منشور دعائيّ

حصّن نفسك من هجمات The Wolf

مخاطر الأمان في أفلام "The Wolf" وحلول HP

جدران الحماية لا يمكنها الصمود وحدها أمام الهجمات المتطورة من قبل المتسللين، مثل The Wolf. لذا، يتعين عليك استخدام عدة طبقات من الحماية عند كل جهاز طرفي في البنية الأساسية. ساعد في حماية أجهزتك وبياناتك وهوياتك ومستنداتك باستخدام حلول الأمان من HP.

الموسم 1 The Wolf

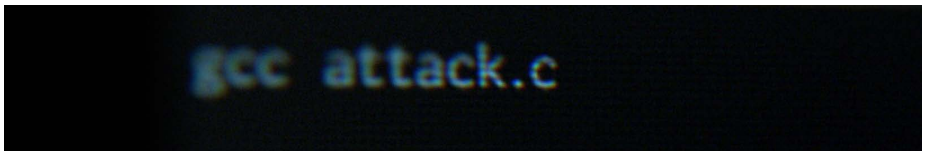
يخترق "The Wolf" مؤسسة مالية عالمية عن طريق استغلال نقاط الضعف بها. إذ يستخدم جهازًا محمولاً للوصول إلى الطابعة وينشر برنامجًا ضارًا لاعتراض البيانات وقراءتها. وبعد ذلك، يستخدم The Wolf بريدًا إلكترونيًا "للتصيد الاحتيالي" ليخدع مستخدمًا من خلال إرسال تعليمات برمجية ضارة مخفية داخل ملف PDF إلى طابعة.

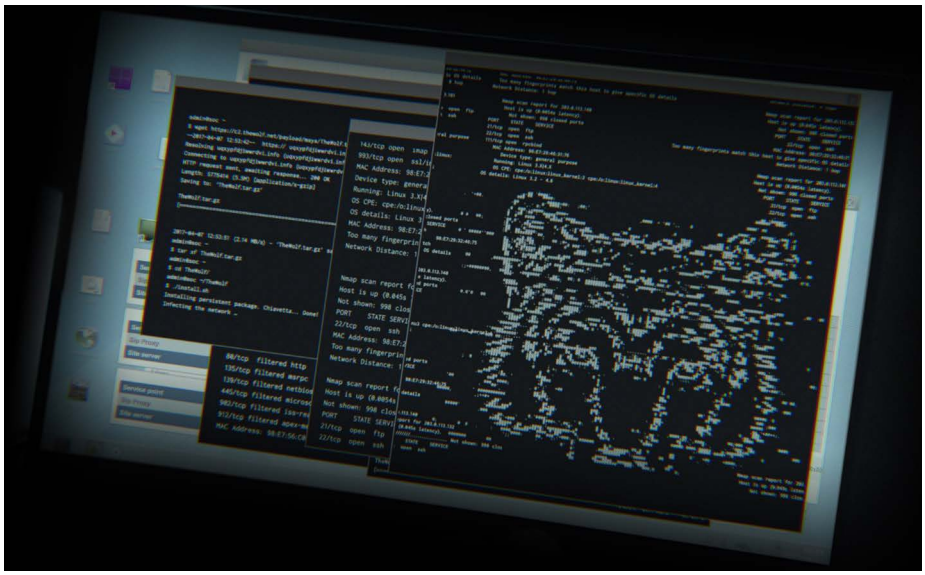
وبالتالي، يخترق البرنامج الضار الموجود على الطابعة جدار الحماية ويصل إلى مستوى BIOS لأجهزة كمبيوتر الشركة بحيث يمكنه جمع البيانات والعودة مجددًا حتى بعد نشر دفاعات الشبكة.

يأخذ The Wolf ورقة مهملة من درج استقبال المطبوعات بالطابعة ويدمر صفقة الشركة القادمة، مما يقضي على ثقة حملة الأسهم.

نقاط الضعف

- تمكين ميزة Wi-Fi أو Bluetooth® بالطابعة دون طلب مصادقة المستخدم
- عدم تشفير ملفات بيانات الطابعات
- عدم تعرف المستخدمين على الرسائل الإلكترونية أو ملفات الطباعة المشبوهة
- عدم وجود حماية من البرامج الضارة على الطابعات وأجهزة الكمبيوتر على مستوى BIOS
- يتم ترك المستندات الحساسة مكشوفة في أدراج استقبال المطبوعات





الموسم 2 استمرار المطاردة

يستهدف "The Wolf" سجلات المرضى المخزنة عن طريق أحد أكبر شركات إدارة السجلات الطبية على مستوى العالم. فهو يخترق جهاز كمبيوتر، ثم يستخدم منفذ USB للطابعة لتحميل البرامج الضارة خلف جدار الحماية للبحث عن الأجهزة المتصلة لاختراقها.

ولأن الطابعة موجودة على شبكة غير مقسّمة، يستطيع "The Wolf" الوصول إلى الخوادم المتصلة بقواعد البيانات المليئة بالمعلومات الحساسة. وبالتالي، يتمكن من سرقة الملايين من سجلات المرضى السرية التي يمكن قراءتها لأن البيانات غير مشفرة.

تتحملان كل من المستشفى وشركة البرامج المسؤولية عن ذلك، كما أنهما تتعرضان لغرامات كبيرة فضلاً عن النيل من سمعتهما.

نقاط الضعف

- عدم طلب منفذ USB بالطابعة المصادقة
- عدم تشفير ملفات البيانات
- عدم وجود حماية من البرامج الضارة على الطابعات
- عدم مراقبة الطابعة بحثًا عن حوادث الأمان

الموسم 3 True Alpha

يعطل The Wolf العمليات في واحدة من أكبر شركات الشحن في العالم وكذلك العمليات في مطار دولي.

فمن خلال إرساله ملف PDF يبدو موثوقًا به بالبريد الإلكتروني، يخدع موظفًا لدى مكتب في شركة الشحن لإرسال ملف Postscript مفخخ إلى طابعة ما. تنتشر البرامج الضارة الخفية في جميع أنحاء الشبكة عند إرسال الملف إلى الطابعة، حيث يظل غير مكتشف. وقريباً، سيستطيع The Wolf الوصول إلى العرض التقديمي للمؤتمر رفيع المستوى الذي يقدمه المدير التنفيذي والرافعات التي تحمّل البضائع في الميناء وبرنامج الربان الآلي للسفن في البحر.

وبعد ذلك، يركز The Wolf على مطار رئيسي، ويظهر قدرته على التحكم في الإضاءة وعلى الأرجح العديد من الأنظمة المهمة في شبكة المطار. ولكن طابعات HP ساعدت موظفي تكنولوجيا المعلومات في التحقيق ووقف الهجوم.

نقاط الضعف

- إضافة الطابعات الموجودة في المواقع المؤقتة إلى الشبكة دون تكوين الأمان بشكل كافٍ
- عدم احتواء أجهزة الكمبيوتر على أي حماية للتصفح عبر الإنترنت ضد التنزيلات غير المقصودة
- عدم مراقبة أجهزة إنترنت الأشياء وعدم اشتمالها على إمكانات الكشف عن البرامج الضارة
- عدم اتصال "سجلات النظام" للطابعة بأدوات مراقبة التهديدات

كيف يمكنك الحماية من هجمات مماثلة؟

حماية الهوية: طوّر نظام الأمان لتسجيل الدخول باستخدام مصادقة متعددة العوامل على أجهزة كمبيوتر HP Elite.

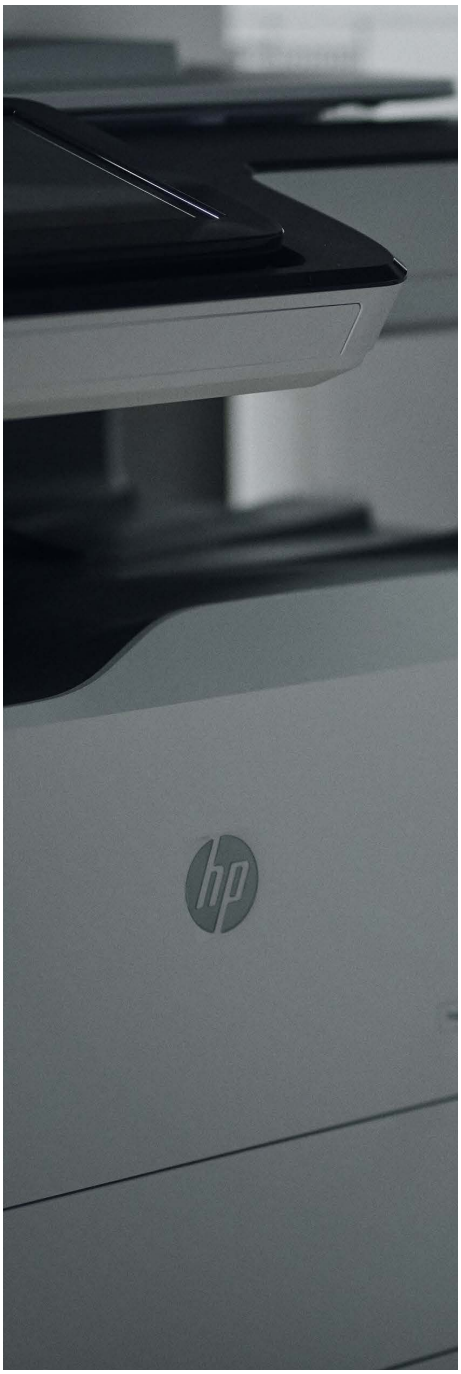
حماية الجهاز: اعمل على الترقية إلى أجهزة كمبيوتر HP Elite وطابعات HP Enterprise العادية ومتعددة المهام باستخدام أساليب الحماية من البرامج الضارة لاكتشاف الهجمات وإيقافها واستعادة الأنظمة بعد الهجمات. أغلق منافذ USB غير المستخدمة أو تحكم في الوصول باستخدام عناصر تحكم المستخدم. اعزل علامات تبويب المستعرض فعليًا عن طريق HP Sure Click لمنع البرامج الضارة النشطة على الويب من الانتشار.[1]

حماية البيانات: استخدم حلول المصادقة وتشفير الطابعة، مثل HP Access Control.[2] واطلب مصادقة المستخدم واعمل على تشفير البيانات عند استخدام خاصيتي Wi-Fi و Bluetooth بالطابعة. استخدم حل مصادقة وتشفير محمول، مثل PrinterOn Enterprise. اعمل على تشفير البيانات أثناء تخزينها ونقلها.

حماية المستند: استخدم حل طباعة عن طريق السحب، مثل HP Access Control.[2]

تحسين المراقبة والإدارة: يمكنك تكوين سياسات أمان الأسطول تلقائيًا باستخدام HP SecurityAdvantage Security Manager[3] أو HP Printer Security-Plug for Microsoft® SCCM للطابعات ومجموعة HP Manageability Integration Kit (MIK)[4] لأجهزة الكمبيوتر الشخصية. قم بتمكين "سجلات النظام" لتعقب أحداث الأمان وتوصيل الأجهزة بأدوات إدارة معلومات وأحداث الأمان (SIEM) للحصول على التنبيهات في الوقت الفعلي. انتقل إلى موفر MPS (خدمات طباعة مدارة) مدرب على الأمان من HP لتكوين الطابعات وصيانتها من أجل الحفاظ على الأمان.

اعمل على حماية أعمالك باستخدام أمان شامل من HP



الطباعة الأكثر أمانًا على مستوى العالم[5]

يمكن لطابعات HP Enterprise العادية ومتعددة المهام اكتشاف الهجمات وإيقافها والتعافي منها تلقائيًا دون تدخل قسم تكنولوجيا المعلومات بفضل ميزات اكتشاف الاختراقات وقت التشغيل و HP Sure Start و HP Connection Inspector. بينما تتضمن وسائل الحماية الأخرى محركات أقراص ثابتة مشفرة وبرامج ثابتة قابلة للترقية فضلاً عن إمكانية إرسال تنبيهات الأمان إلى أدوات SIEM.

hp.com/go/PrintersThatProtect

أجهزة الكمبيوتر الأكثر أمانًا ومرونة في الإدارة على مستوى العالم[6]

تساعد أجهزة الكمبيوتر HP Elite في الحماية من معظم التهديدات الأكثر شيوعًا عن طريق التأمين الشامل للنظام. إذ تقوي المصادقة متعددة العوامل حماية الهوية، كما أن HP Manageability Integration Kit[4] تسهل إدارة الأمان عبر أسطول أجهزة الكمبيوتر. وتشمل وسائل الحماية الأخرى تشفير القرص الثابت و HP Sure Recover[7] و HP Sure Click[1] و HP Sure View.

hp.com/go/ComputerSecurity

PrinterOn Enterprise

احصل على طباعة آمنة وموثوقة داخل الشبكة للمؤسسات. تمكن من توصيل أي جهاز مكتبي أو جهاز محمول بالطابعات من بائعين متعددين سواءً داخل أو خارج الشبكة الموثوقة.

hp.com/go/businessmobileprinting

HP Access Control[2]

تمكن من استعادة التحكم وتعزيز الأمان وخفض التكاليف عن طريق تقديم إمكانات المصادقة والتصريح بالطباعة والطباعة بالسحب المستندة جميعها إلى نوعية دور المستخدم عبر مؤسستك بأكملها.

hp.com/go/hpac

HP JetAdvantage Security Manager[3]

تمتع بخفض التكلفة والموارد للحفاظ على أمان الأسطول باستخدام أداة امتثال أمان شامل للطباعة تستند إلى سياسة. أنشئ سياسة أمان على مستوى الأسطول وقم بإجراء معالجة تلقائية لإعدادات الأجهزة وتثبيت شهادات فريدة وتجديدها وإنشاء تقارير امتثال على مستوى الأسطول.

hp.com/go/securitymanager

تعرّف على المزيد من الموقع
hp.com/go/hpsecure

[1] يتوفر HP Sure Click على معظم أجهزة الكمبيوتر من HP، كما أنه يدعم Microsoft® Internet Explorer و™Chromium. تشمل المرفقات المدعومة ملفات Microsoft Office (تطبيقات Word و Excel و PowerPoint) وملفات PDF للقراءة فقط عندما يتم تثبيت Microsoft Office أو Acrobat.

[2] يتعين شراء HP Access Control بشكل منفصل. لمعرفة المزيد، يُرجى زيارة موقع hp.com/go/hpac.

[3] يتعين شراء HP JetAdvantage Security Manager بشكل منفصل. للحصول على تفاصيل، راجع موقع hp.com/go/securitymanager.

[4] مجموعة HP Manageability Integration Kit ليست مثبتة مسبقًا، لكنها متوفرة على الموقع hp.com/go/clientmanagement.

[5] استنادًا إلى مراجعة HP لميزات الأمان التي تم نشرها عام 2018 لطابعات من فئة منافسة. تقدم شركة HP وحدها مجموعة من ميزات الأمان التي يمكنها مراقبة الهجمات واكتشافها وإيقافها تلقائيًا ثم التحقق الذاتي من سلامة البرامج عند إعادة التشغيل. للاطلاع على قائمة الطابعات، تفضل بزيارة: hp.com/go/PrintersThatProtect. للاطلاع على مزيد من المعلومات: hp.com/go/printersecurityclaims.

[6] استنادًا إلى إمكانيات الأمان الفريدة والشاملة من HP المتوفرة دون تكلفة إضافية وإدارة جميع الجوانب المتعلقة بالكمبيوتر من خلال HP Manageability Integration Kit، بما في ذلك الأجهزة ونظام BIOS وإدارة البرامج باستخدام Microsoft® System Center Configuration Manager من خلال الموزعين الذين تزيد مبيعاتهم السنوية عن مليون وحدة اعتبارًا من نوفمبر 2016 من أجهزة الكمبيوتر الشخصية HP Elite المزوّدة بمعالجات Intel® Core® من الجيل السابع والأحدث وبطاقات رسومات مدمجة Intel® وبطاقة Intel® WLAN.

[7] يتوفر HP Sure Recover في أجهزة كمبيوتر HP Elite المزودة بمعالجات Intel® أو AMD من الجيل الثامن، كما يتطلب اتصال شبكة سلكيًا مفتوحًا. وهو غير متوفر في الأنظمة الأساسية المزوّدة بمحركات أقراص متعددة للتخزين الداخلي وذاكرة Intel® Optane™. ويتعين عليك إنشاء نسخة احتياطية لملفاتك وبياناتك وصورك وفيديوهاتك الهامة وما إلى ذلك قبل الاستخدام لتجنب فقد البيانات.

التسجيل للحصول على التحديثات
hp.com/go/getupdated

المشاركة مع الزملاء

4AA7-0231ARE، أغسطس 2018، مراجعة 1