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

أفضل ممارسات التحكم في بيئات النفاذ المحصنة التي يوصي بها الفريق المعني بمكافحة إساءة استعمال المراسلة

معايير الخروج والدخول والعلاج وتوعية المشترك

مقدمة

نظراً لتزايد إساءة استعمال شبكات المشترك، يتعين على موردي خدمة الإنترنت إنفاذ المزيد من التدابير الاستباقية سعياً إلى حماية شبكاتهم والحركة الناشئة منها. فقد تزايد استخدام مجموعات برمجيات التسلل "Bots" أو شبكات برمجيات التسلل "botnets" الآلية من جانب مرسلي الرسائل الاقتحامية والمحتالين لإساءة استعمال الشبكة من خلال نشر الرسائل الاقتحامية والفيروسات وغير ذلك من البرمجيات الضارة. وتوضع هذه البرمجيات الضارة بصورة متخفية على الحواسيب الشخصية للمشتركين دون معرفتهم، ولذا فإن المشتركين المستعملين يكونون مستهدفين بصورة عالية على أنهم ضالعون دون أن يدروا في هذه الشبكات الضارة.

وسعياً إلى تعزيز مهمة فريق العمل المعني بمكافحة إساءة استعمال المراسلة (MAAWG) في المحافظة على المراسلة الإلكترونية من عمليات الاستغلال والإساءة على الخط، توصي اللجنة الفرعية لمكافحة البرمجيات الاقتحامية والزومبي "Zombie" التابعة لفريق العمل المعني بمكافحة إساءة استعمال المراسلة بأفضل الممارسات التالية من حيث علاقتها بتنفيذ البيئات المحصنة. وتشير البيئة المحصنة إلى البيئة التي تتحكم في المعلومات والخدمات التي يُسمح للمشترك باستخدامها والتي يمنح فيها تصاريح النفاذ إلى الشبكة. والهدف الرئيسي لهذه الممارسات هو مساعدة المستعملين النهائيين على الإحاطة بالبرامج غير المطلوبة أو البرمجيات الضارة الموجودة على حواسيبهم الشخصية وإزالتها، ووقف استخدام الشبكة في أغراض مسيئة. وتقع مسؤولية تنفيذ جميع التوصيات على عاتق موردي خدمات الإنترنت ما لم يذكر غير ذلك.

ويفسر استعمال تعاريف الكلمات الرئيسية مثل **يجب** و**ينبغي** و**يجوز** الواردة في أنحاء هذه الوثيقة حسبما هو موصوف في الوثيقة RFC 2119.

أولاً يجب أن تكون معايير الخروج والدخول في البيئة المحصنة موجزة

سعياً إلى توعية المستعملين بالمخاطر والقضايا ذات الصلة بالبرمجيات الضارة التي تصيب الحاسوب الشخصي، **يجوز** لموردي خدمة الإنترنت تنفيذ بيئة محصنة لحسابات المستعملين الجدد أو أي حساب يرون أنه ينطوي على مخاطر أو يحدث حركة مثيرة للشك. و**ينبغي** أن تكون معايير الدخول والخروج من البيئة المحصنة واضحة وموجزة حتى يمكن أن يفهمها المستعمل النهائي.

موجز التوصيات

أ) **يجب** تقديم إشعار واضح عن المشكلة موضع الشك مثل استخدام الشبكة خارج سياسة الاستعمال المقبول، كما **يجب** تقديم توضيح للإشعار، وعرض عام للعملية الموصى بها لعلاج أو تطهير الحاسوب من البرمجيات الضارة.

ب) **يجوز** إعادة توجيه HTTP [80] لتناسب العنوان على الويب المعزول الملائم أو الموقع على الويب على التوالي.

ج) **يجوز** إعادة توجيه أمر برمجيات التسلل أو حركة التحكم إلى شبكة رصد المقتحمين لتحليلها.

د) **يجب** إدارة جميع SMTP [25] في منطقة معزولة أو عامل نقل رسائل رصد المقتحمين.

هـ) **يجب** إتاحة الفرار الفوري المعتمد على الثقة. ويمكن تأكيد الثقة من خلال إجراء بين الحاسوب الشخصي النظيف أو طلب استخدام الشبكة "كما هي" لفترة معينة من الزمن.

و) **يجوز** توفير الخروج في حالة موافقة مورد خدمة الإنترنت على عملية التطهير أو يجري تحميل برمجيات أمنية وتركيبها.

ز) **يجوز** لمورد خدمة الإنترنت أن يستخدم القياسات الداخلية لسمعة المشترك (تحدد باستخدام تقنيات الرصد مثل مرشاح المحتوى وتفتيش الرزم العميقة وأنماط استعمال السلوك) لإحداث الدخول أو الخروج من البيئة المحصنة.

ح) **يجوز** لمورد خدمة الإنترنت أن يستخدم التكنولوجيات للتحديد الأوتوماتي لهوية الوضع الأمني للمشترك على النحو المعلن عنه ببرمجيات العميل المشترك المركبة والموثوق بها.

ثانياً يجب أن تكون تجارب المعالجة ملائمة للمستعمل النهائي

من المهم، مع مواصلة موردي خدمة الإنترنت جهودهم لحماية شبكاتهم والمشتركين فيها من إساءة الاستعمال الضارة، أن يقوم هؤلاء الموردين بذلك بطريقة لا تسبب مضايقات لا داعي لها للمستعملين النهائيين. و**يجوز** لمورد خدمة الإنترنت، كجزء من الاستثمار، أن يختار أيضاً إتاحة أدوات المعالجة بتكلفة يتحملها المستعمل النهائي. و**يجب** أن تتاح هذه الأدوات بوسائل تتفق مع بيئة الدعم النمطية لمورد خدمة الإنترنت. وعلاوة على ذلك، **يجب** أن تتيح البيئة المحصنة النفاذ إلى مواقع الويب لكي يتمكن المستعمل النهائي من تحميل وسائل التحديث والمستخرجات المتعلقة بالبرمجيات الأساسية والمنطبقة سواء من خلال النفاذ المباشر أو عن طريق آليات التوصيل بالوكالة غير المباشرة. (يعني ذلك إمكانية أن يقدم المورد أو مورد خدمات التطبيقات (ASP) المتعاقد المعالجة عن طريق منفذ واحد مثلما يفعل مايكروسوفت مع تحديث Windows لديه وتحميلاتها المتعددة من الموجه الجديد لإجراء ذلك بنفسه).

موجز التوصيات

أ) **يجب** التمكن من تقديم بدائل العلاج دون مقابل أو المعتمدة على رسوم (أو وصلات إلى الأدوات المتاحة على الخط).

ب) **يجب** توفير معلومات معترف بها تضفي الشرعية على الخبرات مثلما الحال في إشعار وعملية العلاج من جانب مورد خدمة الإنترنت الرسمي. وتتضمن الأمثلة على هذه المعلومات بيانات مثل رقم الحساب أو رد على سؤال سري.

ج) **يجب** توفير تفاصيل عن كيفية الاتصال بجهات دعم العملاء للحصول على مساعدة.

د) **ينبغي** ألاّ يلزم تشغيل الحاسوب الشخصي للمستعمل النهائي حتى تتحقق تجربة العلاج.

هـ) **يجب** توفير وصلات إلى العناوين على الإنترنت URL والميادين التي تساعد في تسوية الظروف غير المطلوبة برفع OS والتحديثات الأمنية (إذا كان ذلك ملائماً).

و) **ينبغي** توفير إمكانية "أنقر لتبادل الحديث مع دعم العملاء" أو **ينبغي** قيام طرف ثالث بتقديم خدمة العميل نيابة عن مورد خدمة الإنترنت.

ز) **ينبغي** توفير الدعم من مورد خدمة الإنترنت أو معلومات عن جهة الاتصال في حالة إساءة الاستعمال (مثل رقم الهاتف).

ح) **ينبغي** إصدار تعليمات للعملاء بإرسال حركة SMTP [25] الضارة لإعادة تشكيل عوامل مستعملي البريد لإرسال حركة بريد إلكتروني الخارجة إلى المنفذ 587.

ط) **ينبغي** تقديم تجارب العلاج الفريدة بحسب الظروف غير المطلوبة والتدابير السابقة للمستعمل أي **ينبغي** أن ينظر المستعمل إلى التجربة التي توفر حلاً للمشكلة المحددة أو نمط البرمجيات الضارة المشكوك فيها.

ي) **ينبغي** توفير عميل أمني يكون أقل ما يكون اقتحاماً ويحمَّل بسرعة ويجري تركيبه بسهولة دون تضارب مع برمجيات التطبيق الأخرى مثل العميل الأمني المشكل بالفعل، ولا يتطلب إعادة تشغيل ولا يتطلب مسحاً كاملاً للحاسوب لرصد وإزالة البرمجيات الضارة.

ك) **يجب** السماح باستثناءات إعادة التوجيه لكي يسمح للمستعمل باستخدام خدمات الطوارئ على الخط.

ثالثاً ينبغي أن تكون توعية المستعمل النهائي محور تركيز رئيسياً

نظراً لأن المستعمل النهائي هو عادةً الحلقة الضعيفة في سلسلة الأمن، **ينبغي** لمورد خدمة الإنترنت أن يبذل جهوداً معقولة لإتاحة وثائق معلومات على موقعه على الويب حتى يمكن للمستعمل النهائي أن يتثقف بصورة استباقية بشأن كيفية التخفيف من مخاطر البرمجيات الضارة. وعلى ذلك، **ينبغي** توفير وثائق معلومات في شكل الأسئلة التي تتردد كثيراً وأشرطة الفيديو الداعمة والدروس التدريبية وقواعد المعارف المعدة للبحث، للمستعمل النهائي بطريقة متسقة مع السطح البيني لخدمة العملاء لدى مورد خدمة الإنترنت. وعلاوة على ذلك، **ينبغي** أن تكون الوثائق المتاحة واسعة بصورة تكفل تغطية التطبيقات عبر الأنماط المختلفة العديدة لتكنولوجيات الإنترنت وعبر الأنماط المختلفة العديدة لخدمات الحاسوب (مثل ويندوز وماك ولينوكس).

موجز التوصيات

أ) **يجب** تقديم معلومات معترف بها تضفي الشرعية على التجربة مثل إشعار رسمي أو عملية رسمية للعلاج يوفرهما مورد خدمة الإنترنت. وتشمل الأمثلة على هذه المعلومات البيانات مثل رقم الحساب أو الرد على سؤال سري.

ب) **ينبغي** توفير التوعية البديهية للمستعمل عن طريق الأسئلة كثيرة التردد والدروس التدريبية.

ج) **ينبغي** توفير أدوات بديلة لمركز التعليم مثل مراكز التحية ومعارف البحث بأشرطة الفيديو البسيطة.

د) **ينبغي** توفير معلومات تعليمية عن الأنماط المتعددة للتطبيقات بما في ذلك البريد الإلكتروني (POP3/SMTP) والتصفح (HTTP).