ERMES®
Intelligent Anti Phishing

UNDETECTED CYBER THREATS

Analisi di attacchi informatici che eludono i sistemi di protezione tradizionali

Gennaio 2021

WHITE PAPER ABSTRACT

INTRODUZIONE

Il cyber crime sta diventando una minaccia sempre più evidente, soprattutto in Europa e negli Stati Uniti.

Il COVID-19 ha inasprito ulteriormente la situazione e il risultato è la **crescita esponenziale di attacchi informatici** che, sfruttando il progresso tecnologico e l'evoluzione del contesto lavorativo, eludono i sistemi di sicurezza tradizionali.

IL CRESCENTE CONFLITTO TRA AZIENDE ED HACKERS

Le aziende combattono ogni giorno una dura battaglia contro i criminali informatici, e i numeri della stessa non possono lasciare indifferenti i principali attori coinvolti. CISO, IT manager, CTO e fornitori di servizi IT, infatti, molto spesso legano la loro carriera all'efficacia dei sistemi di protezione da loro implementati.

$6000 Miliardi

I danni causati dal cyber crime previsti nel 2021[1]

$170 Miliardi

La spesa in cybersecurity prevista nel 2022 per combattere gli attacchi dei cyber criminali[2]

[1]: *Cybersecurity Ventures*
[2]: *Gartner*

L'EVOLVERSI DEL CYBERCRIME

Con l'obiettivo di eludere i sistemi di protezione aziendale, i cyber criminali sfruttano l'anello debole della catena di sicurezza, introducendosi all'interno dei sistemi aziendali attraverso l'inconsapevole aiuto dei singoli utenti.

L'utilizzo di informazioni esposte sul web permette infatti di nascondere minacce informatiche dietro a dei contenuti apparentemente affidabili.

Molte di queste minacce e attacchi rimangono invisibili ai tradizionali sistemi di sicurezza aziendale, che non sono in grado di rilevare le minacce che sfruttano l'evolversi del contesto contemporaneo.

LO STUDIO DI ERMES

Il campione

13
AZIENDE

361
DIPENDENTI

+86M
CONNESSIONI ANALIZZATE

Attraverso uno studio condotto nel 2020, Ermes ha voluto **misurare l'efficacia delle soluzioni di sicurezza tradizionali nel prevenire e proteggere dipendenti ed aziende dalle sofisticate tipologie di attacchi informatici che colpiscono durante la navigazione**.

Installando il proprio software su dispositivi aziendali quali PC, tablet e cellulari, è stato analizzato un campione di aziende di varie dimensioni ed operanti in diversi settori, tutte coperte dai principali strumenti di sicurezza.

I RISULTATI

il **91,97%** degli impiegati coinvolti nello studio **ha esposto i propri dati** a sistemi di web tracking durante la navigazione.

+139K titoli di pagina e **+33K frasi di ricerca** sono stati esposti sul web.

+4 siti pericolosi raggiunti da ciascun dipendente
ogni anno, senza che queste connessioni vengano precluse dai sistemi di sicurezza.

il **93,2%** **dei tentativi di raggiungere siti considerati pericolosi non sono stati inibiti dai sistemi di sicurezza tradizionali.**

OSSERVAZIONI CONCLUSIVE

Il volume di informazioni personali che gli impiegati espongono durante la navigazione è estremamente alto, configurando il rischio che tali informazioni possano essere usate per creare attacchi informatici sofisticati.

Ancor più critico è stato riscontrare che **le soluzioni di sicurezza non siano state in grado di prevenire gli attacchi avvenuti durante la navigazione web**. Tali problematiche sono emerse in maniera omogenea tra le diverse realtà analizzate, indipendentemente dalle dimensioni, settore o sistema di protezione in essere.

CHI SIAMO

ERMES®
Intelligent Anti Phishing

Realtà italiana innovatrice nell'ambito della sicurezza informatica, proteggiamo impiegati ed aziende da quelle minacce web che eludono i sistemi di sicurezza tradizionali e colpiscono fortemente l'odierna compagine lavorativa. Attraverso l'utilizzo di una tecnologia proprietaria all'avanguardia, basata su Intelligenza Artificiale e Deep Learning, la soluzione di Ermes ha già protetto +30 Mila utenti, bloccando oltre 360 Miliardi di connessioni pericolose.