلة للتخلص لمكافحة الرسائل الإلكترونية الاقتحامية بسيط وفعال. وكما تم شرحه، فإن عناوين الرسائل الإلكترونية القابلة للتخلص التي يتم مهاجمتها من قبل مرسلي الرسائل الإلكترونية الاقتحامية يمكن إلغاؤها وإعادة إرسالها إلى مجلد الرسائل المهملة (Junk mail) أو إلى سلة المهملات. وأيضاً، يمكن تقديم تقرير على أساس عنوان فردي من عناوين الرسائل الإلكترونية القابلة للتخلص. إن آلية عناوين الرسائل الإلكترونية القابلة للتخلص لإستلام الرسائل الإلكترونية تضمن مستويات عالية من الأمن وتحمي الرسائل الإلكترونية الأصلية من التعرض للخطر. تؤدي عناوين الرسائل الإلكترونية القابلة للتخلص إلى إدارة أفضل لعناوين المراسلة الخاصة بالمستخدم. وعند تغيير عناوين الرسائل الإلكترونية القابلة للتخلص الخاصة بعنوان أصلي واحد، فإن المستخدم يحتاج فقط لتحديث عنوان المراسلة الأصلي جنباً إلى جنب مع عناوين الرسائل الإلكترونية القابلة للتخلص. وأيضاً في حالة تغيير العنوان الأصلي للمستخدم، فهو فقط بحاجة إلى تحديث مزود خدمة عناوين الرسائل الإلكترونية القابلة للتخلص وأيضاً العنوان الجديد لرسائل المستخدم بدون تكليف نفسه عناء تبليغ الجميع بعناوينه.

المحددات: عند استخدام عناوين الرسائل الإلكترونية القابلة للتخلص، قد يحتاج المستخدم إلى الحفاظ على قائمة عناوين المراسلة الأصلية و عناوين الرسائل الإلكترونية القابلة للتخلص المتعلقة بها. قد تكون عملية إدارة قائمة تحوي عددا كبيرا من عناوين المراسلة مزعجة بعض الشيء. وحيث أن المزودين الموثيقين لخدمة عناوين الرسائل الإلكترونية القابلة للتخلص لا يقدمون خدماتهم مجاناً، فإن بعض المستخدمين قد يعتبرون الإنفاق مقابل هذه الخدمة أمراً غير منطقي لأنها بشكل رئيسي عبارة عن تحسين لخدمة مجانية. (خدمة الرسائل الإلكترونية). وفي العديد من الحالات، قد يرغب المستخدمون في استخدام عناوين الرسائل الإلكترونية القابلة للتخلص للتسجيل والاشتراك في خدمات إلكترونية مباشرة متنوعة. بعض هذه الخدمات توجب على المستخدمين تزويدها بالرسائل الإلكترونية الحقيقة لقبول التسجيل. وفي مثل هذه الحالات تكون عناوين الرسائل الإلكترونية القابلة للتخلص غير مساعدة حيث أن مزودي الخدمة يريدون الحصول على الرسائل الإلكترونية الحقيقية للمشتركين فيها لكي يكون مستوى التحقق من الشرعية افضل.