SINTESI DELLA SOLUZIONE

HP WOLF SECURITY

HP WOLF ENTERPRISE SECURITY

HP SURE CLICK ENTERPRISE

SOLUZIONE BASATA SU Bromium

PROTEZIONE DAI DOWNLOAD DI DOCUMENTI E FILE DANNOSI

DOWNLOAD E APERTURA IN TUTTA SICUREZZA DEI DOCUMENTI E FILE ESEGUIBILI PROVENIENTI DA SITI WEB SCONOSCIUTI O NON CLASSIFICATI

PROTEZIONE DAI DOWNLOAD DANNOSI CON USABILITÀ E PRESTAZIONI DELLE APPLICAZIONI NATIVE

ELIMINAZIONE DELLE POLICY DI SICUREZZA IT RESTRITTIVE CHE LIMITANO L'ACCESSO AI FILE SCARICATI, IMPEDENDO LO SVOLGIMENTO DEI FLUSSI DI LAVORO

SOTTO ATTACCO: I DOWNLOAD DI FILE DANNOSI POSSONO ARRIVARE DA VARIE FONTI

Per svolgere il proprio lavoro gli utenti devono essere in grado di scaricare file da fonti esterne. In genere gli utenti fanno clic rapidamente sui documenti condivisi, in media entro quattro minuti dall'arrivo nella loro casella di posta. I download dannosi possono infiltrare l'organizzazione in vari modi, ad esempio:

- Navigazione Web
- Clic su collegamenti condivisi
- Installazione di programmi
- Trasferimenti di file tramite FTP

I download dannosi sono particolarmente efficaci, perché i siti web dannosi sono molto diffusi, di breve durata e caratterizzati da contenuti estremamente mutevoli, che ne impediscono una classificazione accurata; con tipi di malware unici e polimorfici che eludono tutti i metodi di rilevamento tradizionali.

La diffusione dei malware tramite download di file è efficiente, economica e in continua evoluzione. Può assumere molte forme:

- **Download intenzionali:** l'utente avvia il download di un documento o di un file eseguibile durante la normale navigazione web.
- **Falsi aggiornamenti eseguibili:** l'utente viene indotto con l'inganno a scaricare un file dannoso mentre visita un sito web.
- **Collegamenti a documenti**: l'utente riceve un collegamento a un documento in una e-mail o un programma di chat che lo invita a scaricare un documento contenente malware.
- **Reindirizzamenti ad altri URL:** il collegamento iniziale reindirizza l'utente a un URL alternativo che lo inviata a scaricare un file.
- **DNS dannosi**: se il record di ricerca DNS è compromesso, l'utente rischia di scaricare un file dannoso anche se non commette alcun errore.
- **Driver e utilità fittizi:** l'utente viene reindirizzato a un sito di download non ufficiale e installa il malware accidentalmente.
- **Attacchi "watering hole":** un hacker infetta un sito Web che viene normalmente utilizzato dalla vittima designata, sostituendo o reindirizzando i download di file.

HP SURE CLICK ENTERPRISE È UNA SOLUZIONE BASATA SU BROMIUM CHE ISOLA LE APPLICAZIONI PER PROTEGGERE LE ORGANIZZAZIONI DALLE MINACCE DERIVANTI DAI DOWNLOAD DANNOSI

HP Sure Click Enterprise[3] 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.

Grazie all'isolamento basato su hardware, ogni documento o file eseguibile scaricato viene eseguito nel proprio container sicuro. Le minacce inviate tramite download di file vengono completamente isolate dall'host e da tutte le altre applicazioni, al fine di prevenire la contaminazione incrociata. Alla chiusura dell'applicazione o del file, la micro-VM viene distrutta insieme a tutte le minacce che contiene. Tutte le informazioni relative alla strategia di attacco dei malware 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

PROTEZIONE AUTOMATICA DI TUTTI I DOWNLOAD DAL WEB

Apertura in sicurezza di tutti i documenti o file eseguibili scaricati, indipendentemente dalla fonte (HTTP/ HTTPS, FTP e così via). Grazie all'isolamento all'interno delle micro-VM protette, gli utenti possono scaricare i file e accedervi in tutta sicurezza, mantenendo invariata l'esperienza utente.

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.

OGGI IL 38% DEI MALWARE SI NASCONDE ALL'INTERNO DI UN DOCUMENTO DI WORD.[1]

- Safety Detectives

DAL 2007, NEL 2020 I SITI DI PHISHING HANNO REGISTRATO UN AUMENTO SUPERIORE AL 750%.[2]

- Comparitech 2021

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

1. 15 (CRAZY) Malware and Virus Statistics, Trends & Facts (safetydetectives.com)
2. Malware Statistics in 2021: Frequency, impact, cost & more (comparitech.com)
3. 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.

4AA7-7469ITE, aprile 2021, Rev 2

HP WOLF SECURITY