# DOSSIER STAMPA

**ERMES: INTELLIGENT ANTI PHISHING 2020**

**7 PLUS DI ERMES**

**TRE (INTENSI) ANNI DI STORIA**

**GLI SQUALI DEL WEB**

**LE PRINCIPALI MINACCE PER LA CYBER SECURITY**

**EVOLUZIONE DEL PHISHING**

**SHARK PHISHING… CONTRO GLI SQUALI DELLA RETE**

**3 PAROLE-CHIAVE PER LA SICUREZZA**

**AREA STAMPA ONLINE**
*Testi e immagini in alta risoluzione*

**Ufficio Stampa Threesixty**
Gabriella Braidotti 348-3152102 g.braidotti@360info.it
Andrea Toninello 328-96669921 a.toninello@360info.it

## ERMES: LA CYBER SECURITY DEL 2020

Nata nel 2018 all'interno dell'Incubatore I3P del Politecnico di Torino, **Ermes - Intelligent Anti Phishing** è l'azienda italiana fondata da **Hassan Metwalley** che sta rivoluzionando i sistemi di sicurezza informatica corporate, offrendo soluzioni totalmente automatiche basate sull'intelligenza artificiale.

### IL PROBLEMA

Lo smartphone ha mutato radicalmente anche le abitudini lavorative. La navigazione di manager e dipendenti su operatore telefonico, wifi o reti VPN per smaltire il carico di posta elettronica; i continui login sulle proprie piattaforme da remoto hanno reso ogni utente un potenziale portatore di attacchi informatici. Prima dell'avvento di tablet e smartphone gli attacchi avvenivano tramite phishing generico, infettando l'hardware e passando dalla singola macchina al server.
Firewall e crittografia sono alla base dei vari sistemi di protezione tradizionale. Lo stesso protocollo HTTPS, un tempo indice di privacy e maggiore sicurezza della navigazione, non garantisce però l'utente dall'attacco digitale.
Oggi l'elemento umano è quasi sempre al centro di incidenti e violazioni di cybersecurity. Si parla infatti di Spear Phishing e in generale di nuove formule di attacchi, più subdoli e devastanti. Nel report *SANS 2019 State of OT/ICS Cybersecurity Survey* curato da Barbara Filkins si parla del 48% degli attacchi da browser. Una percentuale che sale al 55% se parliamo di attacchi mirati (Spear Phishing) e destinata a crescere drasticamente nei prossimi anni.

### L'IDEA

Ermes ha sviluppato un sistema di protezione e prevenzione che sopperisce alle carenze dei filtri tradizionali assicurando una tutela integrale della navigazione. Gli algoritmi brevettati non solo analizzano il traffico di ogni utente proteggendolo in tempo reale, ma sviluppano continuamente nuovi "anticorpi".
In pratica si attiva dall'interno una vera e propria "caccia agli squali informatici" in tre fasi: preparazione, esecuzione e prevenzione.
Una soluzione in grado di bloccare totalmente la fuoriuscita di informazioni sensibili verso i Web tracker per prevenire ogni possibile minaccia dal web.
Il sistema nesso a punto da Ermes si installa in pochi minuti, è completamente automatico e non richiede interventi di manutenzione. Inoltre le aziende possono facilmente personalizzare una dashboard con report e statistiche.

## 7 PLUS DI ERMES

1. **SICUREZZA**
   Il sistema Ermes può leggere, filtrare e manipolare qualsiasi tipo di traffico sul Web, anche quello cifrato (come ad esempio il protocollo https) che attualmente rappresenta la quasi totalità.

2. **VELOCITÀ**
   Lo scudo intelligente ripulisce il traffico e migliora la navigazione per l'utente finale che diventa in media fino a 4 volte più veloce.

3. **COPERTURA A 360°**
   Ermes - Intelligent Anti Phishing protegge tutti i dispositivi aziendali (desktop, notebook, smartphone, tablet) ovunque essi si trovino (al lavoro, a casa, in aeroporto, ecc.) e con qualsiasi tipo di connessione (via cavo, wifi, 3G, ecc.).

4. **NIENTE VPN**
   Il sistema messo a punto da Ermes consente alle aziende di lavorare anche senza una rete virtuale privata (VPN).

5. **ALGORITMO INTELLIGENTE**
   Grazie ad algoritmi brevettati, Ermes rileva automaticamente sia nuovi tracker che quelli che hanno semplicemente mutato il loro comportamento. È di fatto l'unico sistema che al momento può garantire una protezione aggiornata in tempo reale.

6. **SCALABILITÀ**
   L'installazione dell'algoritmo avviene tramite un computer "Master" dell'azienda e si applica poi a tutti i device. Un metodo che rende l'installazione dello scudo intelligente Ermes facile, veloce e soprattutto scalabile.

7. **RISPARMIO**
   Tra i vantaggi non è certo trascurabile il risparmio economico. Con una media del 30% in meno di traffico Web non solo diminuisce il carico di lavoro per la propria infrastruttura di rete interna ma si abbattono anche i costi del servizio web.

## TRE (INTENSI) ANNI DI STORIA

Ermes - Intelligent Anti Phishing nasce da un gruppo di studio sul fenomeno del web tracking e della privacy guidato da Marco Mellia professore del Dipartimento di Elettronica e Telecomunicazioni del Politecnico di Torino, oggi advisor dell'azienda.
I due fondatori, **Hassan Metwalley** (CEO) e **Stefano Traverso** (CTO), sono infatti due ex ricercatori Post-doc presso il Telecommunication Networks Group del Politecnico.
Prima spin-off del Politecnico di Torino, poi incubata presso I3P (l'Incubatore Imprese Innovative di dello stesso istituto universitario) oggi Ermes è una realtà aziendale che coinvolge una trentina di ingegneri informatici esperti in cyber security, data science, big data, machine learning e intelligenza artificiale.

La soluzione tecnologica sviluppata è frutto di un lungo lavoro di ricerca finanziato con un bando Proof of Concept da parte del Politecnico di Torino coperto da brevetto Europeo e uno in **estensione internazionale**.
Il settore in cui si inserisce Ermes è quello dell'Endpoint Security, che si occupa di sistemi di protezione per i singoli dispositivi. Un mercato in crescita esponenziale nell'ultimo quinquennio che vale già oggi oltre 5.000 miliardi di dollari a livello mondiale con previsioni di **8.540 miliardi** di dollari nel 2021. Restringendo l'analisi al mercato europeo (30% del totale) parliamo di un mercato da **1,7 miliardi di dollari** nel 2021 con un CAGR del **12,7% dal 2016.**

Una crescita ulteriormente rafforzata dal regolamento europeo sulla protezione dei dati (**GDPR**) e dalla direttiva sulla sicurezza delle reti e dei sistemi informativi (**NIS**). Entrambi gli impianti legislativi, infatti, puntano ad incrementare l'awareness verso tematiche di privacy e cyber security, obbligando al tempo stesso le aziende a dotarsi di prodotti di protezione contro le minacce informatiche.

Se il settore pubblico è al centro dell'attenzione dei criminali (+44%) aumentano gli attacchi ai centri di ricerca e formazione (+55%), ai fornitori di servizi di cloud computing (+36%) e al mondo finanziario (+33%). **Il 30% delle aziende che subisce un attacco informatico arrivano a dichiarare fallimento** e chiudere l'attività durante il primo anno dall'attacco, il 50% entro il secondo anno.
Il World Economic Forum nel 2019 ha classificato i cyber-attack al secondo posto in ordine di gravità dopo i rischi causati dal global warming.

## GLI SQUALI DEL WEB

La navigazione Web è collegata alle informazioni personali di un utente. Posizione, interessi, acquisti e altro ancora possono essere tracciati per analizzare i modelli di attività a fini commerciali ma – sempre più- anche per aggredire tramite gli utenti aziende e istituzioni.
Naturalmente l'uso del tracciamento web è oggetto di direttive come quella dell'Unione Europea sull'uso dei cookies nonché sulla privacy ma non tutti prestano attenzione al funzionamento dei web tracker.
Esistono soluzioni per ridurre il monitoraggio web di terze parti, ma poche sono effettivamente funzionanti. Anche la disattivazione dei cookie o navigazione in incognito ormai non bastano ad arginare le modalità con cui l'utente viene monitorato.

FINGERPRINTING CANVAS - consente ai siti di identificare e tracciare gli utenti utilizzando elementi tipici di HTML5 anziché i cookie del browser.

TRACCIAMENTO TRA DISPOSITIVI - viene utilizzato dagli inserzionisti per identificare quali canali hanno più successo nell'aiutare a convertire i browser in acquirenti.

PERCENTUALE DI CLIC - utilizzata dagli inserzionisti per misurare il numero di clic che ricevono sui propri annunci per numero di impressioni.

TRACCIAMENTO DEL MOUSE - raccoglie le posizioni del cursore sul computer.

IMPRONTA DIGITALE DEL BROWSER - è un modo per identificare gli utenti ogni volta che vanno online anche quando abbiano disabilitato il salvataggio dei cookie. Attraverso l'impronta digitale i siti possono recuperare diverse informazioni relative al dispositivo: sistema operativo, lingua, fuso orario, posizione geografica e versione del browser senza bisogni di autorizzazione.

SUPERCOOKIES O EVERCOOKIES - sono difficili da rilevare e da rimuovere poiché sono memorizzati in modo diverso rispetto ai cookie standard e si rigenerano automaticamente, anche senza navigare sul web.

WEB BEACON - vengono comunemente utilizzati per verificare se una persona che ha ricevuto un'e-mail la legga o meno.

## GLOSSARIO DEL TRACCIAMENTO

**WEB TRACKING** - Il tracciamento Web è la pratica mediante la quale gli operatori di servizi esterni si appoggiano a siti web per raccogliere, archiviare e condividere informazioni sull'attività di chi naviga online. L'analisi del comportamento dell'utente può essere utilizzata per fornire contenuti relativi alle sue preferenze implicite.

**PROFILAZIONE** - Le società pubblicitarie raccolgono informazioni sugli utenti per riuscire a personalizzare gli annunci pubblicitari. Le attività degli utenti includono non solo siti visitati, video guardati, interazioni sui social network ma anche stato della batteria dello smartphone, posizione o transazioni online.
Portali come Netflix raccolgono informazioni su ciò che gli utenti guardano in modo da costruire palinsesti di successo.

**TEST DI USABILITÀ** - La pratica di testare la facilità d'uso di un progetto. Gli utenti vengono osservati mentre completano le attività. Ciò dovrebbe contribuire a identificare i problemi in modo che possano essere risolti.

**GOOGLE TRACKING** - I motori di ricerca come Google tengono traccia delle attività e degli utenti e delle keyword utilizzate in modo da migliorare la pertinenza delle risposte nonché suggerire siti o prodotti “simili”.

**FILTER BUBBLE O BOLLA DI FILTRAGGIO** - La bolla di filtraggio è il risultato del sistema di personalizzazione dei risultati di ricerche su siti che registrano la storia del comportamento dell'utente.

**INDIRIZZI IP** - Ogni dispositivo collegato a Internet dispone di un proprio indirizzo IP, un numero che dunque identifica gli utenti su Internet. I Web tracker determinano la posizione geografica degli utenti anche da questo indirizzo.

**COOKIE** - Sono informazioni salvate dal browser web. Quando un utente visita un sito questo potrebbe memorizzare un cookie in modo da riconoscerlo in futuro, quando dovesse tornare sullo stesso sito. I cookie proprietari vengono creati dal dominio visitato dall'utente. Questi sono i cookie considerati buoni. Aiutano a fornire un'esperienza migliore agli utenti.

Le terze parti vengono create da siti diversi da quello che gli utenti visitano. Inseriscono metodi di tracciamento aggiuntivi per registrare pagine visitate e contenuti letti; cronologia di navigazione; clic su annunci online; orari di visita di un sito. Vengono utilizzati per far pervenire all’utente annunci mirati.

## LE PRINCIPALI MINACCE PER LA CYBER SECURITY

**Furto d'identità** - Le informazioni su dipendenti e loro dispositivi vengono tracciate e archiviate su sistemi esterni all'azienda mettendo a rischio non solo la privacy, ma anche la sicurezza del singolo ma dell'intera rete dell'azienda.

**Keylogging** - I servizi di terze parti incorporati nei siti possono registrare e archiviare qualsiasi azione eseguita sulle pagine visitate, come clic e sequenze di tasti. I dati raccolti contengono anche credenziali e numeri di carta di credito.

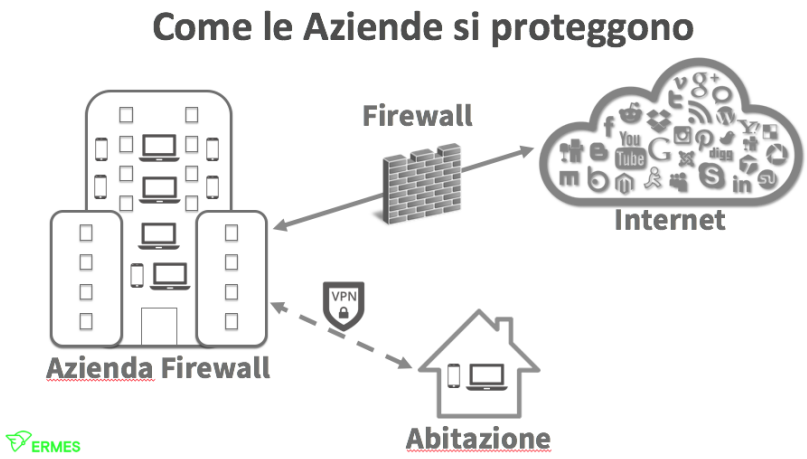
**Tabnabbing** - Furto delle credenziali di accesso attraverso false tab o finestre web simili a quelle dei siti di utilizzo comune come Facebook, gmail, ecc.. L'utente immette senza saperlo username e password.

**Fraudolent Data Collection** - Le informazioni sensibili vengono esposte a terzi sconosciuti dalla normale navigazione dei dipendenti. Cronologie web, tracce di clic, contatti e credenziali forniti nei moduli possono essere rubati e utilizzati per scopi dannosi.

**Spionaggio digitale** - I profili creati dai tracker sono fuori dal controllo dell'azienda. Questi possono essere ceduti a concorrenti o utilizzare per bloccare linee produttive.

**Cryptojacking** - Molti siti incorporano script che sfruttano le risorse di calcolo disponibili sui dispositivi dei visitatori per estrarre criptovalute. I dipendenti vedono rallentare le prestazioni dei loro dispositivi (fino al 95%) e prendono involontariamente parte a una rete di mining spesso illegale.

## EVOLUZIONE DEGLI ATTACCHI INFORMATICI




Fino a qualche anno fa le aziende si proteggevano tramite Firewall (vere e propria mura cibernetiche per difendere i server da attacchi diretti) e linee VPN (per le comunicazioni e la navigazione da remoto).

Se il firewall resta il principale baluardo contro gli hacker, l'aumento di traffico cifrato (protocollo https://) ha reso indispensabile aggiungere nuovi livelli di protezione della navigazione per sopperire alle lacune di web filtering e proxy.
Il sistema Ermes si innesta proprio su questo gap potenziando i filtri tradizionali.
Una tutela integrale della navigazione che rappresenta oggi la soluzione più sicura rispetto ai moderni attacchi informatici.

Il progressivo spostamento di dati e attività aziendali sul cloud ha contribuito a rendere i browser (come Chrome, Firefox, Safari ecc) veri e propri portali di accesso per gli hacker.
E se il 48% degli attacchi è legato ai browser (report SANS 2019), il 55% passa attraverso l'identità digitale dei singoli utenti.
Invece di aggredire le sempre piú sofisticate protezioni dei sistemi aziendali, gli hacker si sono focalizzati sull'errore umano sviluppando nuovi sistemi di phishing. Tramite le credenziali degli utenti può essere facilissimo entrare all'interno dell'azienda senza dover fare breccia nelle protezioni hardware.

Il furto dell'identità digitale diventa così **un pericolo concreto non solo per la privacy** ma anche per le aziende che possono subire danni importanti.
Secondo il Rapporto CLUSIT 2019 sulla sicurezza informatica in Italia il numero di casi censiti, orientati soprattutto a finalità di crimini informatici e di furto di dati personali, è aumentato del 99% rispetto al 2017.

## SHARK-PHISHING CONTRO GLI SQUALI DELLA RETE

Il termine phishing è una variante di *fishing* (letteralmente "pescare") e indica un tipo di truffa, effettuata su Internet per carpire informazioni personali, dati finanziari o codici di accesso. In origine si trattava di invio massivo di messaggi per indurre gli utenti a scaricare virus oppure a fornire informazioni riservate.
Negli ultimi anni si è evoluta anche grazie all'utilizzo di social media, ai continui login anche da smartphone.

Si parla di Spear Phishing per indicare una "pesca" più mirata e importante (con tanto di "fiocina") rivolta cioè a danneggiare una specifica azienda colpendo pochissimi dipendenti (spesso meno di 5) sfruttando i loro interessi e la loro vita.
Da una e-mail simile per grafica e contenuto a quelle provenienti da fonti attendibili, vicine all'utente, si conduce il destinatario a un sito fittizio che non punta più a infettare con malware, ma punta a rubare identità digitali o credenziali con cui poi attaccare l'azienda bypassando le normali protezioni tipo firewall o VPN.
Email provenienti da onlus, organizzazioni benefiche, ma anche banche, aziende o piattaforme frequentate normalmente dall'utente.

Sofisticate tecniche di social engineering su misura sono sempre più in grado di personalizzare in modo efficace messaggi e siti. Anche i massimi dirigenti possono così aprire e-mail portatrici di pesanti attacchi informatici, che possono arrivare a bloccare completamente le linee produttive di un'azienda (ormai per il 99% informatizzate).
Secondo le più recenti indagini sulla cyber security la percentuale delle persone in grado di riconoscere i diversi tipi di phishing non arriva al 18%. Questa nuova tipologia di attacchi può distribuire malware per la violazione dei computer, organizzandoli in enormi reti denominate *botnet* che possono essere utilizzate per attacchi DoS (Denial-of-Service). Considerando che lo spear phishing ha percentuali di successo 10 volte superiori al phishing classico, è fondamentale che aziende e dipendenti maturino una nuova consapevolezza.
Il sistema messo a punto da Ermes attiva una vera e propria "caccia agli squali informatici" tramite tre fasi: preparazione, esecuzione e prevenzione.
"*Ciò che meglio descrive l'unicità del nostro sistema rispetto ai vari dispositivi di protezione sul mercato è che si tratta di una vera e propria strategia di contrattacco*" spiega Hassan Metwalley, fondatore di Ermes "*Dallo studio delle più recenti evoluzioni dello spear phishing è evidente che si tratta di sistemi sofisticati, in continua evoluzione, che possono contare su risorse importanti, provenienti dalla 'parte oscura' del web. I nostri algoritmi diventano un prezioso alleato delle aziende: una sorta di cacciatore di squali, in grado di prevenire gli attacchi degli hacker*".

## LE 3 PAROLE CHIAVE DELLA SICUREZZA

Il sistema messo a punto da Ermes attiva una vera e propria “caccia agli squali informatici” in tre fasi: preparazione, esecuzione e prevenzione.

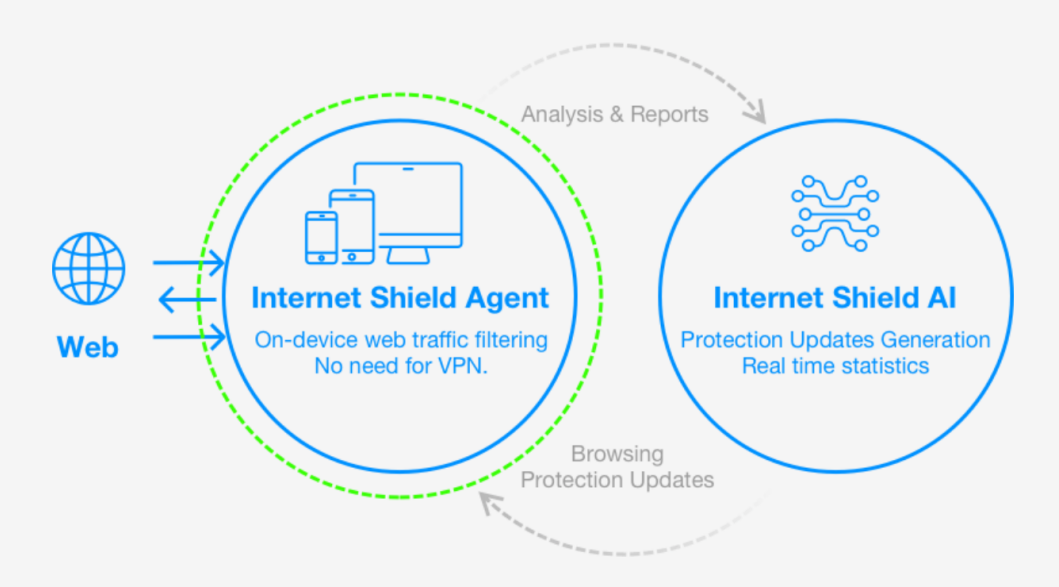
**PREPARAZIONE** – Il sistema Ermes filtra il web-tracking dal dispositivo su cui viene installato. Normalmente ogni licenza copre due dispositivi per utente: ad esempio il computer dell’ufficio e lo smartphone o due laptop. Anche tutte le operazioni di web-keylogging (ovvero tutti gli inserimenti di password) vengono filtrati e protetti.

**ESECUZIONE** - In pratica tutta la navigazione dell’utente viene protetta (anche da pubblicità). Il primo effetto sensibile è la velocità di navigazione. Si attiva uno scudo efficace contro malvertising (attacchi che attraverso finti annunci pubblicitari reindirizzano l’utente verso siti potenzialmente dannosi); cybersquatting (azioni volte ad appropriarsi dei siti di grandi marchi commerciali, aziende o personaggi famosi, causando enormi danni reputazionali) o quelle forme di pishing che spingono l’utente a cedere credenziali sfruttando la disattenzione (tabnabbing).

**PREVENZIONE** – Oltre a difendere da ogni attacco di Spear Phishing l’algoritmo brevettato da Ermes va costantemente a caccia di nuove potenziali forme di aggressione. Si pensi al diffondersi del cryptokacking: il furto di energia ai dispositivi e in particolare ai potenti server delle aziende con effetti di perdita di operatività fino al 95%. Un’altra potenziale falla nei sistemi aziendali complessi è rappresentato da versioni dei browser non sempre aggiornate. Basta un computer con un sistema operativo “non in dominio”, non aggiornato per mettere a rischio l’intera rete aziendale. Ermes protegge anche da rischi di extention vetting, aggressioni cioè che passano attraverso estensioni del browser.

In pratica il sistema Ermes utilizza l’AI (Artificial Intelligence) per proteggere i dispositivi aziendali da attacchi di nuova generazione che passano attraverso i browser e non possono essere affrontati dagli strumenti esistenti.
Un vantaggio competitivo che si aggiunge alla protezione della navigazione che supera del 90% i filtri sul mercato; e alla tutela della privacy del dipendente che viene messo al riparo da tracciamento e profilazione.

L’eliminazione di pubblicità accelera di almeno 4 volte il browser e permette un risparmio del 30% di banda utilizzata. In pratica un risparmio di 36h/anno di navigazione.




## ERMES SHARK PHISHING

Il sistema di difesa e prevenzione dagli attacchi informatici brevettato da Ermes è stato scelto da aziende come Reale Mutua Assicurazioni, Lavazza, Carrefour, Unione Industriali Torino, Cuki.
Viene attivato con un'installazione plug&play veloce su singoli dispositivi e con un periodo di prova che consiste in una prima fase di 30 giorni di ricognizione delle potenziali fonti di attacchi e malware; un'area-test di 15 gg con il sistema Ermes attivato e una presentazione dei risultati al 50° giorno.
L'attivazione prevede un costo per licenza/annua-utente che copre due dispositivi.

Fast&Safe è una soluzione più specifica per le PMI che coniuga la protezione da Spear Phishing e in generale dai più elaborati attacchi informatici all'aumento delle prestazioni dei singoli dispositivi coperti.
La velocità di navigazione e il risparmio in termini di banda rappresentano in tal senso il maggiore plus per le piccole e medie aziende.