Brochure

Geef The Wolf geen kans

Veiligheidsrisico's in de serie "The Wolf" en de oplossingen van HP

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

Seizoen 1 The Wolf

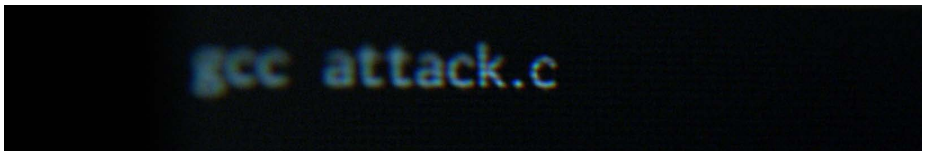
The Wolf schakelt een wereldwijd opererende financiële instelling uit door gebruik te maken van kwetsbare endpoints. Met een mobiel device verschaft hij zich toegang tot een printer en infecteert die met malware om data te onderscheppen en te lezen. Met een phishing-e-mail laat The Wolf vervolgens een gebruiker kwaadaardige code, verborgen in een pdf, naar een printer sturen.

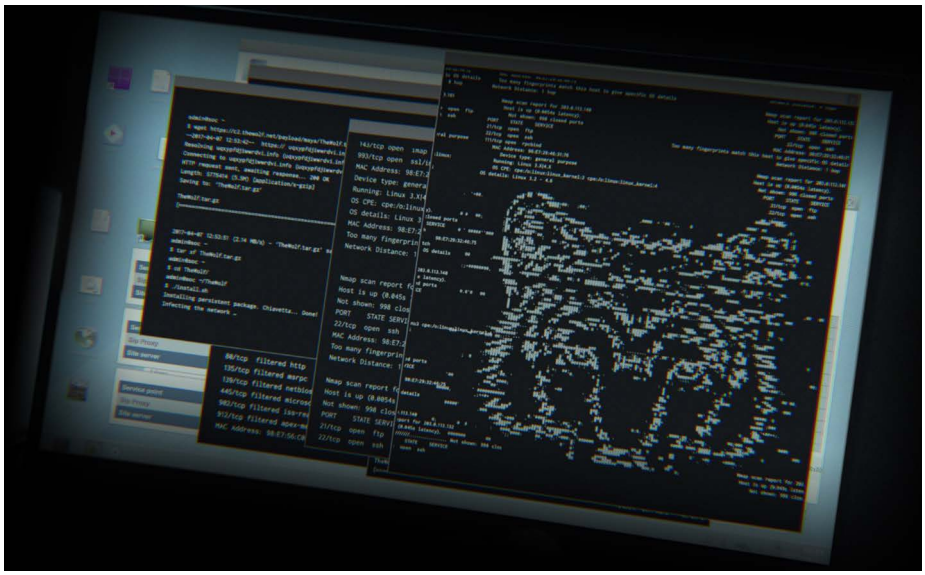
De malware op de printer breekt door de firewall en bereikt het BIOS-niveau van de bedrijfspc's zodat het gegevens kan verzamelen en zichzelf opnieuw kan installeren na het implementeren van netwerkverdedigingsmechanismen.

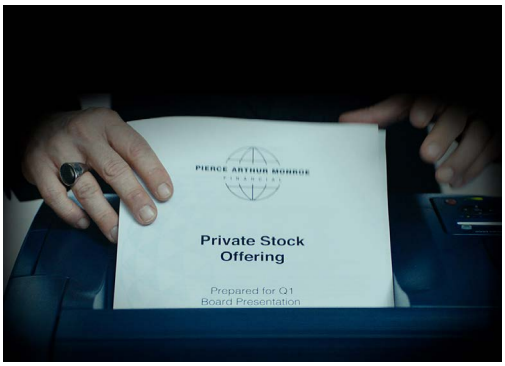
The Wolf neemt een achtergelaten afdruk uit de uitvoerlade van een printer en saboteert de volgende beursdeal van het bedrijf waardoor het vertrouwen van de aandeelhouders keldert.

Kwetsbaarheden

- Wifi of Bluetooth® op de printer staat open en er wordt geen gebruikersverificatie gevraagd
- Databestanden op de printer zijn niet versleuteld
- Gebruikers herkennen verdachte e-mails of printbestanden niet
- Printers en pc's hebben geen bescherming tegen malware op BIOS-niveau
- Gevoelige documenten liggen in uitvoerlades van de printers







Seizoen 2 The Hunt Continues

The Wolf richt zich op patiëntendossiers die zijn opgeslagen bij een van de grootste dossierverwerkingsbedrijven in de medische wereld. Hij hackt een pc en gebruikt dan de USB-poort van een printer om malware te uploaden achter de firewall om zo toegang te krijgen tot aangesloten apparaten.

Omdat de printer zich in een niet-gesegmenteerd netwerk bevindt, heeft The Wolf toegang tot servers die verbonden zijn met databases met vertrouwelijke informatie. Hij steelt miljoenen vertrouwelijke patiëntendossiers, die leesbaar zijn omdat de gegevens niet versleuteld zijn.

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

Kwetsbaarheden

- 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

Seizoen 3 True Alpha

The Wolf verstoort de operaties bij een van de grootste rederijen ter wereld en op een internationale luchthaven.

Via het sturen van een onschuldig ogende pdf krijgt hij een kantoormedewerker van de rederij zo ver dat deze een bewapend Postscript-bestand naar een printer stuurt. Verborgen malware verspreidt zich door het hele netwerk wanneer het bestand naar de printer wordt gestuurd, waar het onopgemerkt blijft zitten. Al snel heeft The Wolf toegang tot de exclusieve conferentiepresentatie van de CEO, kranen in de haven en de autopilootsoftware van schepen op zee.

Vervolgens richt The Wolf zijn aandacht op een grote luchthaven en zien we hoe hij de lichten en mogelijk ook tal van andere kritische luchthavensystemen beheert. HP printers hielpen het IT-personeel de aanval te onderzoeken en te stoppen.

Kwetsbaarheden

- Printers op tijdelijke locaties worden aan het netwerk toegevoegd zonder adequate beveiligingsconfiguratie
- Pc's hebben geen browserbescherming tegen ongewilde downloads
- IoT-apparaten worden niet gemonitord en omvatten geen malwaredetectiemogelijkheden
- De syslogs van de printers zijn niet verbonden met de monitoringtools voor beveiliging

Hoe kunt u zich tegen dergelijke aanvallen beschermen?

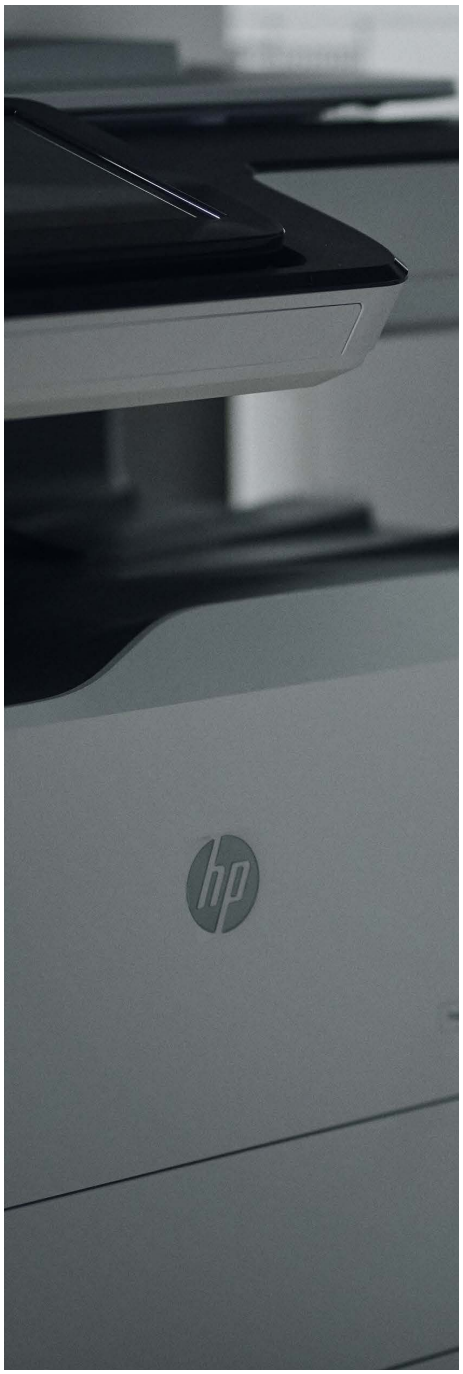
Identiteitsbescherming: Verbeter de beveiliging bij het aanmelden met een verscherpte multi-factor authenticatie op HP Elite pc's.

Apparaatbescherming: Upgrade naar HP Elite pc's en HP Enterprise printers en MFP's met malwarebescherming om automatisch aanvallen te detecteren, te stoppen en ervan te herstellen. Sluit niet-gebruikte USB-poorten of beperk de toegang met gebruikersrechten. Isoleer browsertabs fysiek metHP Sure Click om te voorkomen dat malware van het internet zich verspreid.[1]

Bescherm uw gegevens: Voer een authenticatie- en versleutelingsoplossing voor printers in, zoals HP Access Control.[2] Vereis authenticatie en versleutel gegevens als u de wifi en Bluetoothfuncties van de printer gebruikt. Voer een mobiele authenticatie- en versleutelingsoplossing in zoals PrinterOn Enterprise. Versleutel gegevens, zowel in de opslag als bij de overdracht ervan.

Documentbescherming: Installeer een pull-printoplossing zoals HP Access Control.[2]

Verbeter de bewaking en het beheer: Configureer automatisch het beveiligingsbeleid van het printerpark met HP JetAdvantage Security Manager[3] of de HP Printer Security Plug-in voor Microsoft® SCCM voor printers en de HP Manageability Integration Kit (MIK)[4] voor pc's. Activeer syslogs om beveiligingsproblemen te traceren en sluit apparaten aan op Security Information and Event Management (SIEM) tools voor meldingen in real-time. Ga naar een MPS-dienstverlener die getraind is in HP-beveiliging voor het configureren en onderhouden van de veiligheid van uw printers.



Bescherm uw bedrijf met uitgebreide beveiliging van HP

De veiligste printers ter wereld[5]

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

hp.com/go/PrintersThatProtect

De veiligste, best te beheren pc's ter wereld[6]

HP Elite pc's beschermen u tegen de meest gangbare bedreigingen met beveiliging onder, in en boven het besturingssysteem. De multi-factor authenticatie van HP versterkt de bescherming van identiteit en de HP Manageability Integration Kit[4] maakt het gemakkelijk om beveiliging van alle pc's te beheren. Andere beschermingen omvatten versleuteling van de harde schijf, HP Sure Recover[7], HP Sure Click[1] en HP Sure View.

hp.com/go/ComputerSecurity

PrinterOn Enterprise

Betrouwbaar en veilig printen op het netwerk van uw bedrijf. Sluit vrijwel alle desktops of mobiele devices aan op printers van meerdere fabrikanten, zowel binnen als buiten het vertrouwde netwerk.

hp.com/go/businessmobileprinting

HP Access Control[2]

Herstel de controle, versterk de beveiliging en reduceer kosten met printauthenticatie op basis van functies, autorisatie en veilige pull-printingfunctionaliteit voor heel uw onderneming.

hp.com/go/hpac

HP JetAdvantage Security Manager[3]

Bespaar kosten en middelen voor de beveiliging van uw printerpark met een allesomvattende op een beleid gebaseerde compliancetool voor printbeveiliging. Voer een beveiligingsbeleid voor al uw printers in, automatiseer het herstel van apparaatinstellingen, installeer en vernieuw unieke certificaten, en creëer compliancerapporten voor alle hardware.

hp.com/go/securitymanager

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

[1] HP Sure Click is beschikbaar op de meeste pc's van HP en ondersteunt Microsoft® Internet Explorer en Chromium™. Ondersteunde bijlagen omvatten Microsoft Office (Word, Excel, PowerPoint) en pdf-bestanden in leesmodus, maar enkel als Microsoft Office of Adobe Acrobat geïnstalleerd zijn.

[2] HP Access Control moet apart worden aangeschaft. Kijk voor meer informatie op hp.com/go/hpac.

[3] HP JetAdvantage Security Manager moet apart worden aangeschaft. Kijk voor meer informatie op hp.com/go/securitymanager.

[4] De HP Manageability Integration Kit is niet vooraf geïnstalleerd, maar beschikbaar op hp.com/go/clientmanagement.

[5] Gebaseerd op een evaluatie door HP van in 2018 gepubliceerde beveiligingskenmerken van concurrerende printers uit dezelfde klasse.Alleen HP biedt een combinatie van beveiligingskenmerken die aanvallen kunnen detecteren, deze automatisch kunnen stoppen en daarna bij het opnieuw opstarten de software-integriteit valideren. Kijk voor een lijst van printers op hp.com/go/PrintersThatProtect. Kijk voor meer informatie op: hp.com/go/printersecurityclaims.

[6] Gebaseerd op de unieke, uitgebreide, gratis beveiligingsfuncties van HP en het beheer met de HP Manageability Integration Kit van alle aspecten van de pc waaronder hardware-, BIOS- en softwarebeheer met Microsoft® System Center Configuration Manager onder fabrikanten met meer dan één miljoen verkochte units per jaar in november 2016 op HP Elite pc's met 7e-generatie en hogere Intel® Core®-processors, Intel® integrated graphics en Intel® WLAN.

[7] HP Sure Recover is beschikbaar op HP Elite pc's met 8e-generatie Intel®- of AMD-processors en vereist een open, bekabelde netwerkverbinding. Niet beschikbaar op platforms met meerdere interne opslagschijven, Intel® Optane™. Om te voorkomen dat u gegevens verliest, moet u een back-up maken van belangrijke bestanden, gegevens, foto's, video's enz.

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

Delen met collega's

4AA7-0231NLE, augustus 2018, Rev. 1