HP WOLF SECURITY

HP WOLF ENTERPRISE SECURITY

HP SURE CLICK ENTERPRISE

SOLUZIONE BASATA SU Bromium

CONTENIMENTO DEGLI ATTACCHI DI PHISHING

APERTURA IN SICUREZZA DI QUALSIASI COLLEGAMENTO, ANCHE SE DANNOSO

ELIMINAZIONE DELLE POLICY DI SICUREZZA IT RESTRITTIVE CHE LIMITANO L'ACCESSO AGLI URL CONDIVISI DA PARTE DEGLI UTENTI

DIFESA DAI COLLEGAMENTI DI PHISHING CON USABILITÀ E PRESTAZIONI DEL BROWSER NATIVE

I COLLEGAMENTI DI PHISHING CONTINUANO A ELUDERE LE DIFESE MULTILIVELLO

Nonostante i progressi delle tecniche anti-phishing e la formazione dei dipendenti, gli attacchi di phishing sono sempre più diffusi, perché sono estremamente efficaci. Dopotutto, i dipendenti hanno la necessità di fare clic sui collegamenti per svolgere il loro lavoro e l'ingegneria sociale ostacola l'identificazione di quelli di phishing.

I collegamenti di phishing sono così efficaci perché i siti web dannosi sono numerosi e di breve durata. I loro contenuti, inoltre, variano spesso per evitarne una classificazione accurata. A questo si aggiunge il fatto che i dipendenti fanno clic sui collegamenti senza riflettere e lasciano sempre caselle e-mail e client di chat aperti, creando un percorso di accesso istantaneo per i criminali informatici.

UN METODO ECONOMICO ED EFFICACE PER L'INVIO DEI PAYLOAD DANNOSI

I collegamenti 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, che 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 accidentale:** 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 dannosi in allegati e-mail legittimi
- Collegamenti o messaggi mirati sulle piattaforme di social media
- Collegamenti condivisi all'interno di programmi di chat

HP SURE CLICK ENTERPRISE È UNA SOLUZIONE BASATA SU BROMIUM CHE ISOLA LE APPLICAZIONI PER IMPEDIRE ALLE MINACCE DI ACCEDERE ALL'HOST

HP Sure Click Enterprise[1] offre una rete di sicurezza virtuale agli utenti dei PC, persino quando le minacce sconosciute riescono a superare altre difese. La virtualizzazione basata su hardware isola i contenuti ad alto rischio per proteggere il PC, i dati e le credenziali dell'utente rendendo inoffensivi i malware, mentre il personale IT ottiene una threat intelligence utile ad aumentare ulteriormente il livello di sicurezza dell'organizzazione.

HP Sure Click Enterprise utilizza la sicurezza basata su virtualizzazione per proteggere le aziende dalle minacce di phishing, facendo in modo che tutti i collegamenti condivisi vengano aperti in una scheda del browser all'interno di una micro-VM. Grazie all'isolamento basato su hardware, ogni scheda del browser viene eseguita nel proprio container sicuro, completamente isolato dall'host e da tutte le altre schede del browser, in modo da prevenire la contaminazione incrociata. Quando si chiude la scheda del browser, la micro-VM viene distrutta insieme a tutte le eventuali minacce che contiene. Tutte le informazioni relative alla strategia di attacco dei malware vengono inviate al controller HP Sure Click Enterprise e condivise con tutti gli altri dispositivi HP Sure Click Enterprise della rete, rafforzando ulteriormente l'infrastruttura e riducendo la superficie di attacco complessiva.

ISOLAMENTO DELL'APPLICAZIONE: PROTEZIONE PRIMA DEL RILEVAMENTO

CONTENIMENTO DELLE MINACCE DI PHISHING

Apertura di ogni collegamento in una scheda del browser separata e isolata in una micro-VM. L'eventuale malware presente nel collegamento viene contenuto, così host e rete non sono esposti ad alcun rischio. In questo modo i dipendenti sono liberi di fare clic su qualunque collegamento in sicurezza.

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.

SECONDO I RICERCATORI FAU, IL 78% DELLE PERSONE DICHIARA DI ESSERE A CONOSCENZA DEI RISCHI RELATIVI A COLLEGAMENTI SCONOSCIUTI NELLE E-MAIL. EPPURE FA CLIC SU DI ESSI.

- Keepnet Lab[2]

QUASI IL 70% DELLE VIOLAZIONI È DOVUTO AD ATTACCHI DI INGEGNERIA SOCIALE, COME PHISHING E MESSAGGI E-MAIL COMPROMESSI, E AGLI ERRORI DEGLI UTENTI.

- Verizon DBIR 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. 2020 Phishing Statistics - Phishing Stats - Phishing Fact and Figures (keepnetlabs.com)
3. Verizon 2020 Data Breach Investigations Report, 19 maggio 2020

4AA7-7469ITE, aprile 2021, Rev 2

HP WOLF SECURITY