ADVNET | ADVANCED THINKING

Vincere la guerra ai Ransomware e proteggere i propri dati

L'approccio Advnet

IMMUTABILITA'

“La nostra visione al problema è tesa ad affiancare e aiutare i nostri clienti, portando una mentalità nuova, focalizzata sulla cultura aziendale della protezione del dato, indipendentemente dalla scelta di avere i propri dati in azienda o di adottare una strategia cloud o Hybrid. Introducendo soluzioni innovative, Advnet permette di rendere i propri clienti resilienti alle cyber-minacce, anche a fronte di inevitabili mutazioni future di questa tipologia di attacchi, sempre più raffinati.”

Andrea Cappozzo
IT Innovation Architect, Advnet

La minaccia Ransomware

Secondo il rapporto annuale IOCTA 2021 (Internet Organized Crime Threat Asessment), presentato da EUROPOL lo scorso ottobre, il RANSOMWARE rimane la principale minaccia informatica del 2021 e lo sarà anche per il 2022.

Nonostante gli attacchi siano in sostanziale calo e declino, per una maggiore consapevolezza delle vittime, un incremento dell'uso di dispositivi mobili e la maggior difficoltà di individuare vulnerabilità significative nei sistemi, il ransomware continua a mantenere la sua posizione al top come principale minaccia informatica a livello mondiale.

Il Ransomware rimane sempre un grande business. Utilizzare malware per cifrare files e computers, rendere impossibile l'accesso ai dati se non a fronte del pagamento di un riscatto, può avere impatti enormi per le aziende, sia del settore privato che nel pubblico.

Ciò che il rapporto IOCTA mostra chiaramente è uno shift degli attacchi verso targets più precisi il cui business o i cui dati rappresentino un valore maggiore per l'attaccante.

Le implicazioni per le aziende colpite possono essere enormi: non soltanto la perdita dei dati, ma anche sanzioni regolatorie a seguito di un cyber-attack (vedi la normativa GDPR).

Ma non solo.

Danni di reputazione e immagine con i propri clienti e perdita di fiducia degli stessi possono essere ancora più gravi rispetto al valore stesso dei dati compromessi.

"L'approccio di Advnet è da sempre a 360° rispetto alla minaccia Ransomware."

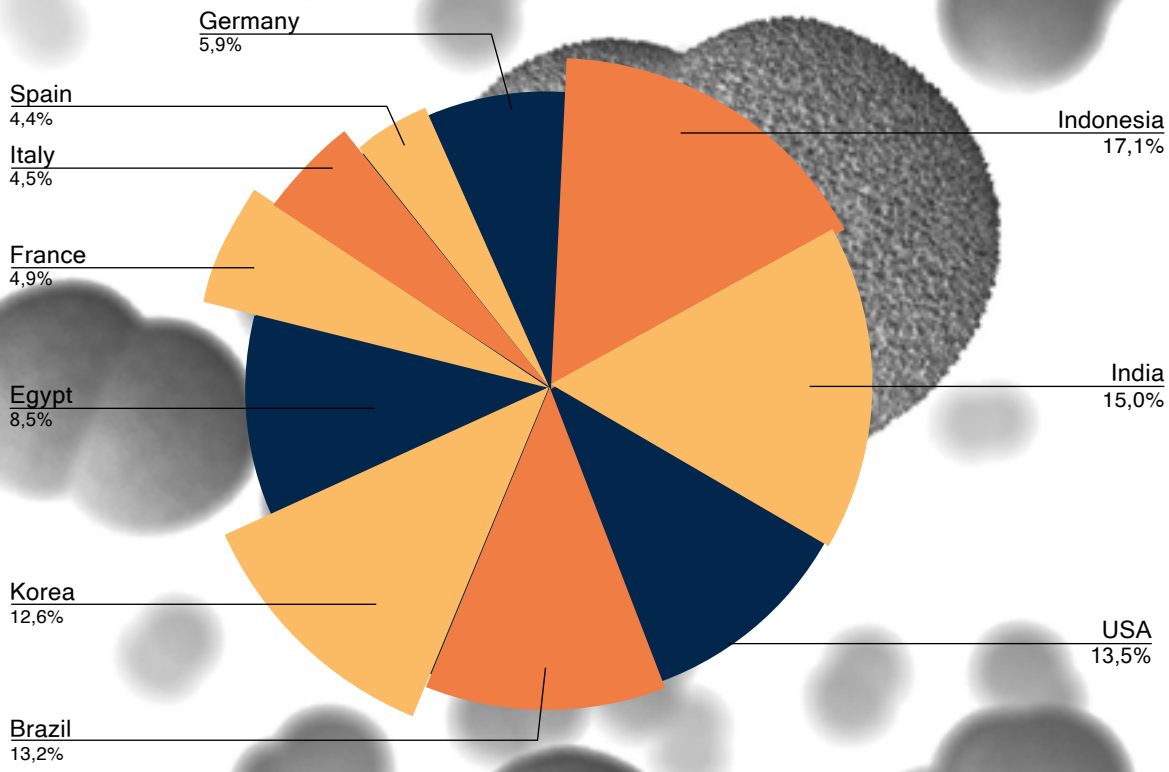
La visione Advnet

... focalizzarsi infatti soltanto su alcuni aspetti, come ad esempio utilizzare engine antivirus aggiornati, efficienti e moderni, è uno degli aspetti della soluzione, un tampone temporaneo, ma di certo non la soluzione stessa definitiva al problema dato che gli attacchi si fanno sempre più sofisticati ed intelligenti.

Gli strumenti principali di veicolo delle infezioni rimangono gli stessi degli ultimi anni: mail di phishing e vulnerabilità del protocollo RDP (Remote Desktop Protocol) per le connessioni remote ai sistemi Windows.

Quest'ultima particolare vulnerabilità permette all'attaccante di penetrare un sistema aziendale senza richiedere interazioni con la vittima o azioni dell'utente e gli permette di eseguire del codice che compromette l'integrità della macchina stessa fino ad ottenerne il controllo completo.

I malware iniettati cercano le vulnerabilità presenti e una volta scovate compromettono il sistema. A questo punto l'attaccante gode della libertà e del tempo per poter studiare con calma e senza troppe preoccupazioni l'architettura IT della potenziale vittima.



L'Italia non è ovviamente esente dalla minaccia, come molti casi hanno dimostrato negli ultimi anni.
Il nostro paese rappresenta infatti il 4.5% degli attacchi globali ed il trend è in crescita.

La domanda successiva, naturale, è: come le nostre aziende possono difendere il proprio business da questa minaccia globale?

Ciò che Advnet ha osservato direttamente sul campo, in questi anni di lotta al cyber crimine, è la tendenza nuova a non colpire indiscriminatamente l'infrastruttura client-server per produrre il maggior danno possibile alla vittima, ma piuttosto agire per steps graduali cercando dapprima di effettuare una escalation dei privilegi e venire in possesso di credenziali amministrative, chiavi di volta per accedere a tutti i sistemi informatici aziendali.

Successivamente colpire in modo preciso l'infrastruttura di Backup e Disaster Recovery e renderla inutilizzabile.

E solo allora colpire i dati e sistemi aziendali, rendendo così la richiesta di riscatto la sola via per la vittima per recuperare i propri dati perduti.

KEY WORD
#IMMUTABILE

agg. [dal lat. immutabĭlis].
Che non muta o non può mutare, quindi fisso, stabile, costante, sempre uguale, detto in genere di cose astratte: l'i. destino; decisione, proposito, risoluzione i.; leggi, regole i.; con i. volontà; con i. affetto, devozione.

Nel prossimo **WhitePaper I 02** parleremo di "Best Practices per una azienda resiliente"

In **WhitePaper I 03** introdurremo il concetto di **IMMUTABILITA'.** In questo documento proporremo le soluzioni studiate per i nostri clienti.

sommario
IMMUTABILITA'

ADVNET ADVANCED THINKING

Advnet s.r.l.
Via Marco Corner, 19/21
36016 Thiene (VI) Italy

Tel 0445 371093
Fax 0445 371094

www.advnet.it
info@advnet.it