SINTESI DELLA SOLUZIONE

HP WOLF SECURITY

HP WOLF ENTERPRISE SECURITY

# HP SURE CLICK ENTERPRISE

SOLUZIONE BASATA SU Bromium

## BLOCCO DEGLI ALLEGATI E-MAIL DANNOSI

POSSIBILITÀ DI APRIRE IN TUTTA SICUREZZA QUALSIASI ALLEGATO E-MAIL RICEVUTO TRAMITE OUTLOOK O WEBMAIL, ANCHE SE CONTIENE MALWARE

ELIMINAZIONE DELLE POLICY DI SICUREZZA IT RESTRITTIVE CHE LIMITANO L'ACCESSO AGLI ALLEGATI E-MAIL

MAGGIORE PRODUTTIVITÀ DEGLI UTENTI, PERMETTENDO AI DIPENDENTI DI APRIRE GLI ALLEGATI E-MAIL

### I DIPENDENTI DEVONO APRIRE GLI ALLEGATI E-MAIL PER SVOLGERE IL PROPRIO LAVORO

I dipendenti hanno spesso a che fare con allegati e-mail per il proprio lavoro: lettura di curricula, elaborazione di fatture, ricezione di notifiche di recapito, condivisione di rendiconti finanziari o attività su contratti legali in collaborazione con utenti esterni. Di solito, quindi, li aprono perché appaiono sicuri. I criminali informatici conoscono bene questa vulnerabilità e la sfruttano a proprio vantaggio.

Oggi i ransomware vengono spesso recapitati per e-mail all'interno di documenti di Microsoft Office o file PDF compromessi. I criminali informatici utilizzano questo metodo perché funziona. In base alle statistiche del 2019, gli attacchi ransomware hanno causato perdite per oltre 7,5 miliardi di dollari alle organizzazioni.[1]

Anche le applicazioni legittime (molte delle quali sono esplicitamente incluse nelle whitelist, inclusa la Microsoft Office Suite) possono essere sfruttate per eludere le difese multilivello e ottenere un punto di accesso all'organizzazione attraverso un singolo host compromesso.

Nonostante i notevoli progressi nelle tecnologie di rilevamento dei malware, il costante miglioramento dei gateway di sicurezza e-mail e l'incremento dei corsi di sensibilizzazione degli utenti, gli allegati e-mail dannosi riescono comunque a superare tutte le difese, provocando violazioni, perdite e persino la distruzione dei dati.

Oggi i malware più sofisticati eludono con semplicità le difese tradizionali basate sul rilevamento, arrivando tramite e-mail.

**Le cifre parlano chiaro:**

- Più del 90% degli allegati e-mail dannosi ha capacità polimorfiche.[2]
- Il 53% dei virus viene diffuso tramite file .exe[3] e il 46% degli hacker inoltra malware quasi esclusivamente tramite e-mail.[3]

### I MALWARE INVIATI TRAMITE E-MAIL SONO ECONOMICI, EFFICIENTI E IN CONTINUA EVOLUZIONE

**Gli attacchi più efficaci per i criminali informatici di oggi sono:**

- **Ransomware:** i dati sul PC della vittima vengono crittografati con una chiave simmetrica, e l'utente deve scegliere se pagare il riscatto o ripristinare il computer. Sono frequenti e vengono recapitati principalmente tramite documenti dannosi.
- **Trojan basati su macro:** rilasciano nell'host file binari dannosi che stabiliscono una comunicazione con server remoti di comando e controllo per ricevere ulteriori istruzioni e scaricare ulteriori codici dannosi.
- **Malware fileless:** sfruttano strumenti come PowerShell per eseguire comandi senza rilasciare alcun file nell'host.
- **Collegamenti dannosi:** si nascondono all'interno di allegati e-mail apparentemente innocui per superare le difese multilivello e hanno come risultato download drive-by o exploit del browser.

## HP SURE CLICK ENTERPRISE ISOLA LE APPLICAZIONI PER CATTURARE I MALWARE NASCOSTI NEGLI ALLEGATI E-MAIL

Gli utenti possono disporre di una rete di sicurezza virtuale che li protegge da minacce note e sconosciute, isolando i contenuti ad alto rischio; vengono inoltre forniti insight utili per migliorare il livello di sicurezza dell'organizzazione. Grazie alla sicurezza basata sulla virtualizzazione, HP Sure Click Enterprise apre gli allegati e-mail (come documenti di Microsoft Office e file PDF) in una micro-VM isolata. I malware possono così avviare ed eseguire azioni, ma non ottengono mai l'accesso all'endpoint o alla rete. In pratica, i malware restano intrappolati all'interno del container della micro-VM, che li rende completamente innocui per l'utente, e vengono poi distrutti quando l'utente chiude l'allegato e-mail.

La possibilità di eseguire i malware cambia completamente la cultura degli Help Desk, perché gli utenti finali possono vantarsi di aver catturato un malware, anziché lamentarsi dei vincoli imposti dalla sicurezza informatica.

## ISOLAMENTO DELL'APPLICAZIONE: PROTEZIONE PRIMA DEL RILEVAMENTO

### CONTENIMENTO DEGLI ALLEGATI E-MAIL

Tutti gli allegati e-mail vengono aperti in una micro-VM isolata. L'eventuale malware presente nell'allegato viene contenuto e non è in grado di accedere all'host, così la rete non è esposta ad alcun rischio.

### 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 46% DEGLI HACKER INVIA MALWARE QUASI ESCLUSIVAMENTE TRAMITE E-MAIL[3]**

- Verizon DBIR 2020[3]

**LE ULTIME STATISTICHE SUI VIRUS INFORMATICI MOSTRANO CHE IL 53% DEI VIRUS VIENE DIFFUSO TRAMITE FILE .EXE.**

- Checkpoint 2020[3]

**"È UN OTTIMO PRODOTTO E PROTEGGE LA NOSTRA AZIENDA IN MODO ESTREMAMENTE EFFICACE."**

- IT Systems Analyst di un'azienda bancaria inclusa nelle Global 500[4]

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

1. 34 Shocking 22 Shocking Ransomware Statistics for Cybersecurity in 2021 (2019) - SafeAtLast.co
2. Top 10 Email Malware Threats | eSecurity Planet /
3. A Not-So-Common Cold: Malware Statistics in 2021 | DataProt
4. TechValidate. https://www.techvalidate.com/tvid/813-0A2-81D
5. 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.



4AA7-7467ITE, aprile 2021, Rev 2

HP WOLF SECURITY