Broszura

Strzeż się Wilka

Zagrożenia dla bezpieczeństwa w filmach „Wilk” i rozwiązania HP

Same zapory sieciowe nie są w stanie stawić oporu wyszukanym atakom hakerów, takich jak tytułowy Wilk. Użytkownicy powinni stosować wiele warstw ochronnych w każdym punkcie końcowym infrastruktury. Rozwiązania HP w zakresie bezpieczeństwa pomagają chronić urządzenia, dane, tożsamość i dokumenty użytkowników.

Sezon 1 Wilk

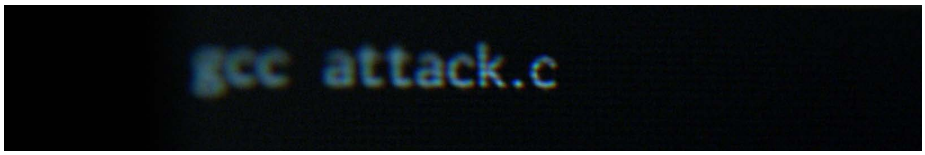
Wilk niszczy globalną instytucję finansową, wykorzystując jej najbardziej narażone na atak punkty końcowe. Za pomocą zdalnego urządzenia uzyskuje dostęp do drukarki i wprowadza do niej złośliwe oprogramowanie umożliwiające przechwytywanie i odczyt danych. Następnie wysyła wiadomość typu „phishing", nakłaniając użytkownika do przemycenia złośliwego kodu ukrytego w pliku PDF do druku.

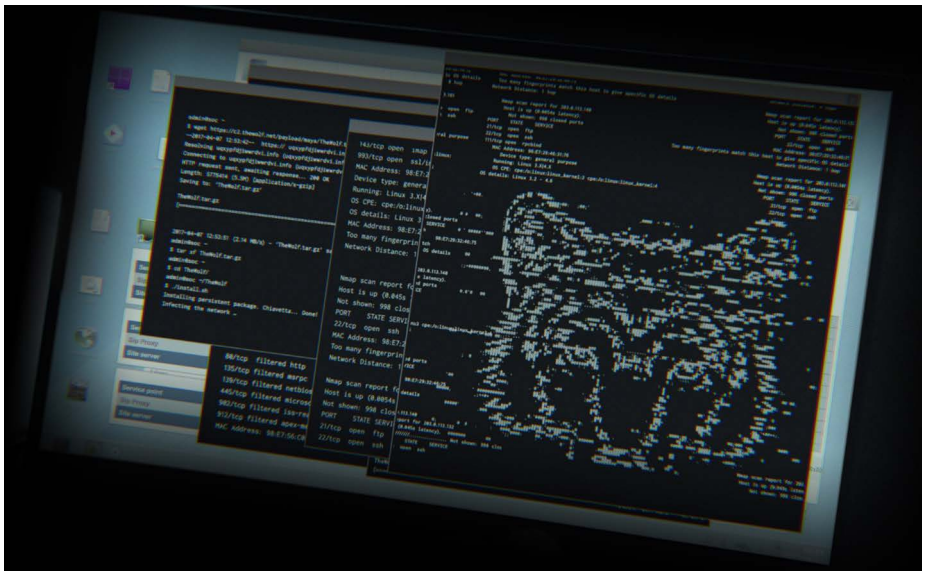
Złośliwy program, który trafił do drukarki, pokonuje zaporę sieciową i dociera do systemu BIOS firmowych komputerów, dzięki czemu może gromadzić dane, a nawet wznowić swoje działanie po wdrożeniu sieciowych zabezpieczeń.

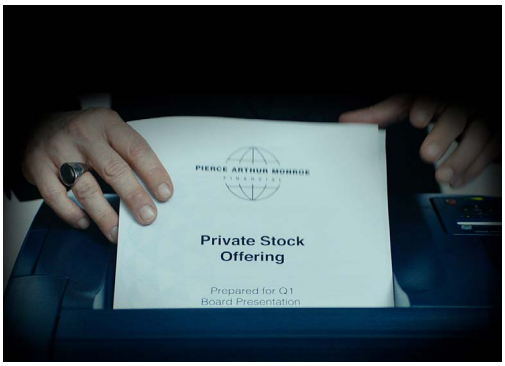
Wilk zabiera porzucony w odbiorniku drukarki wydruk i dokonuje sabotażu transakcji związanej z udziałami firmy, co kompletnie rujnuje zaufanie udziałowców.

Punkty narażone na atak

- Drukarka Wi-Fi lub Bluetooth® jest otwarta i nie wymaga uwierzytelnienia użytkownika.
- Pliki z danymi w drukarce nie są szyfrowane.
- Użytkownicy nie rozpoznają podejrzanych wiadomości e-mail i plików do wydruku.
- Drukarki i komputery nie są chronione przed złośliwym oprogramowaniem na poziomie systemu BIOS.
- Wrażliwe dokumenty są pozostawiane w odbiornikach drukarek.







Sezon 2 Polowanie trwa

Celem Wilka jest zdobycie dokumentacji medycznej pacjentów, przechowywanej przez jedną z największych na świecie firm zarządzających danymi medycznymi. Włamuje się on do komputera, a następnie używa portu USB drukarki do ominięcia zapory sieciowej i zainstalowania złośliwego oprogramowania, które wyszuka podłączone urządzenia i pozwoli wykraść z nich dane.

Ponieważ drukarka jest podłączona do sieci niepodzielonej na segmenty, Wilk może uzyskać dostęp do serwerów podłączonych do baz danych informacji wrażliwych. Wykrada miliony poufnych rejestrów pacjentów, które można z łatwością odczytać, gdyż nie zostały zaszyfrowane.

Za zaistniałą sytuację jest odpowiedzialny zarówno szpital, jak i producent, więc zostają na nich nałożone wysokie kary finansowe, a incydent ma niekorzystny wpływ na ich reputację.

Punkty narażone na atak

- Port USB drukarki nie wymaga uwierzytelnienia przed użyciem.
- Pliki z danymi nie są szyfrowane.
- Drukarki nie są chronione przed złośliwym oprogramowaniem.
- Drukarki nie są monitorowane pod kątem zdarzeń naruszających ochronę bezpieczeństwa.

Sezon 3 Prawdziwy drapieżnik

Wilk zakłóca działanie jednej z największych na świecie firm transportowych oraz międzynarodowego portu lotniczego.

Wysyłając e-mail z niewinnie wyglądającym dokumentem PDF, doprowadza do tego, że jeden z pracowników firmy transportowej wysyła „uzbrojony" plik PostScript do drukarki. Gdy plik trafi już do drukarki, gdzie pozostaje niewykryty, ukryte w nim złośliwe oprogramowanie zaczyna rozprzestrzeniać się po całej sieci. Wkrótce Wilk uzyskuje dostęp do poufnej prezentacji konferencyjnej jednego z dyrektorów firmy, dźwigu załadunkowego portu oraz oprogramowania autopilota jednej z jednostek morskich.

Następnie Wilk skupia się na dużym porcie lotniczym, popisując się zdolnościami sterowania oświetleniem, a co za tym idzie – potencjalnie wieloma krytycznymi systemami sieci lotniska. Drukarki HP pomogły pracownikom działu IT wykryć i zatrzymać atak.

Punkty narażone na atak

- Drukarki wykorzystywane w lokalizacjach tymczasowych są podłączane do sieci bez adekwatnej konfiguracji zabezpieczeń.
- Komputery nie mają zabezpieczeń chroniących przed przypadkowym pobraniem plików podczas korzystania z przeglądarki internetowej.
- Urządzenia IoT nie są monitorowane i nie mają funkcji wykrywania złośliwego oprogramowania.
- Dzienniki systemowe drukarek nie są połączone z narzędziami do monitorowania zagrożeń.

W jaki sposób można się chronić przed podobnymi atakami?

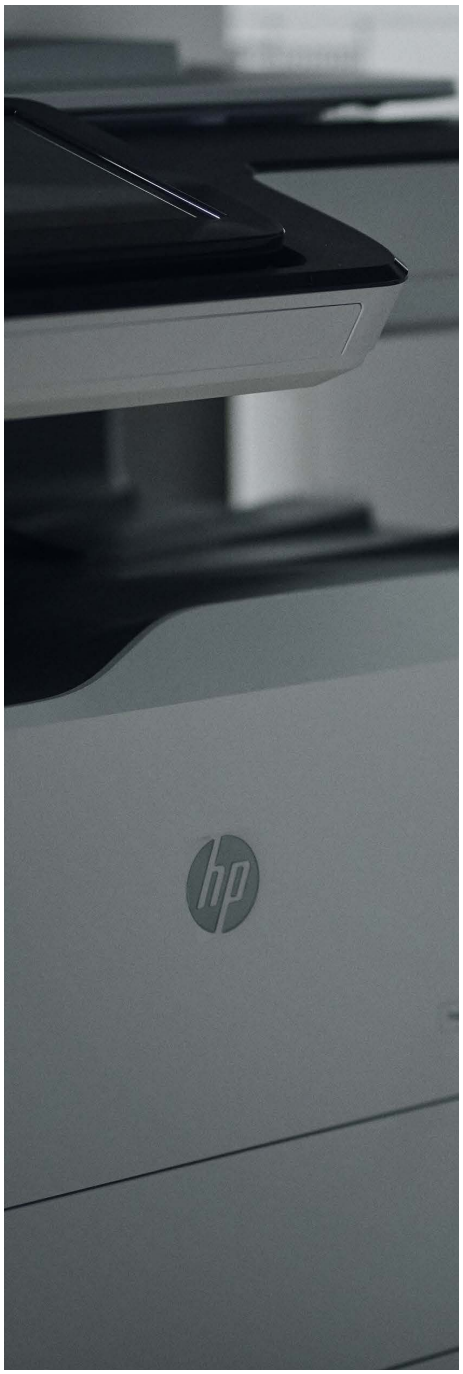
Ochrona tożsamości: poprawienie bezpieczeństwa logowania poprzez wprowadzenie uwierzytelniania wieloskładnikowego na komputerach HP Elite.

Ochrona urządzeń: przejście na komputery HP Elite oraz drukarki i urządzenia wielofunkcyjne HP Enterprise z ochroną przed złośliwym oprogramowaniem w celu automatycznego wykrywania i zatrzymywania ataków oraz przywracania stabilności systemów. Zamknięcie nieużywanych portów USB lub kontrola dostępu poprzez nadzór użytkowników. Fizyczne odizolowanie kart przeglądarki za pomocą HP Sure Click, co pozwoli zapobiec rozprzestrzenianiu się złośliwego oprogramowania działającego w oparciu o sieci.[1]

Ochrona danych: wdrożenie rozwiązania uwierzytelniającego i szyfrującego dla drukarek, jak np. HP Access Control.[2] Wprowadzenie procedur uwierzytelniania użytkowników oraz szyfrowania danych podczas korzystania z funkcji Wi-Fi i Bluetooth drukarki. Wdrożenie rozwiązania uwierzytelniającego i szyfrującego dla urządzeń mobilnych, w tym między innymi PrinterOn Enterprise. Szyfrowanie danych magazynowanych i przenoszonych.

Ochrona dokumentów: wprowadzenie rozwiązania umożliwiającego bezpieczne drukowanie, jak HP Access Control.[2]

Skuteczniejszy monitoring i procedury zarządzania: automatyczna konfiguracja zabezpieczeń floty dzięki rozwiązaniom HP JetAdvantage Security Manager[3] lub HP Printer Security Plug-in for Microsoft® SCCM dla drukarek oraz HP Manageability Integration Kit (MIK)[4] dla komputerów. Umożliwienie dziennikom systemowym śledzenia zdarzeń związanych z bezpieczeństwem oraz połączenie urządzeń z systemami SIEM (Security Information and Event Management), które zapewnią alerty w czasie rzeczywistym. Zwrócenie się do przeszkolonego przez firmę HP dostawcy usług MPS w celu skonfigurowania zabezpieczeń drukarek i ich dalszego zarządzania.



Ochrona firmy dzięki kompleksowym zabezpieczeniom HP

Najbezpieczniejsze na świecie drukowanie[5]

Drukarki i urządzenia wielofunkcyjne HP Enterprise są w stanie automatycznie wykrywać i zatrzymywać ataki oraz powracać po nich do stabilnego działania bez interwencji działu IT, dzięki takim funkcjom jak wykrywanie ingerencji w trakcie uruchamiania czy rozwiązaniom HP Sure Start i HP Connection Inspector. Inne środki ochrony obejmują szyfrowane dyski twarde, oprogramowanie firmowe z opcją rozbudowy i możliwość wysyłania alarmów bezpieczeństwa do narzędzi SIEM.

hp.com/go/PrintersThatProtect

Najbezpieczniejsze na świecie i dające najwięcej możliwości zarządzania komputery[6]

Komputery HP Elite pomagają w ochronie przed najpowszechniejszymi zagrożeniami poprzez zabezpieczenie przede wszystkim systemu operacyjnego. Funkcja uwierzytelnienia wieloskładnikowego zwiększa ochronę tożsamości, a narzędzie HP Management Integration Kit[4] ułatwia zarządzanie bezpieczeństwem we flocie komputerów. Inne zabezpieczenia obejmują szyfrowanie dysków twardych oraz rozwiązania HP Sure Recover[7], HP Sure Click,[1] i HP Sure View.

hp.com/go/ComputerSecurity

PrinterOn Enterprise

Niezawodne i bezpieczne drukowanie mobilne w sieciach firmowych. Możliwość podłączenia prawie każdego komputera stacjonarnego i urządzenia przenośnego do drukarek różnych dostawców, niezależnie od tego, czy jest to sieć zaufana czy nie.

hp.com/go/businessmobileprinting

HP Access Control[2]

Przywracanie kontroli, zwiększanie bezpieczeństwa i ograniczanie kosztów dzięki uwierzytelnieniu wydruku na podstawie roli, autoryzacji i bezpiecznemu drukowaniu w systemie kolejki wydruku w całej organizacji.

hp.com/go/hpac

HP JetAdvantage Security Manager[3]

Zmniejszenie kosztów i zużycia zasobów w celu zagwarantowania bezpieczeństwa floty dzięki kompleksowemu narzędziu do zarządzania zgodnością druku opartemu na regułach. Ustanowienie polityki bezpieczeństwa dla całej floty, automatyzacja działań naprawczych związanych z ustawieniami urządzeń, instalowanie i odnawianie unikatowych certyfikatów, a także tworzenie raportów zgodności dla całej floty.

hp.com/go/securitymanager

Więcej informacji:
hp.com/go/hpsecure

[1] Aplikacja HP Sure Click jest dostępna na większości komputerów HP i obsługuje przeglądarki Microsoft® Internet Explorer oraz Chromium™. Obsługiwane załączniki obejmują pliki pakietu Microsoft Office (Word, Excel, PowerPoint) oraz pliki PDF tylko w trybie do odczytu, jeśli na komputerze zainstalowane jest oprogramowanie Microsoft Office lub Adobe Acrobat.

[2] Rozwiązanie HP Access Control jest sprzedawane oddzielnie. Więcej informacji można znaleźć na stronie hp.com/go/hpac.

[3] Oprogramowanie HP JetAdvantage Security Manager należy zakupić osobno. Szczegółowe informacje są dostępne na stronie hp.com/go/securitymanager.

[4] Narzędzie HP Manageability Integration Kit nie jest fabrycznie zainstalowane; jest ono dostępne na stronie hp.com/go/clientmanagement.

[5] Na podstawie recenzji HP dotyczącej udostępnionych w 2018 r. funkcji zabezpieczeń konkurencyjnych drukarek tej samej klasy. Tylko firma HP oferuje funkcje zabezpieczeń, które monitorują, wykrywają i automatycznie powstrzymują ataki, a następnie kontrolują integralność oprogramowania po ponownym uruchomieniu. Lista drukarek: hp.com/go/PrintersThatProtect. Więcej informacji: hp.com/go/printersecurityclaims.

[6] Na podstawie unikatowych i kompleksowych funkcji zabezpieczeń HP bez ponoszenia dodatkowych kosztów oraz funkcji zarządzania wszystkimi elementami komputera, w tym sprzętem, w zestawie HP Manageability Integration Kit oraz funkcji zarządzania systemem BIOS i oprogramowaniem przy użyciu menedżera konfiguracji Microsoft® System Center Configuration Manager w komputerach HP Elite z procesorami Intel® Core® 7. lub nowszej generacji, zintegrowanymi kartami graficznymi Intel® i kartami sieciowymi WLAN Intel® wśród dostawców z roczną sprzedażą powyżej 1 mln sztuk według stanu na listopad 2016 r.

[7] Rozwiązanie HP Sure Recover jest dostępne na komputerach HP Elite z procesorami Intel® lub AMD 8. generacji i wymaga otwartego, przewodowego połączenia sieciowego. Rozwiązanie nie jest dostępne na platformach wyposażonych w kilka wewnętrznych pamięci masowych, Intel® Optane™. Aby uniknąć utraty danych, przed użyciem tego rozwiązania należy wykonać kopię zapasową ważnych plików, danych, zdjęć, filmów itd.

Zarejestruj się, aby otrzymywać aktualne informacje:
hp.com/go/getupdated

Udostępnij współpracownikom

4AA7-0231PLE, sierpień 2018, wer. 1