أساليب رسائل البريد الإلكتروني الاقتحامية

مقدمة

يستخدم مرسلو الرسائل الاقتحامية عدة أساليب لنشر الرسائل الاقتحامية عبر البريد الإلكتروني. وبعض هذه الأساليب تستغل الثغرات في مواصفات شبكات الكمبيوتر وأنظمة اتصالات الكمبيوتر الحالية، بينما بعض الرسائل الاقتحامية يسلك طرقاً التفافية حول التدابير الأمنية المتعلقة بأنظمة الاتصالات وتقنية المعلومات. وتقدم هذه المقالة إيجازاً عن الأساليب التي يطوعها مرسلو الرسائل الاقتحامية لنشر الأنواع المختلفة من رسائل البريد الإلكتروني الاقتحامية.

أساليب الرسائل الإلكترونية الاقتحامية

يقوم مرسلو الرسائل الاقتحامية بتجميع عناوين البريد الإلكتروني من خلال عمليات الجمع العشوائي للعناوين الإلكترونية "email address harvesting". وتشير عملية "الجمع العشوائي للعناوين الإلكترونية" إلى الأساليب المستخدمة في تجميع عناوين البريد الإلكتروني دون معرفة مستلمي الرسائل بذلك. ومن بين الطرق التي يستخدمها مرسلو الرسائل الاقتحامية ما يلي:

- الحصول على العناوين من مرسلي رسائل اقتحامية آخرين.
- عمل مواقع إلكترونية تطلب التسجيل أو مواقع إلكترونية تقدم اشتراكات مجانية ويتم تجميع العناوين الإلكترونية من خلالها.
- استخدام برامج كمبيوتر تسمى برامج الجمع العشوائي لعناوين البريد الإلكتروني "harvesting bots"، والتي تتصفح المواقع الإلكترونية والمدونات والمنتديات والجماعات الإخبارية، وتقوم بتجميع العناوين الإلكترونية.
- استخدام طريقة التركيب العشوائي للعناوين الإلكترونية (dictionary attacks) لتجميع عناوين البريد الإلكتروني.

ولإرسال رسائلهم الإلكترونية الاقتحامية، يحتاج مرسلو هذه الرسائل إلى نطاقات إنترنت وإعداد خادم بريد أو أكثر. بعد ذلك يستخدمون برامج تسمى برامج الرسائل الاقتحامية "SPAM bots"[1] لإرسال رسائل بريد إلكتروني اقتحامية متعددة. ويميل مرسلو الرسائل الاقتحامية إلى إخفاء هويتهم عند إرسال رسائلهم الاقتحامية، وذلك عبر استخدام الوسائل التالية:

- تمرير مسارات رسائلهم الإلكترونية عبر مرحلات مفتوحة[2] أو اتصالات وكيل مفتوحة[3].
- تضليل ترويسة الرسالة الإلكترونية، وخصوصاً حقل (المرسل/من) في ترويسة الرسالة الإلكترونية.
- تضليل عنوان بروتوكول الإنترنت لخوادم البريد لديهم وكذلك اسم النطاق لكل رسالة إلكترونية تصدر عنهم. وعلى الرغم من أن عملية تضليل بروتوكول الإنترنت تعتبر معقدة وليست مجدية اقتصادياً لإرسال الرسائل الاقتحامية، إلا أنه يظل ممكناً لمرسلي الرسائل الاقتحامية استخدام أسلوب

---

[1] *برامج الرسائل الاقتحامية التي تسمى (SPAM bots) هي برامج يتم إعدادها على خوادم البريد لتأليف وإرسال رسائل إلكترونية اقتحامية بالجملة. وقد لوحظ أن هذه البرامج لا تلتزم بدقة بمواصفات بروتوكول النقل البسيط (SMTP).*

[2] *مرحلات البريد المفتوحة هي عبارة عن خوادم توجد في الشبكات العامة (الإنترنت)، وتسمح لأي شخص بإرسال رسائل إلكترونية من خلالها باستخدامها كخادم بريد وإخفاء هوية خادم البريد الحقيقي.*

[3] *اتصالات الوكيل المفتوحة هي خوادم الوكيل الموجودة في الشبكات العامة (الإنترنت)، وهي تستثني الرسائل الواردة (من أي مكان كانت) ومن ثم تحول الحركة إلى واجهة أخرى بحيث تبدو الحركة وكأنها ناشئة عنها، ومن المرجح أن يساء استخدام خوادم الوكيل المفتوحة بسبب سوء إعداداتها أو افتقارها لضوابط دخول مناسبة. ويمكن لمرسلي الرسائل الاقتحامية إرسال رسائلهم الاقتحامية عبر هذه الخوادم وإخفاء هوية خادم البريد الفعلي الذي قام بإرسال الرسائل الاقتحامية.*

تضليل أو تمويه بروتوكول الإنترنت لتزوير عناوين بروتوكول الإنترنت في الرسائل التي يرسلونها.

وقد يستفيد مرسلو الرسائل الاقتحامية كذلك من خوادم البريد ضعيفة الإعداد التي لا تلتزم بدقة بمواصفات بروتوكول النقل SMTP، بحيث يمارسون قرصنتهم عبرها لإرسال الرسائل الاقتحامية. ومن الأمثلة الشائعة على عدم الالتزام هي الخوادم التي لا تطلب اسم مستخدم وكلمة مرور للاتصال معها عبر خدمة (telent). ويمكن لمرسلي الرسائل الاقتحامية استعمال هذه الخوادم بسهولة لإرسال رسائلهم الاقتحامية التي تزور هوياتهم. كما أن بعض مرسلي الرسائل الاقتحامية يستخدمون التروجانات (أحصنة طروادة)[4] للسيطرة على أجهزة كمبيوتر في نطاقات مختلفة، وبذلك تصبح تلك الأجهزة حاضنة لنشاطات إرسال الرسائل الاقتحامية ويبقى المرسل الحقيقي مجهولاً. كما يمكن لمرسلي الرسائل الاقتحامية القيام بصورة غير مباشرة بإرسال الرسائل الاقتحامية من خلال تضليل حقل تروسية (المسار العائد) "Return-Path" للرسالة الإلكترونية كي يكون لها عنوان مشروع. وبالتالي، يبدأ العنوان المشروع باستلام رسائل إلكترونية راجعة (غير مستلمة)، وإجابات غير مطلوبة ورسائل أخطاء مما يسبب إزعاجاً كبيراً. ويلجأ مرسلو الرسائل الاقتحامية مؤخراً إلى إنشاء حسابات بريد إلكتروني متعددة على خدمات البريد الإلكتروني المجانية من خلال تشغيل لغة تشتمل على أوامر (HTTP POST) بأسماء مستخدمين وكلمات مرور مختلفة. وبعد ذلك يشغلون كوداً يتضمن أوامر متعددة (HTTP POST) لرسالة بريد إلكترونية لإرسال رسائلهم الاقتحامية. ويخفي هذا الأسلوب الهوية الحقيقية لمرسلي الرسائل الاقتحامية ويتيح لهم إرسال رسائل اقتحامية بالجملة دون تكبد أية تكاليف رئيسية.

ويؤلف مرسلو الرسائل الاقتحامية رسائلهم الإلكترونية بحيث تحتوي على مواد إعلانية ومحتويات تافهة وطرق خداع وتضليل مختلفة. وقد لوحظ مؤخراً أن مرسلي الرسائل الاقتحامية يؤلفون رسائلهم الإلكترونية من خلال:

- تضمين محتوى رسائلهم الاقتحامية ضمن محتويات ومضامين أخرى شرعية.
- وضع موادهم غير المطلوبة على الإنترنت ويدرجون عنوان موقع (URL) يشير إلى موقع الويب في رسائلهم الاقتحامية.
- يعتمون أو يشوشون على النص في الرسالة الإلكترونية [5]
- تضمين كود (HTML) ولغات ويب في جسم الرسائل الإلكترونية.[6]
- تضمين رسائلهم داخل صورة مرفقة بالرسالة الإلكترونية.

---

[4] *التروجانات (أحصنة طروادة) هي برامج كمبيوتر تُظهر أن لها وظائف معينة، بينما هي في حقيقة الأمر تستخدم تلك الوظائف كغطاء لوظائفها الحقيقة.*

[5] *النصوص المشوشة لرسالة إلكترونية تشير إلى طباعة كلمة أو كلمات باستخدام رموز غير أبجدية. ومثال ذلك طباعة كلمة "Viagra" على النحو التالي "Vi@gra" ويستخدم هذا الأسلوب لطباعة كلمات تعطي انطباعاً عن وجود محتوى رسالة اقتحامية.*

وُهلين ف

[6] *حيث أم معظم برامج البريد الإلكتروني تدعم عرض محتويات النصوص المكتوبة بلغة (HTML)، فإن مرسلي الرسائل الاقتحامية يميلون نحو تضمين كود HTML داخلي في رسائلهم الإلكترونية يحتوي على روابط لاسترجاع محتويات موجودة في الويب، مثل الصور أو المواقع الإلكترونية المحتوية على محتويات رسائل إلكترونية أو لغة رمزية لكي يحصل مرسلو الرسائل الاقتحامية على إفادة بأن الرسالة قد قرأت وأن حساب البريد الإلكتروني المرسل إليه يعتبر نشطاً. ويمكن أن تستخدم النصوص (scripts) لإنزال كود خبيث و/أو نصوص برمجية لتنفيذ كود خبيث.*