



Tenete il Lupo a distanza

I rischi legati alla sicurezza nei video di "The Wolf" e le soluzioni HP

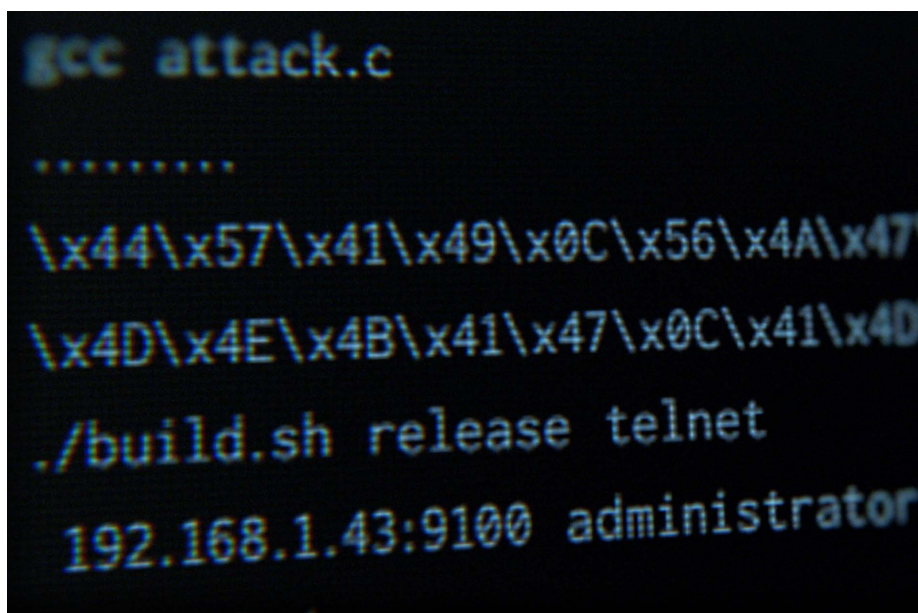
I firewall da soli non possono tenere testa agli attacchi sofisticati di hacker come The Wolf. È necessario applicare livelli di protezione multipli presso ogni endpoint della vostra infrastruttura. Proteggete i vostri dispositivi, dati, identità e documenti con le soluzioni di sicurezza di HP.

Stagione 1 The Wolf

Nel primo video, il Lupo mette fuori gioco un istituto finanziario internazionale sfruttando le vulnerabilità degli endpoint. Il Lupo utilizza un dispositivo mobile per accedere a una stampante e installare il malware per intercettare e leggere i dati. Utilizza quindi un'e-mail di "phishing" per indurre con l'inganno un utente a inviare a una stampante del codice dannoso nascosto in un file di stampa.

Il malware installato nella stampante viola il firewall e penetra nei PC dell'azienda. Il codice risiede a livello del BIOS, pertanto può continuamente fornire dati e persino ripristinarsi dopo l'attivazione di difese di rete.

Infine, il Lupo rinviene un documento riservato nel vassoio di uscita di una stampante multifunzione. La divulgazione di dati sensibili causa all'azienda danni considerevoli in termini finanziari e di immagine.



Vulnerabilità

- La funzionalità Wi-Fi o Bluetooth® della stampante è aperta e non richiede l'autenticazione degli utenti
- I file di dati della stampante non sono crittografati
- Gli utenti non riconoscono le e-mail e i file di stampa sospetti
- Le stampanti e i PC non sono dotati di protezione da malware
- Con i documenti dimenticati nei vassoi di uscita si rischia la divulgazione di informazioni riservate

Come proteggersi da simili attacchi?

Protezione dei dati: disattivare la funzionalità Wi-Fi/Bluetooth o richiedere l'autenticazione; applicare una soluzione di autenticazione e crittografia ai dispositivi mobili, ad esempio, HP JetAdvantage Connect o HP Access Control.

Protezione dei dispositivi: scegliere i PC HP Elite e le stampanti e multifunzione HP Enterprise dotati di protezione da malware per rilevare, bloccare e ripristinare il sistema automaticamente in seguito a un attacco, senza intervento da parte del personale IT. HP Sure Start contribuisce alla correzione automatica dei dispositivi, garantendo il riavvio con una copia sicura del codice BIOS originale.

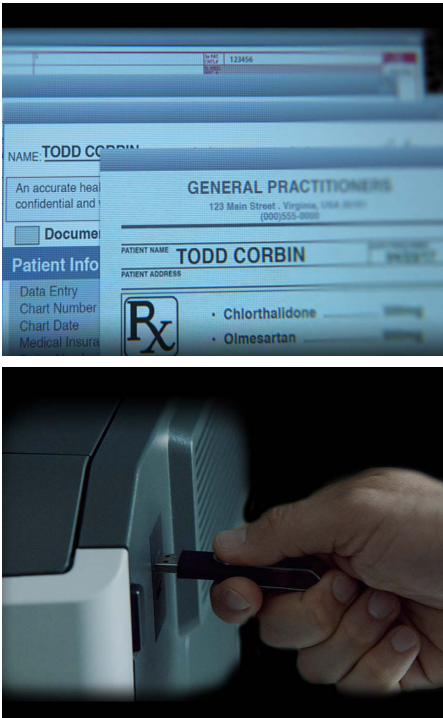
Protezione dei documenti: implementare una soluzione di pull print, come HP Access Control o HP JetAdvantage Secure Print.

Stagione 2 The Wolf: La caccia continua

Nel secondo video, il Lupo prende di mira le informazioni dei pazienti archiviate in una delle più grandi società di gestione di cartelle cliniche al mondo. Penetra in un PC e in seguito nella stampante di un ospedale, utilizzando una porta USB per caricare il malware.

Dal momento che la stampante non protetta è collegata alla rete, il malware ha già oltrepassato il firewall e può cercare altri dispositivi connessi da danneggiare. E poiché la stampante risiede su una rete non segmentata, il Lupo può accedere ai server collegati ai database contenenti informazioni sensibili. sottrae quindi milioni di cartelle cliniche riservate dei pazienti.

L'ospedale e la società informatica sono entrambi responsabili e subiscono sanzioni pecuniarie significative, oltre al danno alla propria reputazione.



Vulnerabilità

- Il PC non viene bloccato quando l'utente si allontana
- La porta USB della stampante non richiede l'autenticazione per essere utilizzata
- I file di dati non sono crittografati
- Le stampanti e i PC non sono dotati di protezione da malware
- Le stampanti non sono monitorate per rilevare eventuali problemi alla sicurezza

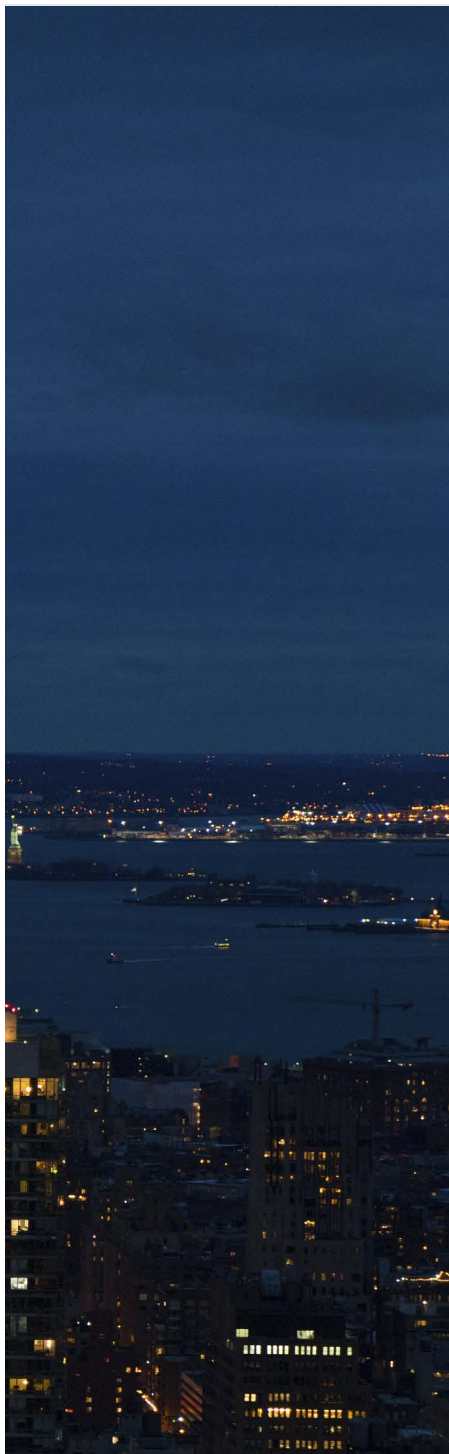
Come proteggersi da simili attacchi?

Protezione dell'identità: utilizzare l'autenticazione a più fattori offerta dai PC HP Elite.

Protezione dei dati: applicare una soluzione di autenticazione e crittografia alle stampanti, ad esempio HP Access Control. disabilitare le porte inutilizzate o gestire l'accesso mediante i controlli utente; utilizzare controlli di crittografia rigorosi per tutti i dati, residenti e in transito.

Protezione dei dispositivi: scegliere i PC HP Elite e le stampanti e le multifunzione HP Enterprise dotati di protezione da malware integrata, che blocca gli attacchi ed effettua la riparazione automatica fino al livello del BIOS con HP Sure Start.

Miglioramento del monitoraggio e della gestione: implementare HP JetAdvantage Security Manager (stampanti) e Management Integration Kit¹ (PC) per configurare automaticamente le policy di sicurezza nel parco dispositivi; abilitare syslogs per tenere traccia degli eventi relativi alla sicurezza; collegare le stampanti agli strumenti SIEM (Security Information and Event Management) per il rilevamento delle intrusioni in tempo reale.



Proteggete la vostra azienda con la sicurezza completa di HP

Le stampanti più sicure al mondo²

Le stampanti e le multifunzione HP Enterprise sono in grado di rilevare, bloccare ed effettuare il ripristino automatico in seguito a un attacco senza alcun intervento da parte dell'IT, con funzionalità quali il rilevamento delle intrusioni in tempo reale e HP Sure Start. Le altre protezioni includono le unità disco rigido crittografate, il firmware aggiornabile e la possibilità di inviare avvisi di sicurezza agli strumenti SIEM.

hp.com/go/PrintersThatProtect

I PC più sicuri e gestibili al mondo³

I PC HP Elite offrono protezione dalle minacce più diffuse proteggendo il sistema operativo ad ogni livello. L'autenticazione a più fattori di HP rafforza la protezione delle identità e il kit HP Management Integration¹ semplifica la gestione della sicurezza nell'intero parco PC.

hp.com/go/ComputerSecurity

HP JetAdvantage Connect

Consente di utilizzare gli strumenti e le policy di rete IT esistenti per gestire la stampa da smartphone e tablet, consentendo nel contempo agli utenti di stampare in tutta sicurezza e con la stessa facilità del PC, senza l'uso di applicazioni.

hp.com/go/JetAdvantageConnect

HP Access Control

Consente di ripristinare il controllo, rafforzare la sicurezza e ridurre i costi fornendo autenticazione della stampa basata su ruoli, funzionalità di autorizzazione e pull print protetta nell'intera azienda.

hp.com/go/hpac

HP JetAdvantage Secure Print

Consente di proteggere i documenti riservati con stampa pull print basata su cloud. Gli utenti eseguono l'autenticazione presso il punto di stampa prescelto per la stampa pull print dei loro processi.

hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Security Manager

Consente di ridurre i costi e le risorse per la gestione della sicurezza del parco dispositivi con uno strumento unico nel settore per la conformità della sicurezza di stampa basata su policy.⁴ Consente di stabilire policy di sicurezza valide per l'intero parco dispositivi, di automatizzare la correzione delle impostazioni dei dispositivi, di installare e rinnovare certificati univoci e generare rapporti di conformità per l'intero parco dispositivi.

hp.com/go/securitymanager

Per saperne di più:
hp.com/go/hpsecure

¹ HP Management Integration Kit non è preinstallato ed è disponibile all'indirizzo hp.com/go/clientmanagement.

² In base a un'analisi condotta nel 2016 da HP sui dati pubblicati relativi alle funzionalità di sicurezza nelle stampanti della concorrenza appartenenti alla stessa categoria. Solo HP offre una combinazione di funzioni di protezione che possono eseguire il monitoraggio al fine di rilevare e arrestare in automatico un attacco, quindi convalidare automaticamente l'integrità del software durante il riavvio. Per un elenco di stampanti, visitare: hp.com/go/PrintersThatProtect. Per maggiori informazioni: hp.com/go/printersecurityclaims.

³ In base alle funzionalità di sicurezza esclusive e complete di HP disponibili senza costi aggiuntivi e alla gestione di ogni aspetto del PC con il kit HP Manageability Integration, inclusi gestione di hardware, BIOS e software utilizzando Microsoft® System Center Configuration Manager, tra i venditori che vantano un volume di vendite annuale superiore al milione di unità a novembre 2016 per i PC HP Elite con processori Intel® Core® di settima generazione, scheda grafica integrata Intel® e WLAN Intel®.

⁴ L'affermazione è basata su una ricerca interna HP sulle offerte della concorrenza (Confronto sulla protezione dei dispositivi, gennaio 2015) e al report sulle soluzioni HP JetAdvantage Security Manager 2.1, elaborato da Buyers Laboratory LLC a febbraio 2015. Per maggiori informazioni, consultare hp.com/go/securitymanager.

Registratevi per ricevere gli aggiornamenti
hp.com/go/getupdated



Condividete con i colleghi

