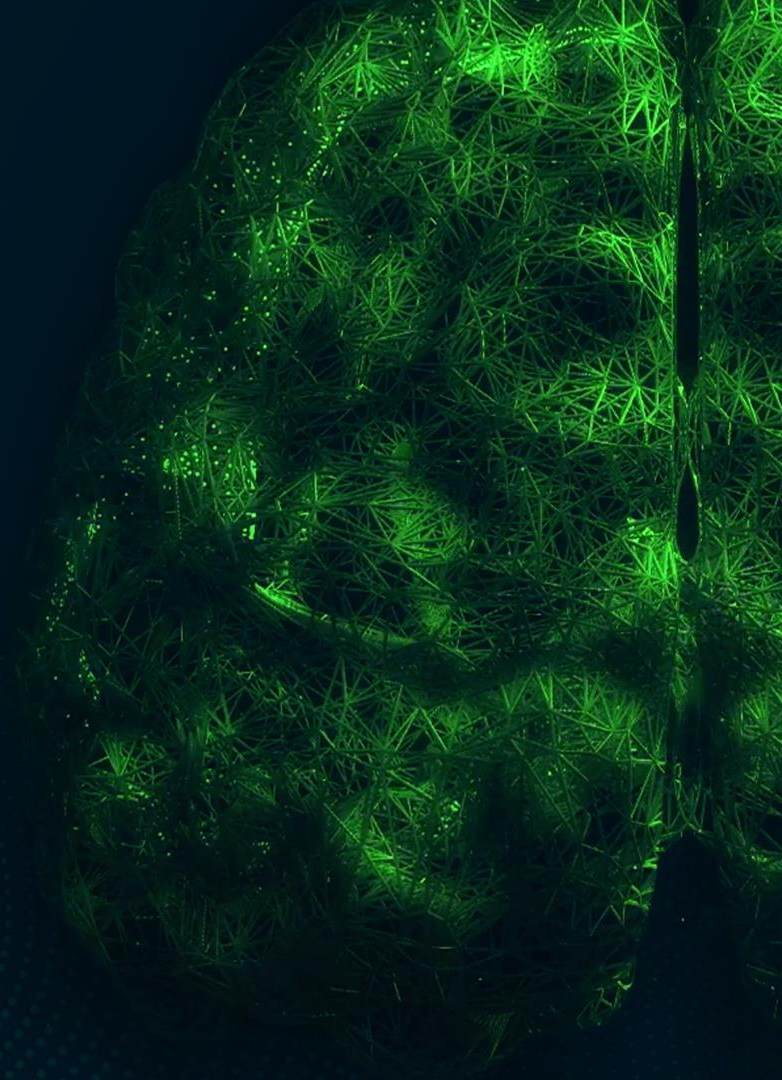
ERMES™

Intelligent Web Protection

Move to the real time human centric protection



ERMES
Intelligent Web Protection

LISTINI PREZZI END USER
LICENZA PER DISPOSITIVO*

MODULI DI SICUREZZA PER UN'OFFERTA PERSONALIZZATA
INVISIBLE USER (WEB TRACKING, MALVERTISING, SESSION REPLAY SCRIPT, CRYPTOJACKING)
ZERO DAY PROTECTION (ANTIPHISHING)
EXTENSION VETTING (MALICIOUS BROWSER EXTENSIONS DETECTION)
BUSINESS ACCOUNT PROTECTION
CYBER SQUATTING & MALICIOUS URLS PROTECTION
CUSTOM CONTENT FILTERING

*** Con "device" si intende PC o mobile per ogni utente, indipendentemente dal browser utilizzato**

CONFIDENTIAL

ERMES
Intelligent Web Protection

LISTINO PREZZI – DESCRIZIONE MINACCE
INVISIBLE USER

Web tracking
E’ la pratica con cui alcuni servizi dei siti web (chiamati Web tracker) raccolgono, memorizzano e condividono le informazioni sulle attività dei visitatori sul Web. L'analisi del comportamento di un utente può essere utilizzata per fornire contenuti che consentano all'operatore di dedurre le sue preferenze e che possano essere di interesse per varie parti, come gli inserzionisti. Inoltre, va considerato che statisticamente ogni anno più del 15% dei web tracker subisce una violazione dei dati a causa diun attacco informatico.

Session-replay script
Servizi web che sono in grado di registrare i tasti, i clic, i movimenti del mouse e lo scorrimento degli utenti quando sono su un sito web, insieme al contenuto completo della pagina web che stanno visitando. Il replay delle sessioni è uno strumento popolare per aiutare le aziende a determinare come vengono utilizzati i loro siti web e per identificare potenziali problemi come link non funzionanti, problemi di progettazione delle pagine o motivi per cui gli utenti abbandonano un sito.

Malvertising
Un portmanteau di "malicious software (malware) advertising", è l'uso della pubblicità online per diffondere malware. In genere consiste nell'iniettare annunci pubblicitari dannosi o carichi di malware in reti pubblicitarie online e pagine web legittime, senza compromettere direttamente tali pagine web.

Crypto Jacking
Servizi Web che sono in grado di sfruttare la potenza computazionale (CPU) dei computer, per estrarre criptovalute, di solito all'insaputa degli utenti. I servizi di cryptojacking possono causare rallentamenti e crash a causa dell'affaticamento delle risorse computazionali.

Approfondimenti: Link 1, Link 2, Link 3, Link 4, Link VIDEO

CONFIDENTIAL

ERMES
Intelligent Web Protection

LISTINO PREZZI – DESCRIZIONE MINACCE
ZERO-DAY PROTECTION (ANTIPHISHING)

Zero-day protection (antiphishing)

I phisher sono diventati molto abili nel loro approccio. Circa l'85% dei siti di phishing esiste per meno di 24 ore, con un ciclo di vita medio inferiore alle 15 ore. In alcuni casi il sito è attivo anche solo per 15 minuti. Il breve ciclo di vita e la natura rapida di molte di queste campagne di phishing non forniscono in genere alle soluzioni tradizionali (WSG/Proxy/Firewall) il tempo sufficiente per analizzare adeguatamente i siti e inserirli nelle blacklist.

Approfondimenti: Link 1, Link 2, Link 3, Download Whitepaper

CONFIDENTIAL

LISTINO PREZZI – DESCRIZIONE MINACCE
EXTENSION VETTING

Extension-Vetting

Le estensioni web (plug-in del browser) sono software che, se possiedono determinati permessi, possono iniettare codice dannoso nelle pagine per causare download di malware, rubare credenziali, reindirizzare a pagine false e così via. Il vetting delle estensioni è la capacità di analizzare e valutare il comportamento di qualsiasi estensione del browser presente sui vari dispositivi aziendali, in modo che gli utenti e gli amministratori IT possano decidere se mantenere o disinstallare tali estensioni.

Approfondimenti: Link 1, Link 2, Link 3, Download Whitepaper

ERMES
Intelligent Web Protection

LISTINO PREZZI – DESCRIZIONE MINACCE
BUSINESS ACCOUNT PROTECTION

Business account protection

Nonostante l'esistenza abituale di policy scritte sull'uso legittimo degli account aziendali, i dipendenti tendono a riutilizzare le proprie credenziali aziendali su siti non legati all'attività lavorativa (ad esempio e-commerce, social network, forum), ampliando così la superficie di rischio per la perdita delle credenziali. Grazie a Ermes, è finalmente possibile applicare politiche di utilizzo degli account, impedendo agli utenti di iscriversi o accedere a siti non legati all'attività lavorativa utilizzando il proprio account aziendale. Inoltre, questa funzione rappresenta un ulteriore livello di protezione contro gli attacchi avanzati di phishing delle credenziali, come la nuova tecnica del Browser In The Browser.

Approfondimenti: Link 1

CONFIDENTIAL

ERMES
Intelligent Web Protection

LISTINO PREZZI – DESCRIZIONE MINACCE
CYBERSQUATTING & MALICIOUS URLs PROTECTION

Cybersquatting
La tecnica di attacco che utilizza nomi di domini web che assomigliano e/o «suonano» come quelli famosi legittimi, con l'obiettivo di ingannare il visitatore e fargli credere che sta visitando la controparte legittima, in modo da incoraggiarlo a svolgere le stesse attività che farebbe sul sito reale, ad esempio accedere a un servizio web aziendale, al sito della banca e così via, fornendo in ultima analisi agli hacker informazioni molto sensibili.

Malicious URLs
Un URL (Uniform Resource Locator) viene classificato come dannoso quando il servizio che fornisce, qualunque esso sia, è riconosciuto per avere comportamenti malevoli. Gli URL dannosi possono essere creati e utilizzati, ad esempio, come punto di distribuzione di malware, oppure possono rimandare a un sito web che esegue attacchi come il download e l'installazione di un eseguibile infetto sul computer dell'utente o l'accaparramento di informazioni sensibili. Gli utenti possono imbattersi in URL dannosi durante la navigazione e/o nelle e-mail di phishing.

Approfondimenti: Link 1, Link 2, Link 3

CONFIDENTIAL

LISTINO PREZZI – DESCRIZIONE MINACCE
CONTENT FILTERING

Content filtering

La maggior parte dei siti web su Internet sono classificati in base allo scopo per cui sono stati creati o ai contenuti che forniscono. Il filtraggio dei contenuti è la capacità di bloccare o consentire i siti web in base alla loro categorizzazione. Il vantaggio di avere questo tipo di funzione è quello di assicurarsi che i dispositivi aziendali non abbiano accesso a siti web non necessari (ovunque si trovino anche fuori l'azienda e/o senza VPN) e di ridurre la superficie di rischio evitando tutte le categorie che di solito nascondono minacce.

CONFIDENTIAL