HP WOLF SECURITY

HP WOLF ENTERPRISE SECURITY

HP SURE CLICK ENTERPRISE

SOLUZIONE BASATA SU Bromium

PREVENZIONE DEL FURTO DI CREDENZIALI

BLOCCO DEI TENTATIVI DI FURTO DELLE CREDENZIALI DA PARTE DEI SITI WEB NON SICURI

VISUALIZZAZIONE DEI SITI WEB IN TUTTA SICUREZZA, SENZA PREOCCUPARSI DELLE VIOLAZIONI

NESSUNA NECESSITÀ DI POLICY DI SICUREZZA IT RESTRITTIVE CHE LIMITANO L'ACCESSO DA PARTE DEGLI UTENTI

RUBARE CREDENZIALI APRE LA PORTA ALLE VIOLAZIONI

Oggi, la principale causa delle violazioni della sicurezza informatica nelle aziende sono gli attacchi di phishing, e le credenziali dei dipendenti sono l'obiettivo preferito degli hacker, perché sono essenziali per eludere gli altri protocolli di sicurezza adottati per proteggere l'azienda. Molto spesso, a un criminale informatico basta conoscere una combinazione corretta di nome utente e password per entrare in possesso della proprietà intellettuale di un'azienda.

Lo spear phishing è particolarmente efficace, perché spesso sfrutta un comportamento positivo, ovvero il desiderio della vittima di rispettare le policy di sicurezza fornendo o aggiornando proprio le credenziali che dovrebbero servire a proteggerla. Questi attacchi sono anche difficili da bloccare, perché i siti web dannosi sono numerosi e di breve durata. I loro contenuti, inoltre, variano spesso per evitarne una classificazione accurata.

IL PHISHING RESTA LA MINACCIA INFORMATICA PIÙ COMUNE ED EFFICACE AI DANNI DELLE AZIENDE

Gli attacchi di phishing sono in continua evoluzione e possono assumere varie forme:

- **Spear phishing:** truffe che ingannano singoli soggetti includendone nomi, ruoli e procedure di lavoro
- **Whaling:** attacchi rivolti ai funzionari delle aziende, spesso assumono la forma di note legali, reclami di clienti o problemi dell'amministrazione
- **Ingegneria sociale:** fa leva sul desiderio di fidarsi e aiutare gli altri, tipico della natura umana
- **Infezione involontaria:** condivisione di collegamenti a notizie o social media compromessi

Gli attacchi di phishing avvengono in vari modi:

- Collegamenti di phishing all'interno di e-mail
- Collegamenti o messaggi mirati sulle piattaforme di social media
- Collegamenti condivisi all'interno di programmi di chat

HP SURE CLICK ENTERPRISE[1] CONTRIBUISCE A PREVENIRE I FURTI DI CREDENZIALI INVIANDO AVVISI AGLI UTENTI E BLOCCANDO LA CONDIVISIONE DELLE INFORMAZIONI DI ACCESSO IN CASO DI SITI WEB DANNOSI O DI SCARSA REPUTAZIONE

Sure Click Enterprise[1] contribuisce a evitare il furto di credenziali impedendo agli utenti di inserire password in siti che raccolgono credenziali dopo aver fatto clic su un link di phishing in un'email, in un client di chat, in un file PDF o in un altro file. Quando un utente visita un sito web che richiede l'immissione di credenziali di accesso, Sure Click Enterprise utilizza il servizio HP Threat Intelligence per eseguire un'analisi in background su reputazione e dominio del sito, al fine di determinarne la sicurezza. In caso di siti noti, sicuri e legittimi, gli utenti potranno inserire le proprie credenziali in tutta libertà come di consueto, senza impedimenti da parte del software.

Se invece si tratta di un noto sito di phishing, un avviso verrà visualizzato sullo schermo quando l'utente tenta di inserire la propria password, così da impedire al sito di acquisire le credenziali. Il software può essere configurato in modo da consentire all'utente di scegliere se chiudere la finestra del browser in sicurezza, oppure continuare sul sito con tutti i campi di immissione dati disattivati.

Se il sito ha una scarsa reputazione, agli utenti viene consigliato di verificarlo ed evitare di inserire le proprie credenziali, a meno che non siano certi che si tratti di un sito sicuro. Gli amministratori possono scegliere di bloccare l'immissione delle credenziali in tali siti oppure consentire agli utenti di proseguire sul sito, inserendo l'indirizzo alla whitelist sul PC dell'utente, così che l'avviso non sia visualizzato per le sessioni future, riducendo i rallentamenti della produttività. Tutte le misure adottate per i siti dannosi noti e di scarsa reputazione vengono registrate e segnalate al controller Sure Click, per consentire al personale IT di esaminare lo stato delle minacce e il comportamento degli utenti.

PROTEZIONE DELLE CREDENZIALI: PER EVITARE LE VIOLAZIONI DOVUTE AGLI ATTACCHI DI PHISHING

IMPEDIRE I FURTI DI CREDENZIALI IN SEGUITO AD ATTACCHI DI PHISHING

Riduce il rischio che i dipendenti vengano ingannati da truffe di phishing.
Sure Click Enterprise impedisce agli utenti di inserire le credenziali di accesso in siti web dannosi noti, e segnala i comportamenti potenzialmente rischiosi in tutti i siti di scarsa reputazione.

SEMPLIFICAZIONE DELLA SICUREZZA INFORMATICA E RIDUZIONE DEI COSTI

Gli avvisi ad alta fedeltà di HP Sure Click Enterprise riducono drasticamente i tempi di triage ed evitano di sprecare risorse per l'analisi dei falsi allarmi. In questo modo è inoltre possibile eliminare tutte le attività di ripristino, ricostruzione o applicazione di patch di emergenza.

CONDIVISIONE DI THREAT INTELLIGENCE IN TEMPO REALE

L'intelligence adattiva identifica e arresta anche gli attacchi più difficili da rilevare, condivide i dati relativi alle minacce sulla rete aziendale in tempo reale e fornisce un'analisi completa della strategia di attacco al SOC.

PROTEZIONE DURATURA GRAZIE ALLA SICUREZZA BASATA SU HARDWARE

Solo HP Sure Click Enterprise si avvale di tecnologie di sicurezza basate sulla virtualizzazione per consentire l'isolamento delle applicazioni basato su hardware, offrendo protezione dalle minacce sconosciute e dai malware polimorfici che solitamente sfuggono anche agli strumenti di rilevamento più avanzati.

IL 67% DELLE VIOLAZIONI È DOVUTO A UN FURTO DI CREDENZIALI

- Verizon DBIR 2020[2]

LE VIOLAZIONI CAUSATE DAL FURTO DI CREDENZIALI COSTANO ALLE AZIENDE DI TUTTO IL MONDO IN MEDIA 3,86 MILIONI DI DOLLARI OGNUNA, E FINO A 8,36 MILIONI DI DOLLARI NEGLI STATI UNITI.

- IBM Cost of a Data Breach Report 2020[3]

Per ulteriori informazioni, consultare **https://www.hp.com/enterprisesecurity**

1. HP Sure Click Enterprise viene venduto separatamente e richiede Windows 8 o 10; sono supportati Microsoft Internet Explorer, Google Chrome, Chromium e Firefox. Gli allegati supportati includono Microsoft Office (Word, Excel, PowerPoint) e i file PDF, se sono installati Microsoft Office o Adobe Acrobat.
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2020/
3. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

4AA7-7469ITE, aprile 2021, Rev 2

HP WOLF SECURITY