This translation is a joint initiative of MAAWG (www.maawg.org) and ITU (www.itu.int/ITU-D/cyb/cybersecurity).

إدارة المنفذ 25 لحيز أماكن الإقامة والحيز الدينامي لبروتوكول الإنترنت ومزايا التقاعس عن اتخاذ إجراءات ومخاطره

مقدمة

يستعمل الأفراد الذين يبعثون الرسائل الاقتحامية وغيرهم من المجرمين على نحو متزايد الفيروسات و"برمجيات التجسس" للتحكم في أعداد كبيرة من الحواسيب. وتتيح الزيادة المستمرة في الحواسيب والتوصيلات "الموصلة دائماً" مثل خط المشترك الرقمي DSL، أو الشبكات الكبلية أو شبكات الشركات أهدافاً أكثر وقدرة أكبر على إحداث دمار شديد. ومع إدخال تغييرات تكنولوجية معدودة، مقترنة بتعليم المستعمل الذي يشمل استخدام برمجيات مكافحة الفيروسات وجدران الحماية، يمكن لأي مقدم خدمة البريد الإلكتروني أن يتحكم أكثر في الحركة الخبيثة المحتملة الناشئة عن أنظمة مستخدميه. ويمكن لمقدمي خدمة البريد الإلكتروني، من خلال إدارة إرسال البريد الإلكتروني من الحواسيب الشخصية، أن يخفضوا تكاليف تسيير أعمالهم، وزيادة رضاء العميل وتقليل مستوى إساءة استعمال الإنترنت المرتبط بخدماتهم.

تهديدات إرسال البريد الإلكتروني وإساءة استعمال

النفاذ غير المنقطع للإرسال (إرسال البريد الإلكتروني) من الحواسيب الشخصية إلى مخدمي البريد الإلكتروني الذي لا يمكن أن يديره أو يرصده مقدم خدمة البريد الإلكتروني يُعرض عملائهم لمخاطر شديدة للوقوع ضحايا للأشخاص والبرمجيات. وتوفر الحواسيب الشخصية التي تخضع لإشراف أطراف ثالثة غير مسموح لها أو غير مكشوفة، التي يطلق عليها عادة "برمجيات التسلل" أو "botnets"، ستاراً لإخفاء شخصية من يستخدمونها للتوصيل مباشرة ببدالة البريد الإلكتروني ومرحلات مخدمات بروتوكول نقل البريد غير المحمية SMTP، وترسل مع ذلك المزيد من الرسائل الاقتحامية والفيروسات. ويمر زهاء 80% من جميع الرسائل الاقتحامية عبر "برمجيات التسلل" إلى الحواسيب الشخصية دون معرفة أو ترخيص من أصحابها.

مخاطر التقاعس عن اتخاذ إجراءات

والآثار السلبية على أصحاب الحواسيب المتأثرة فورية وشديدة. وكثيراً ما يشهد أصحاب الحواسيب فترات تتسم بالبطء في الأداء، وخاصة عندما يحاولون استعمال الإنترنت. ونظراً لعدم درايتهم، يمكن للأفراد الذين يبعثون الرسائل الاقتحامية أن يشبعوا عرض النطاق الصادر أو أن يحدوا بشدة من عرض النطاق الوارد كذلك.

ويستطيع مقدم الخدمة الموصول بالحاسوب بالكاد ملاحظة أن عرض النطاق الإضافي مستخدم، إلا أنه عادةً ما يتأثر سلباً أيضاً. وقد يطلب العميل المتأثر الدعم التقني، الذي يمكن أن يكلف مقدم الخدمة ما مقداره شهر من الإيرادات أو أكثر، أو أن يقرر العميل أن مقدم البرمجية، أو خدمات النداء وخدمات النطاق العريض تؤدي أداءً سيئاً ويقوم بإلغاء الخدمة بأسرها.

وأياً كان طول الفترة التي يبقى فيها المستخدم موصولاً في حالة تلف، يقوم مقدم الخدمة بتجميع الشكاوى ممن يتلقون الرسائل الاقتحامية التي تدفع إلى الخارج عن طريق العميل المصاب بالتلف. ويمكن أن تدفع الشكاوى المرسلة إلى إدارات دعم العميل، وإساءة الاستعمال وعمليات الشبكة إلى رفع التكاليف إلى حدود مؤلمة مع

وجود عدد أصغر من الحواسيب المزودة "ببرمجيات التسلل". وسرعان ما قد يجد مقدم الخدمة شبكته بأسرها على "قائمة سوداء" أو يحظر عليه إرسال البريد الإلكتروني إلى الجمهور المستهدف، وذلك استناداً إلى نمط إساءة الاستعمال النابع من شبكته. ومن الطبيعي أن كل رسالة اقتحامية مرسلة هي أيضاً رسالة اقتحامية مستلمة. والسماح باستمرار هذا النوع من إساءة الاستعمال له أثر سلبي عالمي متناسب على جميع مستعملي الإنترنت وعلى مقدمي خدمات النفاذ وذلك نتيجة لتدني ثقة المستهلك، مما يؤدي بالتالي إلى انخفاض رغبة المستهلكين في استعمال الإنترنت كوسيلة للاتصال والتجارة والمزاح.

أفضل الممارسات في إرسال البريد الإلكتروني

التنظيم الذاتي للصناعة هو أنجع وسيلة للتصدي لإساءة استعمال إرسال البريد الإلكتروني، ويتطلب حجم مشكلة الرسائل الاقتحامية اتخاذ إجراءات فورية. وقد تلقت الوكالات الحكومية على الصعيد العالمي هذه الرسالة المدوية والواضحة: غياب الإجراءات الفورية ونتائجها، تواجه الصناعة تدقيقاً وتنظيماً متزايدين. وبناءً على ذلك، يوصي فريق العمل المعني بمكافحة إساءة استعمال المراسلة بالمجموعة التالية من أفضل الممارسات في إرسال البريد الإلكتروني لمقدمي خدمتي الإنترنت والبريد الإلكتروني:

1. توفير خدمات إرسال البريد الإلكتروني على المنفذ 587، وفقاً للوصف الوارد في RFC 2476.
2. أن تطلب الاستيقان لإرسال البريد الإلكتروني، وفقاً للوصف الوارد في RFC 2554.
3. الامتناع عن التداخل في توصيلية المنفذ 587.
4. تشكيل برمجية البريد الإلكتروني للعميل لاستعمال المنفذ 587 والاستيقان لإرسال البريد الإلكتروني.
5. حجب النفاذ إلى المنفذ 25 لجميع المخدمات على شبكتك، خلاف المسموح لها بذلك صراحة بأداء وظائف ترحيل SMTP. ومن المؤكد أن هذه المخدمات ستشمل مخدمات إرسال البريد الإلكتروني الخاصة بك ويمكن أن تشمل أيضاً مخدمات مشروعة لإرسال البريد الإلكتروني لعملائك المحتملين.
6. حجب الحركة الداخلة إلى شبكتك من المنفذ 25. ويحول ذلك دون إساءة الاستعمال الممكنة بواسطة مرسلي الرسائل الاقتحامية الذي يستخدمون التمرير غير المتوافق والمخادعة في بروتوكول الإنترنت للوصول إلى شبكتك.

اعتمد مقدمو الخدمة من كافة الأحجام هذه الممارسات، بما في ذلك أكثر مقدمي الخدمات شهرة على الصعيد العالمي وكذلك العديد من أعضاء فريق العمل المعني بمكافحة إساءة استعمال المراسلة، دون أي انخفاض يمكن تقديره في قاعدة المستهلكين.

مزايا اعتماد تدابير

توفر المطالبة بالاستيقان والحركة الكلية لإرسال البريد الإلكتروني عن طريق مرحلات مخدم بروتوكول نقل البريد الإلكتروني SMTP، لمقدم خدمة الإنترنت مزايا قيمة. وتمكن هذه التدابير مقدم خدمة الإنترنت (ISP) مما يلي:

رصد معدلات الإرسال، لكل مستهلك و/أو الإرسال الكلي، والحد منه.
إنفاذ سياسات استعمال مقبولة وشروط خدمة إرسال البريد الإلكتروني.

بالإضافة إلى ذلك، يكسب مقدمو خدمة الإنترنت، المزايا النسبية التالية:

تخفيض تكاليف مركز تقديم المساعدة، ودعم العملاء ومراكز تشغيل الشبكة.

.25
تخفيض تكاليف البنية التحتية الناشئ عن التخفيضات في استعمال المنفذ واستهلاك عرض النطاق.

وبمجرد وضع هذه التدابير، لا يمكن للآلات المصابة بالفيروسات أن تكون محركات لإخفاء الشخصية الفردية. ويمكن تحديد الحواسيب المصابة بفيروسات بسرعة ويمكن حجرها إلى أن يصبح المالك مدركاً للمشكلة ويصححها. وخلال هذه العملية، يتعلم المستعملون التهديدات الأمنية ويجري تشجيعهم على حماية أنفسهم بشكل أفضل. وكل هذه التغييرات تزيد سلامة وخصوصية □□□□ المستعملين النهائيين.

المستعمل

لا يستطيع فريق العمل المعني بمكافحة إساءة استعمال المراسلة التأكيد بما فيه الكفاية على أهمية التواصل مع المستعملين وتعليمهم بشأن هذه التهديدات، والإجراءات المتخذة للتصدي لها، والدور الذي يجب أن يضطلع به ملاك الحواسيب في مرحلة الانتقال إلى أسلوب آمن لإرسال البريد الإلكتروني. ويجب على مقدمي خدمات الإنترنت والبريد الإلكتروني أن يحيطوا عملائهم علماً بما يتخذونه من إجراءات، ولماذا يتخذونها ولماذا ستكون شفافة بالنسبة لأغلبية كبيرة منهم.

وتشجع بقوة جميع الموجات الحاملة للبريد الإلكتروني على اعتماد هذه الممارسات التكنولوجية، بأسرع ما يمكن، بحيث تستعيد قدرتها على التحكم في المنفذ 25، وأن توفر التعليم المتقدم لعملائهم، والإبقاء على خدماتها آمنة من إساءة استعمالها.

القراءات ذات الصلة

SMTP Service Extension for Authentication, J. Meyers, March 1999: http://www.ietf.org/rfc/rfc2554.txt

Message Submission, R. Gellens and J. Klensin, December 1998: http://www.ietf.org/rfc/rfc2476.txt

Operation Spam Zombies, Federal Trade Commission, May 2005:
http://www.ftc.gov/bcp/conline/edcams/spam/zombie/

Anti Spam Technical Alliance Technology and Policy Proposal, Anti Spam Technical Alliance, June 11, 2004:
http://www.postmaster.aol.com/asta/proposal_html.html

Stopping Spam - Creating a Stronger, Safer Internet, Industry Canada, April 2005:
http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00329e.html