Akamai

Stato di Internet
Volume 09 | Numero 04

Il ransomware in azione

Panoramica sull'area EMEA

Sommario

I principali risultati emersi dal rapporto

La panoramica sull'area EMEA è un documento integrativo del più ampio rapporto SOTI sul settore del ransomware dal titolo "Il ransomware in azione: l'evoluzione delle tecniche di sfruttamento delle vulnerabilità e l'obiettivo degli attacchi zero-day" (disponibile solo in inglese). All'interno di questo rapporto sono disponibili analisi dettagliate sulle tendenze, sulle metodologie e sulle tecniche di attacco utilizzate dai gruppi di ransomware, una descrizione delle fasi degli attacchi insieme a soluzioni e consigli utili per proteggere la vostra organizzazione, nonché le metodologie impiegate per condurre la nostra ricerca.

Panoramica

Il ransomware continua a creare scompiglio nelle organizzazioni e a mietere un maggior numero di vittime man mano che i criminali continuano ad evolvere e a cambiare le loro tecniche di attacco, ad introdurre nuovi metodi di estorsione, a trarre vantaggio da una superficie di attacco più ampia e a capitalizzare sui vincoli dei budget destinati alla sicurezza. L'impatto di queste pericolose tendenze si riflette nei gruppi di ransomware che dominano il panorama degli attacchi e nel loro crescente successo. Nell'area EMEA, un esempio di questo impatto è rappresentato da una crescita del 18% nel numero di vittime osservata tra il 4° trimestre del 2021 e lo stesso periodo del 2022, con un'impennata del 77% su base annua se si confronta il 1° trimestre del 2022 con lo stesso periodo del 2023.

In questa panoramica sull'area EMEA, condivideremo ulteriori informazioni su come migliorare i sistemi di difesa e la gestione dei rischi relativamente a questo crescente problema, tra cui:

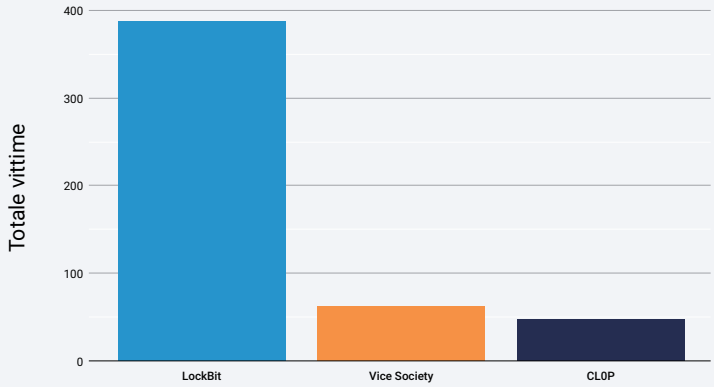
- Nel periodo compreso tra ottobre 2021 e maggio 2023, LockBit ha dominato la scena del ransomware con una maggiore presenza del gruppo CL0P che ha sfruttato le vulnerabilità esistenti in modo aggressivo. L'evoluzione delle tecniche di attacco, dal phishing ad un abuso sempre maggiore delle vulnerabilità zero-day e one-day, ha fatto registrare un aumento nel numero delle vittime.
- Coerentemente con i risultati emersi a livello globale, il settore manifatturiero è il mercato verticale con il maggior numero di aziende vittime di attacchi, seguito dai servizi alle imprese.
- La maggior parte delle vittime di ransomware è rappresentata da organizzazioni di piccole dimensioni con un fatturato inferiore a 50 milioni di dollari. Tuttavia, anche le aziende più grandi sono risultate a rischio di attacchi.

LockBit domina le attività dei gruppi di ransomware

Nonostante una maggiore consapevolezza del ransomware e l'abbondanza di strumenti e best practice disponibili per combattere questa minaccia, il numero di aziende nell'area EMEA che l'hanno subita è aumentato del 18% tra il 4° trimestre del 2021 e lo stesso periodo del 2022, facendo registrare un'impennata del 77% su base annua se si confronta il 1° trimestre del 2022 con lo stesso periodo del 2023. Coerentemente con i dati riportati nel nostro rapporto globale, tra il 1° ottobre 2021 e il 31 maggio 2023, il gruppo LockBit è stato responsabile della maggior parte degli attacchi, facendo registrare un 45% di attacchi nell'area EMEA. Tuttavia, nell'area EMEA, Vice Society ha rimpiazzato ALPHV come secondo gruppo più attivo, mentre il gruppo CL0P è ancora al terzo posto (EMEA - Figura 1).

EMEA: i primi 3 gruppi di ransomware per numero di vittime

1° ottobre 2021 - 31 maggio 2023



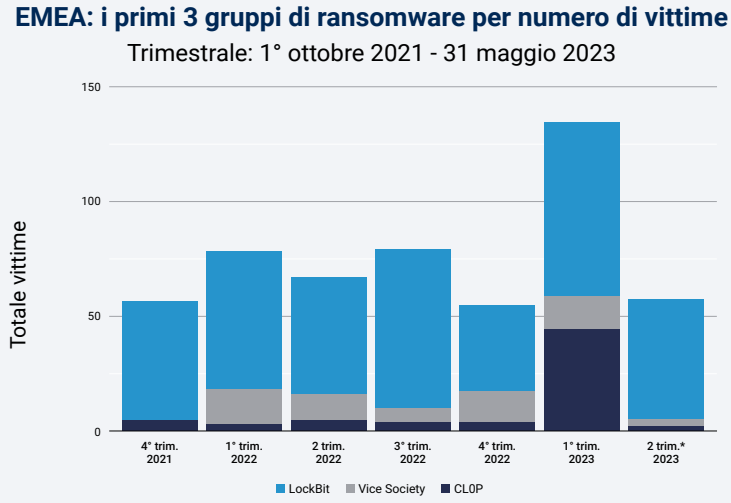
EMEA - Figura 1. La maggior parte delle organizzazioni che hanno subito attacchi di ransomware nell'area EMEA è stata colpita dai gruppi LockBit, Vice Society e CL0P

Analisi trimestrale

Se consideriamo il numero di aziende che hanno subito attacchi da parte di gruppi di ransomware (EMEA - Figura 2), LockBit rimane il gruppo prevalente, mentre la presenza costante di Vice Society va a braccetto con il settore dell'istruzione, che risulta uno dei principali settori presi di mira dal ransomware nell'area EMEA (come mostrato più avanti in Figura 3) in quanto Vice Society è un RaaS (Ransomware-as-a-Service) che colpisce in modo spropositato il settore educativo. Tuttavia, coerentemente con le tendenze sui dati globali, la presenza del gruppo CL0P sta crescendo nello scenario del ransomware nell'area EMEA e il suo picco raggiunto nel 1° trimestre del 2023 può essere attribuito allo sfruttamento da parte del gruppo di varie vulnerabilità zero-day come punto di

**Il 2° trimestre 2023 non è un intero trimestre perché viene considerato il periodo fino al 31 maggio 2023.*

accesso. L'evoluzione delle tecniche di attacco nello scorso semestre, dal phishing ad un abuso delle vulnerabilità sempre maggiore, ha fatto registrare un aumento nel numero delle vittime. Al momento della stesura di questo rapporto, erano disponibili solo dati parziali per il 2° trimestre del 2023*. Alla data del 31 maggio 2023, l'attività del gruppo CL0P è ritornata allo stesso livello che abbiamo registrato nel 2022. Anche se non possiamo stabilire in maniera definitiva i risultati del trimestre, è importante notare che a giugno 2023 CL0P ha pubblicato i nomi di altre aziende nell'area EMEA, che hanno subito lo sfruttamento della vulnerabilità MOVEit, quindi il numero di soggetti coinvolti è destinato probabilmente ad aumentare.

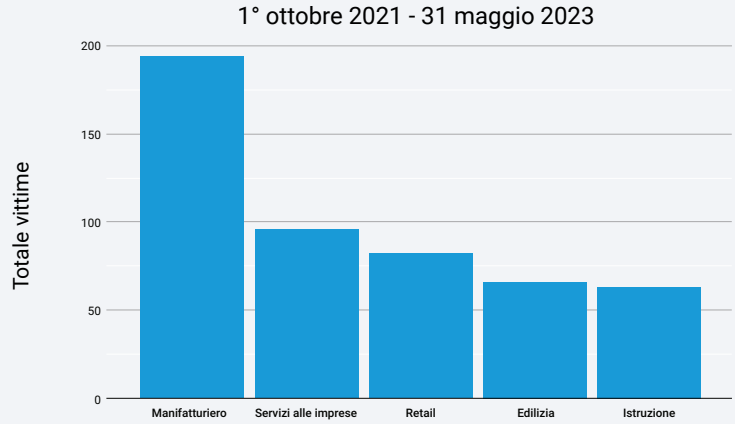


EMEA - Figura 2. Confronto trimestrale del numero di aziende vittime dei tre principali gruppi di ransomware nell'area EMEA: LockBit, Vice Society e CL0P

I principali settori a rischio

I cinque principali settori a rischio di attacchi ransomware nell'area EMEA sono il settore manifatturiero, i servizi alle imprese, il retail, l'edilizia e l'istruzione (EMEA - Figura 3). Si tratta, in realtà, di una tendenza globale e in linea con quanto riportato nel rapporto sul ransomware globale del 2022, in cui il settore manifatturiero e i servizi alle imprese si attestavano nelle prime due posizioni, subendo, in questo periodo, le minacce del gruppo di ransomware Conti. Dopo la scomparsa di Conti, LockBit ha colmato la lacuna lasciata dal gruppo. Abbiamo anche notato una significativa sovrapposizione con i primi cinque settori coinvolti nel nostro precedente rapporto DNS, L'autostrada degli attacchi: un esame approfondito del traffico DNS dannoso, in cui emerge un chiaro collegamento tra il traffico C2 (Command and Control) dannoso e gli attacchi di ransomware.

**Il 2° trimestre 2023 non è un intero trimestre perché viene considerato il periodo fino al 31 maggio 2023.*



EMEA - Figura 3. Il settore manifatturiero è il mercato verticale con il maggior numero di aziende che hanno subito attacchi di ransomware nell'area EMEA

È anche importante notare come LockBit sia il gruppo di ransomware prevalente in ciascuno dei primi quattro settori nell'area EMEA, rappresentando il 45,9% di attacchi nel settore manifatturiero, il 45,4% nei servizi alle imprese, il 45,1% nel retail e il 53,6% nell'edilizia. Fa eccezione il settore dell'istruzione: Vice Society è responsabile della maggior parte degli attacchi (36,5%), mentre LockBit fa registrare il 22,2% degli attacchi.

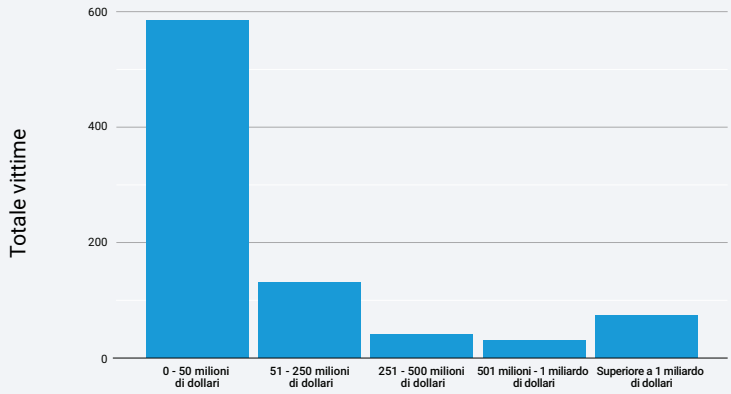
> Ogni organizzazione, indipendentemente dalle sue dimensioni o dal suo fatturato, è a rischio di attacchi di ransomware.

I gruppi di ransomware si focalizzano sul ROI

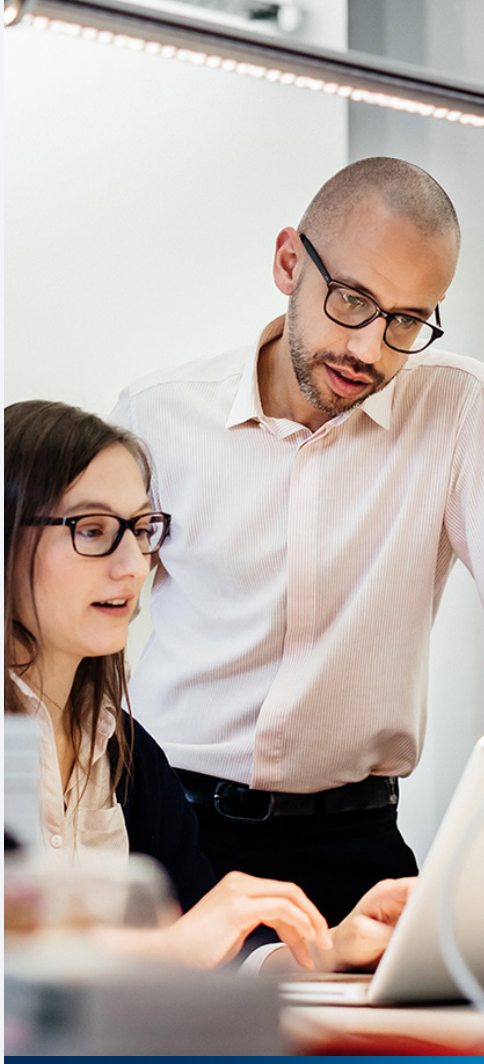
Ogni organizzazione, indipendentemente dalle sue dimensioni o dal suo fatturato, è a rischio di attacchi di ransomware. Tuttavia, rispecchiando la tendenza globale, dai dati emerge come i criminali riescano a sferrare attacchi riusciti nell'area EMEA contro le organizzazioni più piccole (EMEA - Figura 4), probabilmente perché queste aziende dispongono di limitate risorse di sicurezza per combattere i rischi legati al ransomware, il che le rende più vulnerabili e semplici da penetrare, oltre al fatto di avere la possibilità di pagare il riscatto richiesto. Tuttavia, anche le aziende più grandi sono a rischio di attacchi: come mostrano i risultati della ricerca, più elevato è il fatturato dell'organizzazione coinvolta, maggiore è il riscatto richiesto.

EMEA: numero di aziende vittime di gruppi di ransomware per fasce di fatturato

1° ottobre 2021 - 31 maggio 2023



EMEA - Figura 4. La maggior parte delle vittime di ransomware nell'area EMEA è rappresentata da organizzazioni con un fatturato inferiore a 50 milioni di dollari



Conclusioni della panoramica sull'area EMEA

Il ransomware continua a creare scompiglio nelle organizzazioni. I governi nazionali a livello globale e regionale stanno creando un fronte unico per contrastare questa minaccia e diffondere tecniche in grado di aiutare gli addetti alla sicurezza a proteggere le loro organizzazioni e a costruire un adeguato livello di resilienza. L'ENISA, l'agenzia dell'Unione europea per la cybersicurezza, ha emanato una nuova direttiva, la NIS2 (Network and Information Systems Directive), nell'intento di migliorare la cybersicurezza nell'Unione europea, incluse nuove attività come la creazione di un registro delle vulnerabilità AI di fuori dell'Unione europea, altri paesi stanno creando e applicando propri controlli, come la NCA (National Cybersecurity Authority) in Arabia Saudita.

Poiché le autorità di regolamentazione governative hanno messo in atto iniziative e policy per rafforzare gli standard in materia di cybersicurezza, è importante comprendere i requisiti di reportistica locali per includerli nelle proprie linee guida/piano di gestione delle crisi in modo da conoscere le opportunità disponibili per mitigare i rischi mediante un sistema di difesa multilivello.

Per maggiori informazioni, potete consultare il rapporto SOTI sul ransomware globale dal titolo "Il ransomware in azione: l'evoluzione delle tecniche di sfruttamento delle vulnerabilità e l'obiettivo degli attacchi zero-day".

Metodologia

I dati dei ransomware

I dati dei ransomware utilizzati in questo rapporto sono stati raccolti dai siti dannosi di circa 90 diversi gruppi di ransomware. Solitamente, questi gruppi pubblicano informazioni sui loro attacchi, come la data e l'ora, i nomi delle vittime e i domini presi di mira. È importante notare che queste informazioni sono soggette ai contenuti che ciascun gruppo di ransomware desidera pubblicizzare. La riuscita degli attacchi pubblicati non è stata inclusa in questa ricerca,

che si è, invece, focalizzata sulle vittime riportate dai criminali. Per ogni analisi, è stato misurato il numero di vittime specifiche all'interno di ciascun gruppo. I dati delle vittime sono stati combinati con i dettagli ottenuti da ZoomInfo per fornire ulteriori informazioni su ciascuna azienda che ha subito l'attacco, come l'ubicazione, la fascia di fatturato e il settore di appartenenza.

Tutti i dati si riferiscono ad un periodo di 20 mesi compreso tra il 1° ottobre 2021 e il 31 maggio 2023.

Riconoscimenti

Editoria e stesura

Ori David
Badette Tribbey
Charlotte Pelliccia
Lance Rhodes

Revisione e contributi di esperti del settore

Moshe Cohen
Shiran Guez
Ophir Harpaz
Reuben Koh
Richard Meeus
Steve Winterfeld
Maxim Zavodchik

Analisi dei dati

Chelsea Tuttle

Marketing ed editoria

Kimberly Gomez
Georgina Morales Hampe
Shivangi Sahu

Altri rapporti sullo stato di Internet - Security

Leggete i numeri precedenti e consultate le prossime uscite degli acclamati rapporti sullo stato di Internet - Security di Akamai sul sito **akamai.com/soti**

Ulteriori informazioni sulla ricerca delle minacce di Akamai

Tenetevi aggiornati con le ultime pubblicazioni: analisi dell'intelligence sulle minacce, rapporti sulla sicurezza e ricerche sulla cybersicurezza.
akamai.com/security-research

Dati Akamai ricavati da questo rapporto

Potete visualizzare i grafici e i diagrammi citati in questo rapporto in versioni di alta qualità. L'utilizzo e la consultazione di queste immagini sono forniti a scopo gratuito, purché Akamai venga debitamente citata come fonte e venga conservato il logo dell'azienda: **akamai.com/sotidata**

Ulteriori informazioni sulle soluzioni Akamai

Per ulteriori informazioni sulle soluzioni Akamai per i ransomware, visitate la nostra pagina sulle **soluzioni per la sicurezza**.