



Geef The Wolf geen kans

Veiligheidsrisico's in de films over 'The Wolf' en de oplossingen van HP

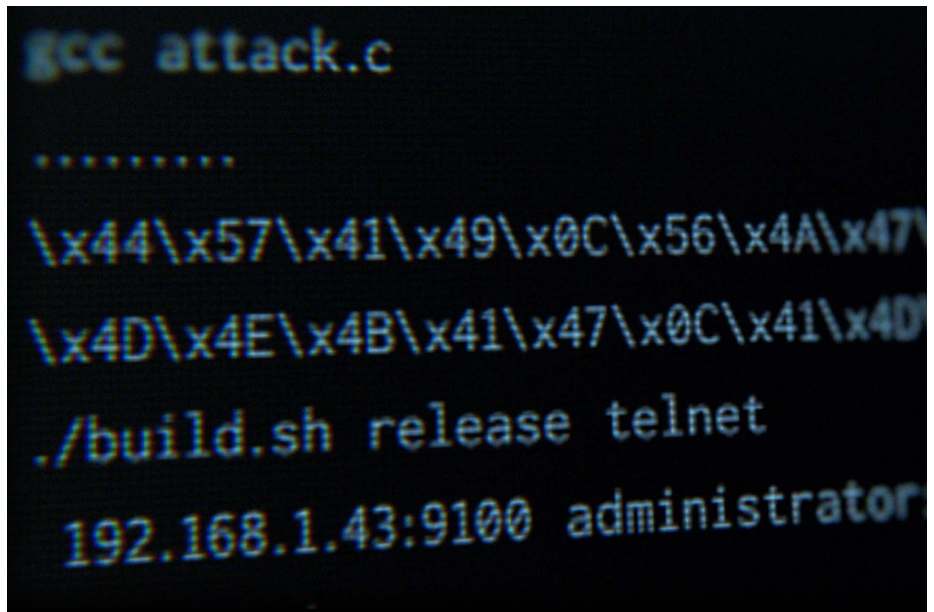
Firewalls alleen zijn niet voldoende om de geraffineerde aanvallen van hackers zoals The Wolf af te slaan. Ieder infrastructuurendpoint moet met meerdere beschermingslagen beveiligd worden. Bescherm uw apparaten, data, identiteit en documenten met beveiligingsoplossingen van HP.

Deel 1 The Wolf

In de eerste film schakelt The Wolf een wereldwijd opererende financiële instelling uit door gebruik te maken van kwetsbare endpoints. The Wolf verschaft zich met een mobiel device toegang tot een printer en infecteert die met malware om data te onderscheppen en te lezen. Vervolgens gebruikt hij een 'phishing'-e-mail om een gebruiker kwaadaardige code, die verborgen is in een printbestand, naar de printer te laten sturen.

De malware in de printer passeert de firewall en verspreidt zich over de pc's in het bedrijf. De code bevindt zich op BIOS-niveau, waardoor deze voortdurend data kan leveren en zichzelf weer kan herstellen nadat netwerkverdediging is geïnstalleerd.

Vervolgens ontdekt The Wolf een vertrouwelijk document in de uitvoerlade van een MFP. Doordat gevoelige data worden gelekt, loopt het bedrijf aanzienlijke financiële en reputatieschade op.



Kwetsbaarheden

- Wifi of Bluetooth® op de printer staat open en er wordt geen gebruikersverificatie gevraagd
- Databestanden op de printer zijn niet versleuteld
- Gebruikers herkennen kwaadaardige e-mails of printbestanden niet
- Printers en pc's hebben geen bescherming tegen malware
- Documenten die in de uitvoerlade achterblijven, kunnen vertrouwelijke informatie bevatten

Hoe kunt u zichzelf tegen dergelijke aanvallen beschermen?

Bescherm uw data: Schakel wifi/Bluetooth uit of laat gebruikers zich authenticeren; gebruik een mobiele verificatie- en encryptie-oplossing zoals HP JetAdvantage Connect of HP Access Control.

Bescherm het apparaat: Upgrade naar HP Elite pc's en HP Enterprise-printers en -MFP's met malwarebescherming om automatisch, zonder tussenkomst van IT, aanvallen te detecteren, te stoppen en ervan te herstellen. HP Sure Start helpt apparaten zichzelf te herstellen door opnieuw op te starten met een veilige, goede kopie van de originele BIOS-code.

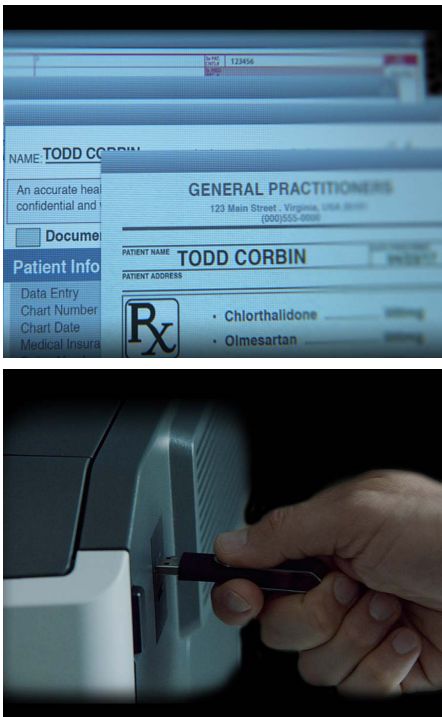
Bescherm de documenten: Installeer een pull-printoplossing zoals HP Access Control of HP JetAdvantage Secure Print.

Deel 2 The Wolf: De jacht gaat door

In de tweede film richt The Wolf zich op patiëntdossiers die zijn opgeslagen bij een van de grootste dossierverwerkingsbedrijven in de medische wereld. Hij hackt een pc en later een printer in het ziekenhuis door malware te uploaden via de USB-poort van de printer.

Omdat de niet-beveiligde printer aangesloten is op het netwerk, bevindt de malware zich al achter de firewall en kan deze direct op zoek gaan naar andere aangesloten apparaten om die ook te besmetten. Omdat de printer zich in een niet-gesegmenteerd netwerk bevindt, heeft The Wolf ook toegang tot servers die verbonden zijn met databases met vertrouwelijke informatie. Hij steelt miljoenen vertrouwelijke patiëntdossiers.

Het ziekenhuis en het softwarebedrijf zijn beide aansprakelijk, krijgen hoge boetes en lopen forse reputatieschade op.



Kwetsbaarheden

- De pc is niet vergrendeld wanneer de gebruiker wegloopt
- De USB-poort van de printer kan zonder authenticatie worden gebruikt
- Databestanden zijn niet versleuteld
- Printers en pc's hebben geen bescherming tegen malware
- Printers worden niet gecontroleerd op beveiligingsincidenten

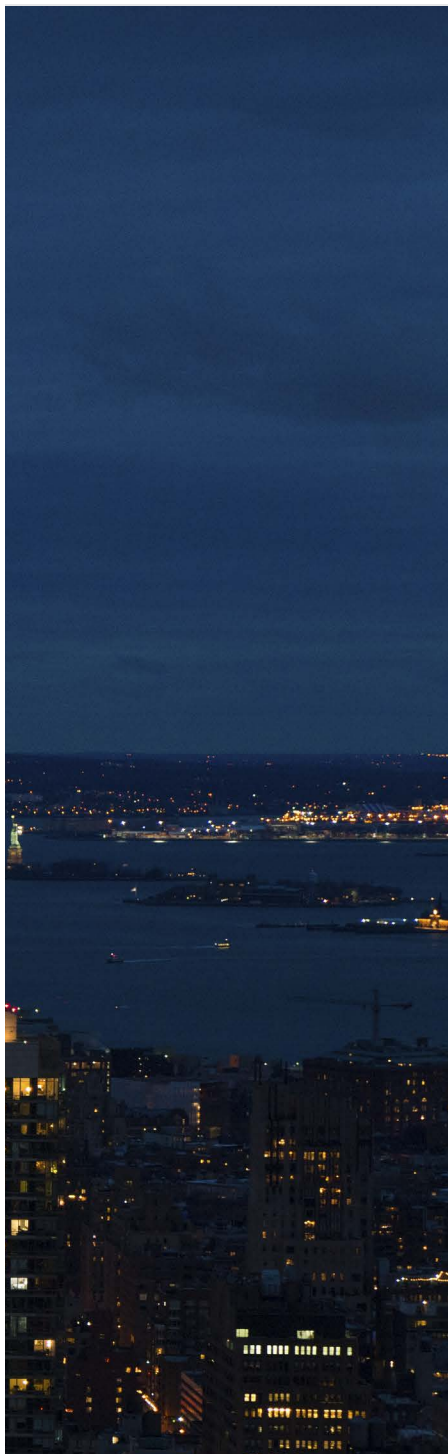
Hoe kunt u zichzelf tegen dergelijke aanvallen beschermen?

Bescherm uw identiteit: Gebruik meervoudige authenticatie op HP Elite pc's.

Bescherm uw data: Gebruik een mobiele verificatie- en encryptie-oplossing zoals HP Access Control; vergrendel niet-gebruikte poorten of beperk de toegang met gebruikersrechten; gebruik krachtige encryptie voor alle data, ook tijdens verzending.

Bescherm het apparaat: Upgrade naar HP Elite pc's en HP Enterprise-printers en -MFP's met malwarebescherming om aanvallen te stoppen, met zelfherstel tot op BIOS-niveau met HP Sure Start.

Verbeter de bewaking en het beheer: Installeer HP JetAdvantage Security Manager (printers) en Management integratiekit¹ (pc's) om automatisch beveiligingsbeleid voor het hele apparaatuurpark te configureren; creëer syslogs om beveiligingsincidenten bij te houden; sluit printers aan op Security Information and Event Management-tools (SIEM) om in realtime waarschuwingen te ontvangen bij een inbreuk.



Bescherm uw bedrijf met uitgebreide beveiliging van HP

De veiligste printers ter wereld²

HP Enterprise-printers en -MFP's kunnen automatisch, zonder tussenkomst van IT, een aanval detecteren, stoppen en ervan herstellen dankzij functionaliteit als runtime inbraakdetectie en HP Sure Start. Andere beschermingsmaatregelen zijn: versleutelde vaste schijven, upgradeable firmware en de mogelijkheid om beveiligingswaarschuwingen te sturen naar SIEM-tools.

hp.com/go/PrintersThatProtect

De veiligste, best beheerbare pc's ter wereld³

HP Elite pc's beschermen u tegen de meest gangbare bedreigingen met beveiliging onder, in en boven het besturingssysteem. HP meervoudige authenticatie versterkt de bescherming van identiteiten en de HP Management integratiekit¹ maakt het gemakkelijk om beveiliging van alle pc's te beheren.

hp.com/go/ComputerSecurity

HP JetAdvantage Connect

Gebruik bestaande IT-netwerkt tools en -policy's om het printen vanaf smartphones en tablets te beheren en gebruikers de mogelijkheid te bieden om net zo gemakkelijk veilig te printen als vanaf een pc, zonder speciale app.

hp.com/go/JetAdvantageConnect

HP Access Control

Herstel de controle, versterk de beveiliging en reduceer de kosten met authenticatie op basis van rollen, autorisatie en veilige pull-printingfunctionaliteit voor uw hele onderneming.

hp.com/go/hpac

HP JetAdvantage Secure Print

Bescherm vertrouwelijke documenten door pull-printing via de cloud. Gebruikers authenticeren zich bij de printlocatie van hun keuze om hun documenten vrij te geven en te printen.

hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Security Manager

Reduceer de kosten en beheer de beveiliging van uw apparatuur met minder mensen dankzij de enige policy-gebaseerde tool voor printbeveiligingscompliance op de markt.⁴ Definieer een beveiligingspolicy voor al uw printers, automatiseer apparaatherstel, installeer en vernieuw unieke certificaten en maak compliancerapporten over uw hele apparatuurpark.

hp.com/go/securitymanager

Kijk voor meer informatie op
hp.com/go/hpsecure

¹ HP Management integratiekit is niet vooraf geïnstalleerd, maar beschikbaar op hp.com/go/clientmanagement.

² Gebaseerd op een evaluatie door HP van in 2016 gepubliceerde ingebouwde beveiligingskenmerken van concurrerende printers uit dezelfde klasse. Alleen HP biedt een combinatie van beveiligingskenmerken die kan bewaken om aanvallen te detecteren, deze automatisch te stoppen en daarna bij het opnieuw opstarten de software-integriteit te valideren. Kijk voor een lijst van printers op: hp.com/go/PrintersThatProtect. Kijk voor meer informatie op hp.com/go/printersecurityclaims.

³ Gebaseerd op HP's unieke, uitgebreide gratis beveiligingsfuncties en beheer met de HP Manageability integratiekit van alle pc-aspecten, inclusief hardware-, BIOS- en softwarebeheer met Microsoft® System Center Configuration Manager onder fabrikanten met > één miljoen verkochte units per jaar in november 2016 op HP Elite pc's met 7e-generatie Intel® Core®-processors, Intel® geïntegreerde graphics en Intel® WLAN.

⁴ Claim over concurrenten is gebaseerd op intern onderzoek van HP naar concurrenten (Device Security Comparison, januari 2015) en een Solutions Report over HP JetAdvantage Security Manager 2.1 van Buyers Laboratory LLC, februari 2015. Kijk voor meer informatie op hp.com/go/securitymanager.

Meld u aan voor updates op
hp.com/go/getupdated



Delen met collega's

