Il ransomware scala le gerarchie aziendali: i manager sono i bersagli principali

zscaler™

ATTIVITÀ DI RICERCA DI THREATLABZ

I report sugli attacchi ransomware si concentrano spesso sulle aziende che hanno subito violazioni, i dati rubati, gli strumenti malware e i pagamenti dei riscatti. Tuttavia, i dati disponibili su chi viene realmente preso di mira all'interno delle organizzazioni sono scarsi. Una nuova ricerca di ThreatLabz colma questa lacuna ed esamina il lato umano degli attacchi ransomware, inclusi i ruoli e le funzioni aziendali più rappresentati tra le vittime. I risultati hanno rivelato che gli operatori di ransomware non prendono di mira individui a caso all'interno delle organizzazioni, ma si concentrano su dipendenti specifici con ruoli privilegiati e funzioni critiche per l'azienda, al fine di aumentare la possibilità di infiltrarsi, muoversi all'interno della rete, esfiltrare informazioni sensibili e monetizzare l'accesso.

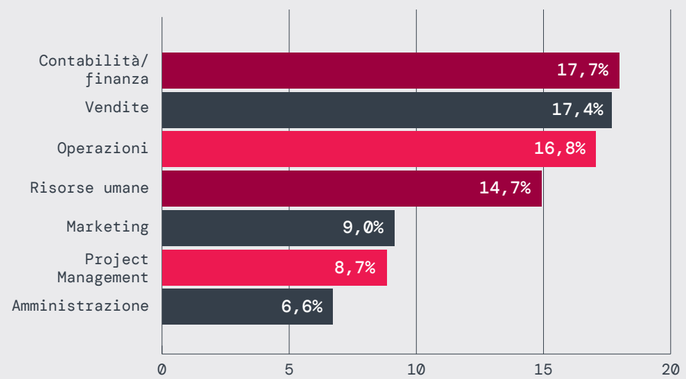
Metodologia

Nell'arco di un mese, ThreatLabz ha identificato 351 vittime compromesse in 334 organizzazioni per mano di un gruppo di hacker specializzato nell'ottenimento dell'accesso iniziale per rubare grandi quantità di dati aziendali e cifrare selettivamente i sistemi critici.

I risultati principali

62% delle vittime ricopriva la carica di manager o superiore

SONO STATI PRESI DI MIRA I RUOLI CRUCIALI PER L'ATTIVITÀ AZIENDALE

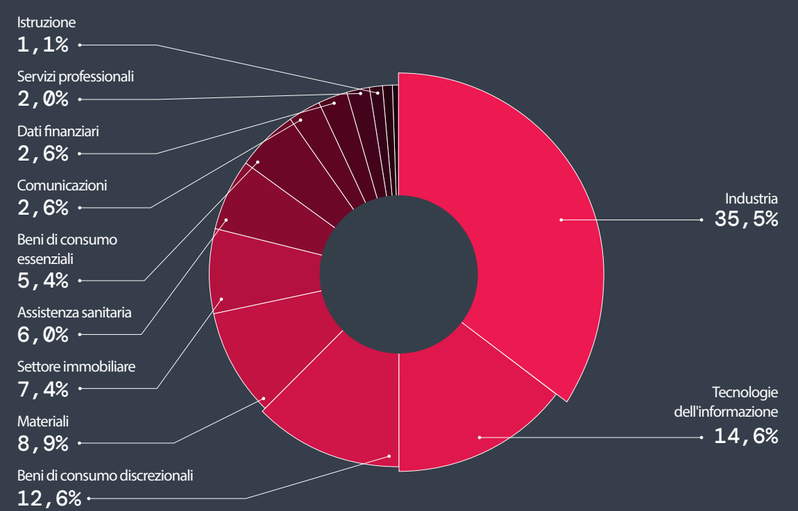


La generazione X ha rappresentato la **percentuale maggiore di vittime:**

44%

Età media: 46
Millennials: **33%**
Gen Z: **14%**
Baby Boomer: **9%**

50% delle vittime lavorava in aziende **industriali e informatiche**



4,6% delle aziende ha registrato la compromissione di più dipendenti

Panoramica delle vittime del ransomware

- Le vittime colpite da questo gruppo di hacker **ricoprivano perlopiù ruoli dirigenziali o di livello superiore**. Questo indica che gli aggressori prendono di mira i dipendenti che hanno un accesso privilegiato ai dati dei clienti, i registri finanziari, i contratti e i sistemi operativi.
- Oltre il 75% delle vittime apparteneva **a cinque aree aziendali:** contabilità/finanze, vendite, operazioni, risorse umane e marketing, in quest'ordine.
- Le vittime avevano un'età molto variabile, dai 23 ai 70 anni, ma **si concentravano soprattutto nella fascia tra i 40 e i 50 anni, con la generazione X** che rappresentava il 43,9% delle vittime.
- A livello dell'organizzazione, **il 50% delle aziende vittime apparteneva a soli due settori:** quello industriale (35,5%) e quello delle tecnologie dell'informazione (14,6%).
- Oltre dieci aziende hanno registrato **la compromissione di più dipendenti**.

Esempi di profili di vittime

Questi profili forniscono esempi concreti di vittime di ransomware e spiegano perché potrebbero essere prese di mira.

Manager delle vendite regionali

Settore: Industriale

Perché vengono presi di mira: accesso agli account dei clienti, alle offerte attive, ai contratti, ai prezzi e alle informazioni sui ricavi.

Responsabile della contabilità dei fornitori

Settore: Tecnologia dell'informazione

Perché vengono presi di mira: accesso a dettagli di pagamento, fatture, approvazioni finanziarie e registri dei fornitori

Property Manager

Settore: Immobiliare

Perché vengono presi di mira: accesso a contratti di locazione, fatture dei fornitori, contratti, dati dei clienti e informazioni finanziarie.

Senior Project Manager

Settore: Beni di consumo discrezionali

Perché vengono presi di mira: accesso al budget dei progetti, ai contratti con i fornitori e a file o documenti riservati.

Insegnamento per le aziende: proteggere gli utenti aziendali ad alto rischio

Questa campagna ribadisce una priorità fondamentale nella difesa contro i ransomware, ovvero la necessità di rafforzare i controlli sugli utenti e sui flussi di lavoro più vicini ai dati aziendali sensibili. Quando gli hacker prendono di mira i dipendenti che si occupano di vendite, finanze, contabilità o operazioni, un singolo account compromesso può creare un rischio per tutta l'azienda.

Gli aggressori sfruttano il senso di urgenza, si spacciano per personale IT e utilizzano strumenti familiari come Microsoft Teams e Quick Assist per conquistare la fiducia delle vittime. Da qui, il rischio aumenta rapidamente e può portare al furto di credenziali, l'accesso remoto, il movimento laterale, il furto di dati, la potenziale crittografia dei file e, infine, l'estorsione.

La prevenzione del ransomware non può fermarsi al rilevamento del malware. Bisogna inoltre tenere conto dei dipendenti il cui accesso, se compromesso, crea il rischio maggiore per l'azienda.

Per ridurre tale rischio, le imprese dovrebbero:

- Implementare la segmentazione tramite un'architettura zero trust per prevenire il movimento laterale e ridurre la superficie di attacco.
- Formare i dipendenti affinché verifichino le richieste provenienti dal "personale IT" utilizzando le informazioni presenti nella directory aziendale.
- Bloccare i messaggi istantanei e le chiamate esterne su piattaforme di collaborazione come Microsoft Teams e Slack.
- Applicare il principio del privilegio minimo per limitare il più possibile l'esposizione a sistemi e dati sensibili.
- Implementare una protezione dalle minacce inline basata sull'intelligenza artificiale e la sicurezza degli endpoint per rilevare e bloccare gli attacchi.
- Monitorare costantemente l'attività di utenti, dispositivi e applicazioni per individuare eventuali segni di compromissione.

X @ThreatLabz | Blog delle attività di ricerca sulla sicurezza di ThreatLabz

© 2026 Zscaler, Inc. Tutti i diritti riservati. Zscaler™ e gli altri marchi commerciali presenti su **zscaler.com/it/legal/trademarks** sono (I) marchi commerciali o marchi di servizio registrati o (II) marchi commerciali o marchi di servizio di Zscaler, Inc. negli Stati Uniti e/o in altri Paesi. Eventuali altri marchi commerciali appartengono ai rispettivi proprietari.

zscaler™ | Act Fast. Stay Secure.