



Strzeż się Wilka

Zagrożenia bezpieczeństwa w filmach „The Wolf”
i rozwiązania HP

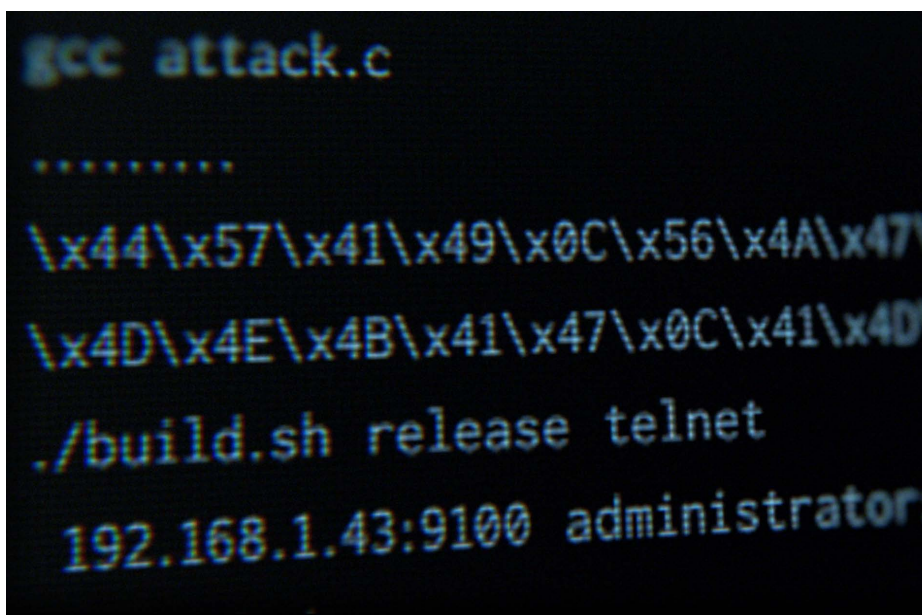
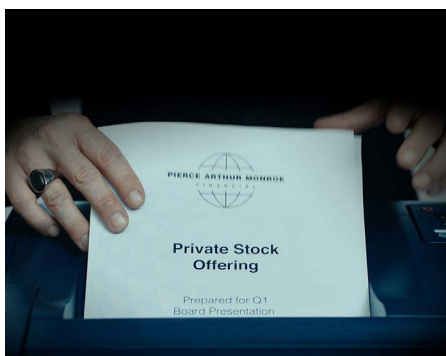
Same zapory sieciowe nie są w stanie powstrzymać wyszukanych ataków hakerów, takich jak tytułowy Wilk. Użytkownicy powinni stosować szereg warstw ochronnych w każdym punkcie końcowym infrastruktury. Rozwiązania HP w zakresie bezpieczeństwa pomagają chronić urządzenia, dane, tożsamość i dokumenty użytkowników.

Sezon 1 The Wolf

W pierwszym filmie Wilk niszczy globalną instytucję finansową, wykorzystując jej najbardziej narażone na atak punkty końcowe. Wilk za pomocą urządzenia zdalnego uzyskuje dostęp do drukarki i wprowadza do niej złośliwe oprogramowanie umożliwiające przechwytywanie i odczyt danych. Następnie wysyła wiadomość typu „phishing”, nakłaniając użytkownika do przekazania złośliwego kodu ukrytego w pliku do wydruku.

Złośliwe oprogramowanie drukarki łamie zaporę sieciową i rozprzestrzenia się w komputerach spółki. Kod znajduje się na poziomie BIOS-u, więc może stale przekazywać dane, a nawet przywrócić działanie po aktywacji systemów ochrony sieci.

Na koniec Wilk odkrywa poufny dokument na odbiorniku urządzenia wielofunkcyjnego. Wyciek danych powoduje znaczne straty finansowe i wizerunkowe firmy.



Punkty narażone na atak

- Drukarka Wi-Fi lub Bluetooth® jest otwarta i nie wymaga uwierzytelnienia użytkownika.
- Pliki z danymi drukarki nie są szyfrowane.
- Użytkownicy nie rozpoznają podejrzanych wiadomości e-mail i plików do wydruku.
- Drukarki i komputery nie są chronione przed złośliwym oprogramowaniem.
- Dokumenty pozostawione na odbiorniku drukarki mogą zawierać informacje wrażliwe.

W jaki sposób można się chronić przed podobnymi atakami?

Ochrona danych: Wyłączenie połączenia Wi-Fi/Bluetooth lub żądanie uwierzytelnienia; zastosowanie uwierzytelnienia mobilnego i szyfrowania, np. HP JetAdvantage Connect lub HP Access Control.

Ochrona urządzenia: Przejście na komputery HP Elite i drukarki HP Enterprise oraz urządzenia wielofunkcyjne z ochroną przed złośliwym oprogramowaniem w celu automatycznego wykrywania i zatrzymywania ataków oraz odzyskiwania stabilności bez interwencji działu IT. HP Sure Start pomaga urządzeniom w samodzielnej naprawie za pomocą bezpiecznej kopii oryginalnego kodu BIOS.

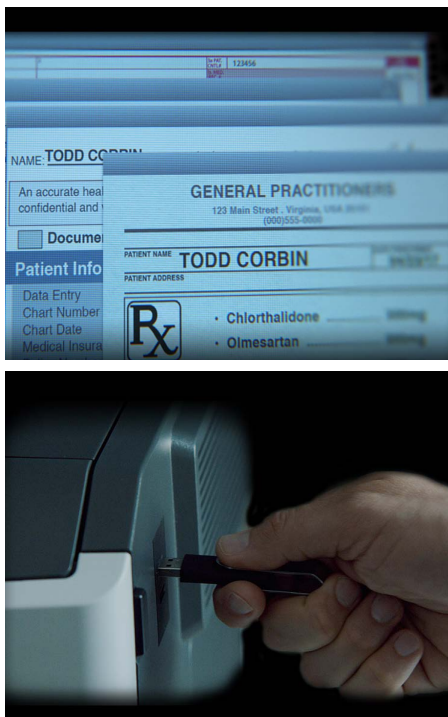
Ochrona dokumentów: Wprowadzenie rozwiązania umożliwiającego bezpieczne drukowanie, jak HP Access Control lub HP JetAdvantage Secure Print.

Sezon 2 The Wolf: Polowanie trwa

W drugim filmie 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 do szpitalnej drukarki, korzystając z jej portu USB, aby wczytać złośliwe oprogramowanie.

Jako że niezabezpieczona drukarka jest podłączona do sieci, złośliwe oprogramowanie pokonuje zaporę sieciową i może wyszukiwać inne połączone urządzenia, które można zainfekować. A ponieważ drukarka jest podłączona do sieci niepodzielonej na segmenty, Wilk może uzyskać dostęp do serwerów podłączonych do baz danych informacji wrażliwych. Kradnie miliony poufnych danych pacjentów.

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

- Komputer nie jest zablokowany, kiedy użytkownik od niego odchodzi.
- Port USB drukarki nie wymaga uwierzytelnienia przed użyciem.
- Pliki z danymi nie są szyfrowane.
- Drukarki i komputery nie są chronione przed złośliwym oprogramowaniem.
- Drukarki nie są monitorowane pod kątem zdarzeń naruszających ochronę bezpieczeństwa.

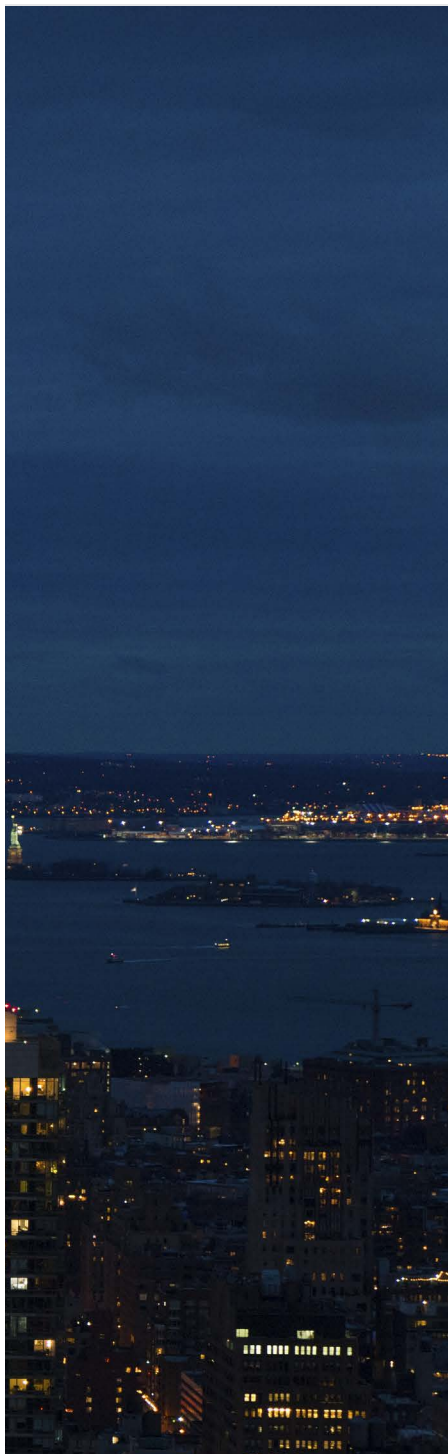
W jaki sposób można się chronić przed podobnymi atakami?

Ochrona tożsamości: Stosowanie wieloczynnikowego uwierzytelnienia na komputerach HP Elite.

Ochrona danych: Zastosowanie uwierzytelnienia drukarki i szyfrowania, np. HP Access Control; Zamknięcie nieużywanych portów lub kontrola dostępu za pomocą kontroli użytkowników; Stosowanie silnej kontroli szyfrowania dla wszystkich danych przechowywanych i przesyłanych.

Ochrona urządzenia: Przejście na komputery HP Elite i drukarki HP Enterprise oraz urządzenia wielofunkcyjne z wbudowaną ochroną przed złośliwym oprogramowaniem w celu niedopuszczenia do ataków i samoregeneracji do poziomu systemu BIOS za pomocą HP Sure Start.

Wprowadzenie skuteczniejszego monitoringu i zarządzania: Wdrożenie HP JetAdvantage Security Manager (drukarki) i Management Integration Kit¹ (komputery) w celu automatycznej konfiguracji polityki bezpieczeństwa urządzeń w całej flocie; umożliwienie syslogom śledzenia zdarzeń bezpieczeństwa; podłączenie drukarek do narzędzi SIEM (Security Information and Event Management) w celu uzyskiwania powiadomień o ingerencjach w czasie rzeczywistym.



Ochrona firmy dzięki kompleksowym zabezpieczeniom HP

Najbezpieczniejsze drukowanie na świecie²

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

hp.com/go/PrintersThatProtect

Najbezpieczniejsze na świecie drukowanie i zarządzanie komputerami³

Komputery HP Elite pomagają w ochronie przed najpowszechniejszymi zagrożeniami poprzez zabezpieczenie przede wszystkim systemu operacyjnego. Funkcja uwierzytelnienia wieloczynnikowego HP Multi-Factor Authenticate zwiększa ochronę tożsamości, a HP Management Integration Kit¹ ułatwia zarządzanie bezpieczeństwem we flocie komputerów.

hp.com/go/ComputerSecurity

HP JetAdvantage Connect

Wykorzystanie istniejących narzędzi sieciowych i polityki IT do zarządzania drukowaniem ze smartfonów i tabletów, przy jednoczesnym zapewnieniu użytkownikom możliwości bezpiecznego wydruku z taką samą łatwością jak z komputera, bez konieczności instalacji aplikacji.

hp.com/go/JetAdvantageConnect

HP Access Control

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 Secure Print

Ochrona dokumentów wrażliwych dzięki drukowaniu w systemie kolejki wydruku w chmurze. Uwierzytelnienie użytkowników następuje w wybranej lokalizacji drukarki w celu ustawienia zadań do drukowania w kolejce.

hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Security Manager

Zmniejszenie kosztów i zasobów mających na celu utrzymywanie bezpieczeństwa floty za pomocą jedynego w branży narzędzia bezpieczeństwa druku na bazie polityki⁴. Zapewnienie polityki bezpieczeństwa całej floty, automatyczna korekta ustawień urządzenia, instalacja i odnawianie unikalnych certyfikatów i tworzenie raportów zgodności dla całej floty.

hp.com/go/securitymanager

Więcej informacji:

hp.com/go/hpsecure

¹ HP Management Integration Kit nie jest wstępnie zainstalowany, jest on dostępny na stronie hp.com/go/clientmanagement.

² Na podstawie recenzji HP dotyczącej udostępnionych w 2016 r. funkcji zabezpieczeń konkurencyjnych drukarek tej samej klasy. Tylko HP oferuje kompleksowy pakiet funkcji bezpieczeństwa, które monitorują, wykrywają i automatycznie powstrzymują ataki, a następnie dokonują samoczynnego zatwierdzenia integralności oprogramowania przy ponownym uruchomieniu. Lista drukarek: hp.com/go/PrintersThatProtect. Informacje dodatkowe: hp.com/go/printersecurityclaims.

³ Na podstawie unikalnych i kompleksowych możliwości HP w zakresie zabezpieczeń HP bez dodatkowych kosztów oraz przy zarządzaniu każdym aspektem funkcjonowania komputera za pomocą HP Manageability Integration Kit, w tym zarządzaniu sprzętem, systemem BIOS i oprogramowaniem za pomocą Microsoft® System Center Configuration Manager, wśród sprzedawców o rocznej sprzedaży powyżej 1 mln szt. (stan z listopada 2016 r.) komputerów HP Elite z procesorami Intel® Core® 7. generacji, zintegrowaną kartą graficzną Intel® oraz łącznością Intel® WLAN.

⁴ Stwierdzenie dotyczące konkurencji bazuje na przeprowadzonych wewnętrznie przez HP badaniach oferty konkurencji (Porównanie bezpieczeństwa urządzeń, styczeń 2015 r.) oraz raporcie na temat rozwiązania HP JetAdvantage Security Manager 2.1 opracowanym przez Buyers Laboratory LLC w lutym 2015 r. Więcej informacji można znaleźć na stronie hp.com/go/securitymanager.

Zarejestruj się, aby otrzymywać aktualizacje
hp.com/go/getupdated



Udostępniij współpracownikom

