

# L'evoluzione della sicurezza di rete

## Breve storia degli attacchi informatici degli ultimi 35 anni

Sebbene oggi i nostri perimetri possano apparire diversi, minacce sempre più gravi, attacchi crescenti e la natura complessa del mondo interconnesso sono tutti catalizzatori che impongono il ricorso a un approccio più flessibile e affidabile alla protezione di risorse, persone e dati.

1986



Si diffonde su MS-DOS il primo virus informatico, **Brain**

1987

**Virus Vienna** neutralizzato "In The Wild" (ITW)

1987

Compare il primo file virus provvisto di auto-crittografia, **Cascade**



1994



Nasce il firewall a livello di applicazione

1991

Primo firewall che include gateway applicazione

1988

Primo worm informatico distribuito tramite Internet, il **worm Morris**



1995

**WM.Concept** è il primo virus diffuso tramite Microsoft Word

1997

Sviluppato e pubblicato il primo software per il controllo del traffico web

1998

Rilascio di **Snort**, sistema IDS (Intrusion Detection System) open source



2008

**Conficker** infetta da 9 a 15 milioni di sistemi Microsoft

2006

Concetto di evasione presentato alla conferenza **Black Hat**

2000

Scoperto il primo attacco Denial-of-Service (**DoS**)

2009

Introdotta il clustering nativo per elevata disponibilità e prestazioni

2012

Introdotta la sicurezza basata su software; la tecnologia blade diventa obsoleta

2012

Introdotta lo strumento **Evader**



2015

Un errore di configurazione di un database espone i dati di 191 milioni di elettori negli Stati Uniti

2013

Un attacco hacker contro i server **Target** compromette i dati di ~70 - 110 milioni di clienti

2013

Una violazione della rete di **Yahoo** causa la compromissione di 3 miliardi di utenti

2016

Nasce Forcepoint, dall'integrazione di Websense, Stonesoft, Sidewinder e altre soluzioni di sicurezza Raytheon

2016

Rilasciate le prime integrazioni di prodotti cloud nativi

2016

Prima segnalazione di **TrickBot**, un trojan informatico che attacca Microsoft Windows

2017

Forcepoint X-Labs individua una **campagna di TrickBot sferrata contro le criptovalute**

2017

Il ransomware **WannaCry** attacca Microsoft Windows in tutto il mondo, colpendo 230.000 computer in un giorno

2018

**Under Armour** svela che un attacco hacker è penetrato nel database di backend dell'app MyFitnessPal

2018

Forcepoint X-Labs **registra l'evoluzione di Emotet**, un trojan bancario poi trasformatosi in piattaforma di propagazione di malware

2019

La borsa neozelandese è costretta a chiudere per ripetuti attacchi DDoS

2020

Prima scoperta della violazione della catena di fornitura software di **Solarwinds**

2020

Forcepoint presenta le **integrazioni** per rispondere alle esigenze delle moderne infrastrutture ibride

2019

Il ransomware **LockerGoga** colpisce un produttore di alluminio norvegese

2020

**Robinhood** svela la violazione di quasi 2.000 account

2021

Un attacco ransomware sferrato contro **JBS Foods** causa la chiusura di 13 stabilimenti di lavorazione della carne negli Stati Uniti

2021

**Colonial Pipeline** viene attaccata tramite la violazione di una password VPN e lascia a secco di carburante la costa est degli Stati Uniti

2021

**Forcepoint** acquisisce CyberInc, Deep Secure e Bitglass

2021

La violazione dei dati locali di **Microsoft Exchange Server** compromette migliaia di vittime ignare

2021

L'attacco ransomware alla catena di fornitura di **Kaseya** paralizza 1.500 organizzazioni

**Proteggi i tuoi asset. Metti al sicuro il tuo perimetro.**

Scopri di più su [Forcepoint Next-Gen Firewall](#)

### Informazioni su Forcepoint

Forcepoint è l'azienda leader nel settore della sicurezza informatica per la protezione degli utenti e dei dati. La sua missione è proteggere le aziende e guidarne la crescita e la trasformazione digitale. Le soluzioni human-centric di Forcepoint si adattano in tempo reale alle modalità di interazione tra persone e dati, consentono un accesso sicuro e, allo stesso tempo, permettono ai dipendenti di creare valore. Dalla sua sede di Austin, Texas, Forcepoint crea ambienti sicuri e affidabili per migliaia di clienti in tutto il mondo.