Broschüre

Schützen Sie sich vor The Wolf

Sicherheitsrisiken, gezeigt in den Filmen „The Wolf“, und HP Sicherheitslösungen zu Ihrem Schutz

Firewalls alleine bieten keinen ausreichenden Schutz vor den raffinierten Angriffen von Hackern wie The Wolf. Jedes Netzwerk-Endgerät in Ihrer Infrastruktur muss auf mehreren Ebenen gesichert werden. Schützen Sie Ihre Geräte, Daten, Identitäten und Dokumente mit Sicherheitslösungen von HP.

Teil 1 The Wolf

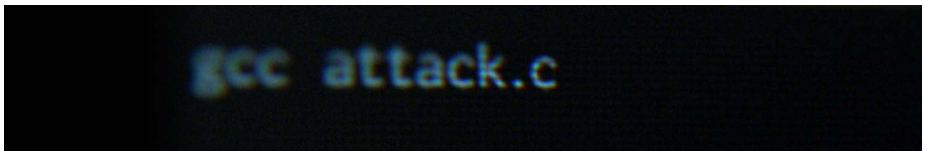
The Wolf bringt einen internationalen Finanzkonzern zu Fall, indem er Schwachstellen von Endgeräten ausnutzt. Er verschafft sich über ein Mobilgerät Zugriff auf einen Drucker und schleust darüber Malware in das Unternehmensnetzwerk ein, um Daten abzufangen und zu lesen. Mithilfe einer Phishing-E-Mail bringt er eine Mitarbeiterin dazu, böswilligen Code, der in einer PDF-Datei verborgen ist, an einen Drucker zu senden.

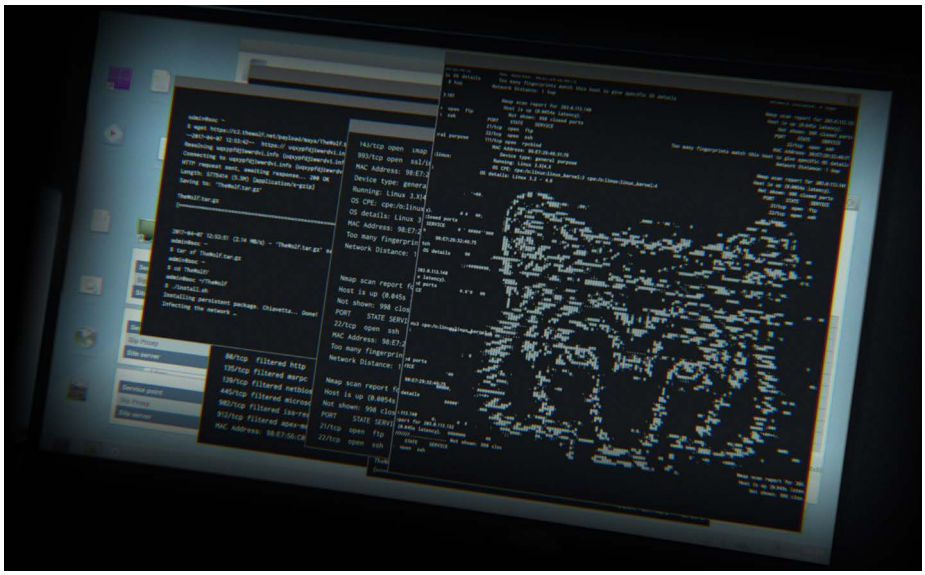
Die Malware im Drucker dringt durch die Firewall hindurch bis zur BIOS-Ebene der Unternehmens-PCs. Dort kann sie Daten sammeln und sich sogar selbst wiederherstellen, wenn sie durch Netzwerkschutzvorkehrungen inaktiviert wurde.

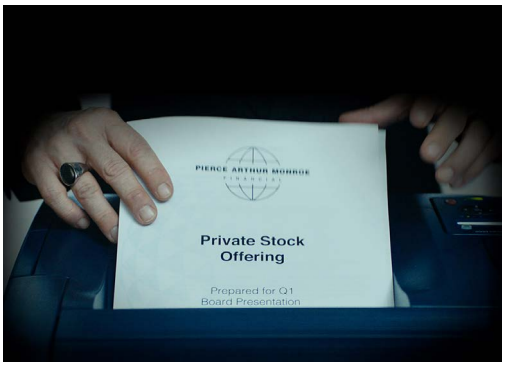
Durch einen im Druckerausgabefach vergessenen Ausdruck gelingt es The Wolf, das bevorstehende Börsengeschäft des Unternehmens zu sabotieren – wodurch das Vertrauen der Investoren von Grund auf erschüttert wird.

Schwachstellen

- Die WLAN- oder Bluetooth®-Schnittstellen von Druckern sind offen und ohne Benutzerauthentifizierung zugänglich.
- Druckerdatendateien sind nicht verschlüsselt.
- Benutzer erkennen verdächtige E-Mails oder Druckdateien nicht.
- Drucker und PCs sind nicht auf BIOS-Ebene gegen Malware geschützt.
- Sensible Dokumente liegen ungeschützt im Ausgabefach.







Teil 2 Die Jagd geht weiter

Diesmal hat es The Wolf auf Patientenakten abgesehen, die bei einem der weltweit größten Aktenverwaltungsunternehmen im medizinischen Bereich gespeichert sind. Er dringt in einen PC ein und lädt über einen USB-Anschluss an einem Drucker Malware hoch, um hinter der Firewall nach vernetzten Geräten zu suchen, die er angreifen kann.

Weil sich der Drucker in einem nicht segmentierten Netzwerk befindet, kann The Wolf auf Server zugreifen, die mit Datenbanken mit sensiblen Informationen verbunden sind. Er stiehlt Millionen von vertraulichen Patientenakten, deren Daten nicht verschlüsselt und damit problemlos lesbar sind.

Sowohl das Krankenhaus als auch das Software-Unternehmen haften für den Schaden und müssen mit beträchtlichen Geldbußen und Rufschädigungen rechnen.

Schwachstellen

- USB-Anschlüsse von Druckern erfordern keine Authentifizierung.
- Datendateien sind nicht verschlüsselt.
- Drucker sind nicht gegen Malware geschützt.
- Drucker werden nicht auf Sicherheitsbedrohungen überwacht.

Teil 3 True Alpha

The Wolf löst Störungen in den Betriebsabläufen bei einer der weltgrößten Reedereien und auf einem internationalen Flughafen aus.

Mithilfe einer harmlos wirkenden PDF-Datei in einer E-Mail erreicht er, dass ein Büromitarbeiter bei der Reederei eine missbräuchliche Postscript-Datei an einen Drucker sendet. Nach dem Versenden der Datei verbreitet sich die darin versteckte Malware über das Netzwerk, wo sie sich unentdeckt festsetzt. Bald verfügt The Wolf über Zugriff auf eine streng vertrauliche Konferenzpräsentation des CEO, auf Kräne, die in einem Hafen Fracht laden, sowie auf die Autopilot-Software von Schiffen auf See.

Als Nächstes nimmt The Wolf einen großen Flughafen ins Visier. Dort demonstriert er seine Fähigkeit, die Beleuchtung zu steuern – und damit potenziell auch diverse kritische Systeme im Flughafennetzwerk zu kontrollieren. Mithilfe von HP Druckern können die IT-Mitarbeiter die Attacke analysieren und stoppen.

Schwachstellen

- Temporär aufgestellte Drucker werden ohne adäquate Sicherheitskonfiguration in das Netzwerk eingebunden.
- PCs besitzen keinen Webbrowsing-Schutz gegen versehentliche Downloads.
- IoT-Geräte werden nicht überwacht und verfügen nicht über Malware-Erkennungsfunktionen.
- Drucker-Systemprotokolle sind nicht mit Tools zur Überwachung von Bedrohungen verbunden.

Wie können Sie sich vor ähnlichen Angriffen schützen?

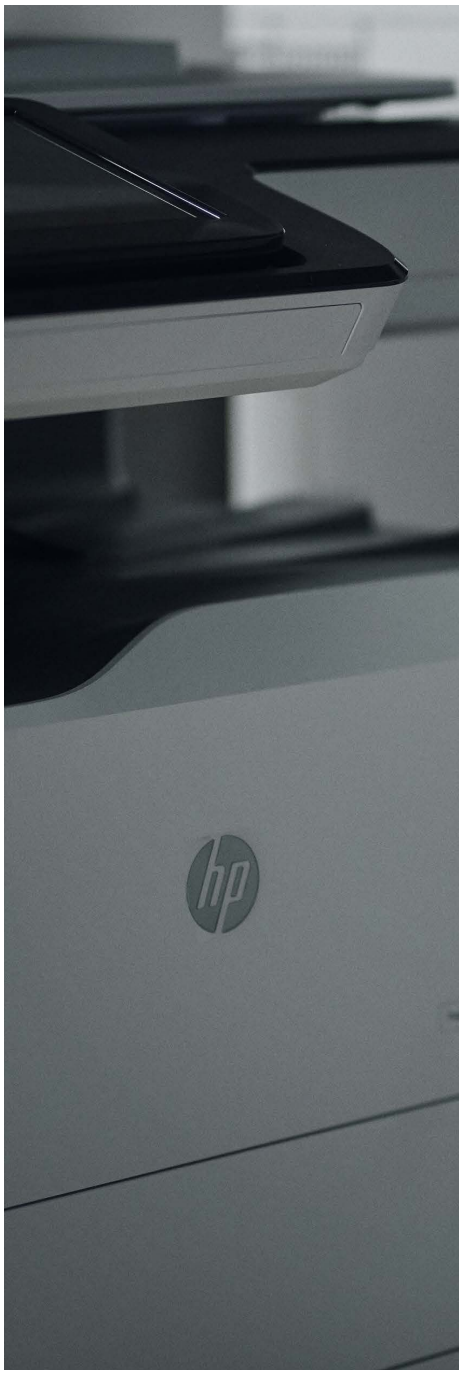
Schützen Sie Identitäten: Erhöhen Sie die Login-Sicherheit mithilfe der speziellen Multi-Faktor-Authentifizierung auf HP Elite-PCs.

Schützen Sie Ihre Geräte: Machen Sie Ihre IT zukunftssicher mit HP Elite-PCs und HP Enterprise-Druckern und -MFPs mit Malware-Schutz, der Angriffe automatisch erkennt, abwehrt und die Funktionalität wiederherstellt. Sperren Sie nicht verwendete USB-Ports oder kontrollieren Sie den Zugriff mithilfe von Benutzereinstellungen. Isolieren Sie Browsertabs physisch mit HP Sure Click, um die Ausbreitung von webbasierter Malware zu verhindern.[1]

Schützen Sie Ihre Daten: Verwenden Sie für Ihre Drucker eine Authentifizierungs- und Verschlüsselungslösung wie HP Access Control.[2] Führen Sie eine obligatorische Benutzerauthentifizierung und Datenverschlüsselung bei Verwendung von WLAN- und Bluetooth-Druckerfunktionen ein. Implementieren Sie eine mobile Authentifizierungs- und Verschlüsselungslösung wie PrinterOn Enterprise. Verschlüsseln Sie Daten bei Speicherung und Übertragung.

Schützen Sie Ihre Dokumente: Implementieren Sie eine Pull-Printing-Lösung wie HP Access Control.[2]

Verbessern Sie die Überwachung und Verwaltung: Konfigurieren Sie automatisch Sicherheitsrichtlinien für die Geräteflotte mit HP JetAdvantage Security Manager[3] oder mit dem HP Printer Security Plug-in for Microsoft® SCCM für Drucker und dem HP Manageability Integration Kit (MIK)[4] für PCs. Aktivieren Sie Systemprotokolle zur Verfolgung von Sicherheitsereignissen und verbinden Sie Ihre Geräte mit Security Information and Event Management-Tools (SIEM) für Echtzeit-Alarmmeldungen. Wenden Sie sich an einen MPS-Anbieter mit spezieller HP Sicherheitsschulung, um Drucker für maximale Sicherheit zu konfigurieren und zu warten.



Schützen Sie Ihr Unternehmen mit den umfassenden Sicherheitsfunktionen von HP

Die weltweit höchste Drucksicherheit[5]

HP Enterprise-Drucker und -MFPs ermöglichen die automatische Erkennung und Abwehr von Angriffen sowie die Wiederherstellung der Funktionalität ohne Eingriffe durch die IT-Abteilung mithilfe von Funktionen wie der Angriffserkennung für die Laufzeitumgebung, HP Sure Start und HP Connection Inspector. Darüber hinaus können Sie weitere Schutzmaßnahmen wie verschlüsselte Festplatten, erweiterbare Firmware und die Funktion zum Senden von Sicherheitswarnungen an SIEM-Tools nutzen.

hp.com/go/PrintersThatProtect

Die sichersten und am einfachsten zu verwaltenden PCs der Welt[6]

HP Elite-PCs bieten Schutz gegen die gängigsten Bedrohungen mit umfassenden Sicherheitslösungen unterhalb, innerhalb und oberhalb der Betriebssystemebene. Die Multi-Faktor-Authentifizierung stärkt den Identitätsschutz und das HP Manageability Integration Kit[4] vereinfacht die Sicherheitsverwaltung für die gesamte PC-Flotte. Als zusätzliche Schutzmechanismen sind Festplattenverschlüsselung, HP Sure Recover[7], HP Sure Click[1] und HP Sure View verfügbar.

hp.com/go/ComputerSecurity

PrinterOn Enterprise

Verlässliches, sicheres mobiles Drucken im Netzwerk für Unternehmen. Verbinden Sie praktisch jeden Desktop und jedes Mobilgerät mit Druckern verschiedener Hersteller innerhalb und außerhalb des vertrauten Netzwerks.

hp.com/go/businessmobileprinting

HP Access Control[2]

Funktionen für rollenbasierte Druckauthentifizierung, Autorisierung und sicheres Pull-Printing im gesamten Unternehmen helfen Ihnen, die Kontrolle zurückzugewinnen, verbessern die Sicherheit und senken die Kosten.

hp.com/go/hpac

HP JetAdvantage Security Manager[3]

Verringern Sie Kosten und Aufwand für die Aufrechterhaltung der Flottensicherheit mit einem umfassenden richtlinienbasierten Tool für Compliance bei der Drucksicherheit. Führen Sie eine flottenweite Sicherheitsrichtlinie ein, automatisieren Sie die Wiederherstellung von Geräteeinstellungen, installieren und erneuern Sie eindeutiger Zertifikate und erstellen Sie flottenweite Compliance-Berichte.

hp.com/go/securitymanager

Weitere Informationen unter
hp.com/go/hpsecure

[1] HP Sure Click ist auf den meisten HP PCs verfügbar und unterstützt Microsoft® Internet Explorer und Chromium™. Geschützte Dateiformate von Anhängen sind Microsoft Office-Dateien (Word, Excel, PowerPoint) und PDF-Dateien im schreibgeschützten Modus, wenn Microsoft Office bzw. Adobe Acrobat installiert ist.

[2] HP Access Control muss separat erworben werden. Weitere Informationen finden Sie unter hp.com/go/hpac.

[3] HP JetAdvantage Security Manager muss separat erworben werden. Nähere Einzelheiten finden Sie unter hp.com/go/securitymanager.

[4] HP Management Integration Kit ist nicht vorinstalliert und kann unter hp.com/go/clientmanagement heruntergeladen werden.

[5] Auf der Basis einer von HP durchgeführten Prüfung der 2018 veröffentlichten Angaben zu Sicherheitsfunktionen von vergleichbaren Druckern anderer Wettbewerber. Nur HP bietet eine Kombination aus Sicherheitsfunktionen, die das Gerät überwachen, Angriffe erkennen und automatisch stoppen und anschließend bei einem Neustart die Integrität der Software eigenständig prüfen können. Eine Liste der Drucker finden Sie hier: hp.com/go/PrintersThatProtect. Weitere Informationen: hp.com/go/printersecurityclaims.

[6] Basierend auf den einzigartigen umfassenden Sicherheitsfunktionen von HP ohne zusätzliche Kosten und der Verwaltung durch das HP Manageability Integration Kit von sämtlichen Aspekten eines PCs, einschließlich Hardware, BIOS und Softwareverwaltung mithilfe des Microsoft System Center Configuration Manager unter Anbietern mit > 1 Million verkaufter Einheiten pro Jahr (Stand: November 2016) von HP Elite PCs mit Intel® Core®-Prozessoren ab der 7. Generation, integrierter Intel®-Grafikkarte und Intel®-WLAN.

[7] HP Sure Recover ist auf HP Elite-PCs mit Intel®- oder AMD®-Prozessoren der 8. Generation verfügbar und erfordert eine offene, kabelgebundene Netzwerkverbindung. Nicht verfügbar für Plattformen mit mehreren internen Speicher-Laufwerken, Intel® Optane™. Vor der Verwendung müssen wichtige Dateien, Daten, Fotos, Videos usw. gesichert werden, um Datenverluste zu vermeiden.

Für aktuelle News anmelden
hp.com/go/getupdated

An Kollegen weiterleiten

4AA7-0231DEE, August 2018, Rev. 1