دراسة حالة

عندما استُهدف مطار لندن في هجوم إلكتروني مدمر، اكتشفت طابعات HP هذا التهديد

التقرير النهائي الرسمي لاختراق البيانات

الصناعة
الطيران

الهدف
التعرُّف على الارتباطات الضعيفة في ممارسات أمان الإنترنت ومعالجتها

المنهج
وضع خطة أمان شاملة بالمشاركة مع خبراء الأمان من HP

تكنولوجيا المعلومات ذات أهمية
- إجراءات الأمان المطبقة على النقاط الطرفية في إنترنت الأشياء
- ميزات الأمان المضمّنة الممكنة في
- طابعات HP
- تحسين مراقبة الأمان في الشبكة

العمل ذو أهمية
تحسين أمان الإنترنت لحماية البنية الدولية المهمة والمحافظة على سلامة المسافرين

نظرة عامة

يخدم مطار لندن* أكثر من ٣٠٠٠٠٠ مسافر كل يوم أثناء سفرهم إلى ٩٤ دولة حول العالم. ويعمل في المطار ما يقرب من ٥٠٠٠٠ ألف شخص من ٣٠٠ شركة، مما يجعله مدينة مصغرة.

ومع نمو المطار، أصبحت بنيته التحتية متصلة ومؤتمتة بشكل متزايد. وأصبحت الأنظمة الداخلية بدءًا من نظام التدفئة والتهوية والتكييف مرورًا بالإضاءة إلى الطابعات على شبكة المطار حاليًا. إذ يتم إجراء الطباعة والمسح الضوئي والنسخ من خلال أسطول يضم أكثر من ٦٠ طابعة متعددة الوظائف من HP منتشرة في جميع أنحاء المطار.

وفي ٢٣ أبريل ٢٠١٨، استخدام إرهابي الإنترنت المعروف باسم The Wolf أنظمة الإضاءة المتصلة بالمطار للوصول إلى الشبكة ونشر برامجه الضارة عليها. ونظرًا لأنه معروف بانتهازيته باستخدام النقاط الطرفية غير المؤمّنة، لجأ خبراء أمان تكنولوجيا المعلومات على الفور إلى سجلات التهديد بطابعات HP Enterprise لديهم كجزء من التحقيق لعزل الهجوم وإيقافه. والمثير للدهشة أن السجلات احتوت على أدلة من The Wolf حول مكان التدخل. وبعد ذلك، لجأ مطار لندن إلى شركة HP لزيادة أمان النقاط الطرفية لديه.

ماذا حدث

بمجرد عثور The Wolf ثغرة أمنية، كأن تكون عن طريق رسائل بريد إلكتروني احتيالية للمستخدمين على الشبكة، استطاع أن يصيب نظام الإضاءة بإنترنت الأشياء ببرامج ضارة. وتمكن بعد ذلك من توسيع نطاق برامجه الضارة عبر الشبكة وإنشاء موطئ قدم في أجهزة النقاط الطرفية الأخرى غير المراقبة.

وعن طريق إخفاء وجوده في أجهزة إنترنت الأشياء غير المراقبة، لا يتم اكتشاف فريق The Wolf من قبل أنظمة مراقبة الشبكات أثناء تطويرهم نقاط انطلاق متعددة للقيام بهجوم مدمر كبير.

وقد وجدت إدارة المطار نفسها أمام محاولة يائسة باضطرارها إغلاق أنظمة متعددة مع الحفاظ على البنية التحتية المهمة، مثل حركة الطائرات والمسافرين.

الرد على الهجوم

تم استئجار The Wolf لمهاجمة شبكة المطار. وقد كان موظفو أمان تكنولوجيا المعلومات في المطار يعتقدون أن شبكة المطار محمية بشكل جيد ضد المتسللين، لكنهم لم يتمكنوا من رؤية التهديدات المختبئة في أجهزة إنترنت الأشياء.

ولحسن الحظ، كانت طابعات HP Enterprise الموجودة في المطار تتضمن HP Connection Inspector الذي أوقف البرامج الضارة عندما قامت بمحاولات مشبوهة للوصول إلى "غرفة الاتصالات" وخوادم التحكم وإخضاعها لأوامر المتسللين.

تم تسجيل الإجراءات في سجلات نظام الطابعة. وبمجرد إدراك موظفي تكنولوجيا المعلومات بوجود خطأ ما، قاموا بفحص سجلات النظام للحصول على تفاصيل حول الهجوم. لكن عامل الوقت يعد مهمًا للغاية عند انتشار البرامج الضارة على الشبكة. وإذا كان موظفو أمان تكنولوجيا المعلومات قد وصلوا سجلات النظام الخاصة باكتشاف التهديدات للطابعات بنظام معلومات الأمان ومراقبة الأحداث (SIEM)، كان سيتم تنبيههم فور حدوث التدخل.

أمان أقوى من أي وقت مضى

بعد الاختراق، راجع موظفو تكنولوجيا المعلومات ممارسات الأمان مع موفر خدمات الطباعة المدارة و HP Security Advisors.

بفضل تثبيت طابعات HP Enterprise، كان مطار لندن بالفعل على المسار الصحيح. إذ لا توفر إلا طابعات HP Enterprise العادية ومتعددة الوظائف فقط إمكانية اكتشاف التدخل وقت التشغيل و HP Connection Inspector لاكتشاف البرامج الضارة وإيقافها أثناء العمليات وفرض إعادة التشغيل. فعند بدء التشغيل، تفحص تقنية HP Sure Start نظام BIOS، كما يمكنها الإصلاح الذاتي في حالة اختراق التعليمات البرمجية بينما تفحص ميزة الإدراج في القائمة البيضاء البرنامج الثابت.

وقد نشر موفر خدمات الطباعة المُدارة HP JetAdvantage Security Manager للتحقق من إعدادات الأمان تلقائيًا في كل مرة تتم فيها إعادة تشغيل الطابعة وإعادة ضبط أي إعدادات تم تغييرها.

وقد اتخذ موظفو أمان تكنولوجيا المعلومات في المطار خطوة لتوصيل سجلات الطابعة بأداة SIEM لديهم. وخلافًا للطابعات من شركات مصنّعة أخرى، يمكن لأجهزة HP تقديم سجلات خاصة بالتهديدات للعديد من أدوات SIEM كي يتمكن موظفو تكنولوجيا المعلومات من الحصول على تنبيهات في الوقت الحقيقي بشأن حوادث الأمان المحتملة. وهذا يحول طابعات HP إلى "عيون" لا تقدر بثمن على الشبكات الموجودة بها.

الخاتمة

بسبب طابعات HP Enterprise بالمطار والقرائن التي تركها The Wolf، تمكن فريق الأمان من عزل الهجوم بسرعة كافية لتجنب تعطيل العمليات والدعاية السلبية وغرامات عدم الامتثال وأضرار العلامة التجارية.

وبفضل استخدام ممارسات أمان أقوى والاستفادة الكاملة من ميزات الأمان المضمّنة في طابعات HP، استطاع المطار تعزيز الأمان في جميع أنحاء الشبكة.

**مطار لندن هو مؤسسة خيالية تم استهدافها في هجوم إلكتروني كبير، يمكنك مشاهدته في فيلم HP Studio باسم "THE WOLF: TRUE ALPHA".*

لمزيد من المعلومات حول حلول HP:
أمان الطباعة: hp.com/go/reinventsecurity
أمان الكمبيوتر: hp.com/go/ComputerSecurity

لمشاهدة أفلام "The Wolf"، زر موقع:
hp.com/thewolf

التسجيل للحصول على التحديثات
hp.com/go/getupdated

المشاركة مع الزملاء

4AA7-3560ARE، أغسطس ٢٠١٨