دراسة حالة

يُظهر اختبار الاختراق تعرض شركة Torvik Industries لاختراق في أمان الإنترنت من قبل The Wolf كان من الممكن إيقافه عن طريق طابعات HP

التقرير النهائي الرسمي لاختراق البيانات

الصناعة
الشحن

الهدف
تحليل مشاكل نقاط ضعف الشبكات وحلها

المنهج
اختبار مدى الاختراق للعثور على نقاط الضعف التي تؤدي إلى الهجوم

النتائج والتوصيات
- تثقيف المستخدمين ليكونوا حذرين من فتح رسائل البريد الإلكتروني المشبوهة ومرفقات الطباعة
- نشر طابعات HP التي يمكنها اكتشاف التهديدات
- تكوين جميع النقاط الطرفية المتعلقة بالأمان، بما في ذلك البنية الأساسية التي تم نقلها أو في أماكن مؤقتة

العمل ذو أهمية
طبِّق إجراءات أمان أقوى لتجنب توقف التشغيل وتحسين ثقة العلامة التجارية. وحسّن السياسات لمراقبة النقاط الطرفية للشبكة في الأماكن المؤقتة.

نظرة عامة

تشحن شركة Torvik Industries* نحو ٨ ملايين حاوية سنويًا. وتعتبر شركة Torvik -بالنسبة لنحو ٢٢٠٠٠ شركة مصنِّعة وتاجر جملة- حلقة الوصل الحيوية بين المنتجات والمستهلكين في جميع أنحاء العالم. وتضم ممتلكات الشركة ساحات الشحن والسفن والمستودعات وجميع التقنيات التي تدعم شبكة Torvik المنتشرة على نطاق واسع.

ومع نمو الشركة، بذلت البنية التقنية للشركة قصارى جهدها من أجل التكيف. وعلى الرغم من قيام موظفي أمان تكنولوجيا المعلومات بتكوين خوادم الشركة، إلا أن بعض الطابعات في مكاتب الأقمار الصناعية أو المواقع المؤقتة تتم إدارتها بشكل غير آمن.

وفي ٢٣ أبريل ٢٠١٨، استغل إرهابي الإنترنت -المعروف باسم "The Wolf"- طابعة غير مؤمّنة لتخريب العمليات في شركة Torvik Industries بدءًا من الرافعات إلى سفن الحاويات. وفي الوقت ذاته، أجرى مستشار الأمان لدى الشركة اختبار الاختراق لتحليل الحدث وقدم توصيات لزيادة الأمان وتدريب الموظفين.

ماذا حدث

استُخدمت قيادة Torvik Industries في توجيه التصويبات في الألعاب ذات الرهانات العالية، ولم يتوقعوا أن يتسلل المتسللون إلى شبكتهم بعمق بحيث يتمكنوا من إغلاق الرافعات الجسرية للشركة وإعادة توجيه السفن في المحيط المفتوح.

وكل ما كان يتعين على The Wolf فعله هو اختراق طابعة تنسيقات عريضة في موقع بناء. ثم استطاع التنقل خفية عبر شبكة الشركة إلى الأهداف الكبيرة في عمليات الشركة. وفي لحظة ما، واجهت شركة الشحن الرائدة هذه اضطرابات تشغيلية هائلة ومراقبة دولية مكثفة، فضلاً عن غضب آلاف العملاء.

كيف حدث ذلك

اعتقد موظفو أمان تكنولوجيا المعلومات بالشركة بأنهم يتمتعون بحماية فائقة. وقد رصدت فرقهم التقنية واللوجستية العمليات العالمية لمشاكل الأمان المحتملة بشكل مستمر. وكانوا يتبعون إجراءات أمان في النقاط الطرفية، مثل الطابعات. لكنهم تجاهلوا شيئًا هو: تكوين أمان طابعة التنسيقات العريضة الموضوعة بشكل مؤقت في مقطورة بناء.

لم يتمكن المتسلل من الوصول إلى الطابعة مباشرة، لكنه ببساطة أرسل رسالة بريد إلكتروني تحتوي على مرفق PDF لموظف Torvik المسؤول عن طباعة المستندات ذات التنسيقات العريضة. كان ملف PDF يحمل ملف Postscript مسلحًا مخفيًا يمكنه فتح نفسه وتشغيله عند إرسال ملف PDF إلى الطابعة. وبمجرد إرسال الموظف لمهمة الطباعة، يتم تضمين البرنامج الضار في الطابعة، ثم ينتشر عبر الشبكة. ومن خلال وضع البرامج الضارة على ملحق بريد إلكتروني يبدو بريئًا، تجاوز المتسلل برنامج مكافحة البرامج الضارة على أجهزة كمبيوتر الشركة.

لقد كان الاختراق ممكنًا نظرًا لعدم امتلاك طابعة التنسيقات العريضة أمانًا قويًا مضمّنًا، مثل اكتشاف التهديد. بالإضافة إلى ذلك، فشلت الشركة في مراقبة وإدارة تكوين كل طابعة بمفردها عبر الأسطول، مثل تلك الموضوعة مؤقتًا في مكاتب الأقمار الصناعية.

إصلاح الاختراق

استعانت شركة Torvik Industries بشركة رائدة لاختبار الاختراق بهدف إجراء تحليل دقيق لأمان الإنترنت في الشركة.

وقد أوصى فريق اختبار الاختراق بتثبيت طابعات HP مزوّدة بميزات أمان مضمّنة، بما في ذلك سلسلة HP DesignJet المزوّدة بميزة "التمهيد الآمن" وإدراج البرنامج الثابت في القائمة البيضاء. فهذه الميزات تساعد الطابعة في اكتشاف التعليمات البرمجية الضارة وتوقف تشغيلها، ثم تنبه قسم تكنولوجيا المعلومات إلى الحاجة إلى إعادة تثبيت برنامج ثابت سليم من HP.

كما أوصوا باستخدام ميزة "الأمان الفوري" الموجودة في HP JetAdvantage Security Manager، فهو برنامج لإدارة الأمان على مستوى الأسطول لتطبيق سياسات الأمان تلقائيًا بمجرد إضافة الأجهزة إلى الشبكة. ويمكن أيضًا لبرنامج HP Security Manager إنشاء تقارير الامتثال التي تظهر كل طابعة من HP حتى إذا كانت بعيدة أو في أماكن مؤقتة. وهذا من شأنه أن يساعد في إثبات المحافظة على تكوينات أمان الأسطول.

وبالإضافة إلى ذلك، اقترح مستشار الأمان برنامجًا تعليميًا لمساعدة الموظفين في التعرّف على رسائل البريد الإلكتروني المشبوهة وتجنب طباعة مرفقات غير معروفة.

الخاتمة

لا تزال شركة Torvik Industries تعاني من آثار خرق أمان الإنترنت الذي أثر على العمليات، فضلاً عن الدعاية القوية لآراء رئيسها غير التقليدية والأعمال الإجرامية. وفي الوقت الذي تسعى فيه الشركة إلى تطوير اتجاه جديد في ريادتها، نجد اتجاه أمان الإنترنت واضحًا: فالتحول إلى طابعات HP وحلولها سيساعد في هزيمة Wolf القادم الذي يتلهف للصيد.

Torvik Industries هي شركة خيالية تم استهدافها في هجوم إلكتروني كبير، يمكنك مشاهدته في فيلم *HP Studio* باسم *"THE WOLF: TRUE ALPHA"*.

لمزيد من المعلومات حول حلول HP:
HP DesignJet: hp.com/go/designjetsecurity
أمان الطباعة: hp.com/go/reinventsecurity

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

التسجيل للحصول على التحديثات
hp.com/go/getupdated

المشاركة مع الزملاء

حقوق الطبع والنشر © لشركة HP Development Company, L.P لعام ٢٠١٨. المعلومات الواردة بهذه الوثيقة عرضة للتغيير بدون إشعار. وتقتصر الضمانات الخاصة بمنتجات وخدمات شركة HP على تلك المنصوص عليها في بيانات الضمان الصريحة المرفقة بتلك المنتجات والخدمات. ويجب عدم تفسير أي مما ورد هنا على أنه يشكل ضمانًا إضافيًا. وتخلي شركة HP مسؤوليتها عن أي أخطاء فنية أو تحريرية أو أي أخطاء ناتجة عن السهو والإغفال وردت في هذا المستند.

4AA7-3562ARE، أغسطس ٢٠١٨