MANDIANT
ORA PARTE DI Google Cloud

Report speciale M-Trends 2023

Sintesi generale

La 14ª edizione del report M-Trends 2023 è disponibile su www.mandiant.com/m-trends

Con i numeri: i dati di M-Trends

Le informazioni fornite si basano sulle indagini di Mandiant Consulting condotte tra il 1° gennaio e il 31 dicembre 2022.

Quali sono le informazioni importanti?

- A livello globale, gli attacchi vengono rilevati più rapidamente, con miglioramenti riscontrati nelle Americhe e nelle regioni EMEA, ma non nella regione APAC.
- I fornitori di sistemi di sicurezza e altre fonti esterne notificano le compromissioni alle organizzazioni più spesso di quanto non facciano i team di sicurezza interni. Tuttavia, quando gli attacchi vengono rilevati dai team interni, il processo è più rapido rispetto a quando vengono notificati da una comunicazione esterna.
- Per ottenere accesso alle organizzazioni, gli aggressori sfruttano ciò che funziona meglio nelle diverse regioni: exploit nelle Americhe, phishing nell'area EMEA e compromissioni precedenti nella regione APAC.

Chiedi al tuo CISO

- Come misuriamo i nostri tempi di rilevamento e risposta e qual è il nostro tempo mediano dal rilevamento alla risposta e alla soluzione?
- Siamo preparati a rilevare e a rispondere al malware, agli exploit e ai vettori di infezione iniziale più comuni, come il phishing?
- Qual è la nostra procedura quando veniamo informati da una terza parte di una potenziale compromissione?
- Come siamo posizionati per garantire la mitigazione degli exploit per i sistemi con vulnerabilità note?

Invasione dell'Ucraina

Quali sono le informazioni importanti?

- Mandiant ha identificato un'ampia attività di spionaggio informatico, attacchi informatici dirompenti e distruttivi e operazioni informative che hanno preceduto e seguito l'invasione dell'Ucraina da parte della Russia il 24 febbraio 2022.
- Le operazioni russe hanno avuto un impatto sui sistemi di controllo industriale e sulle infrastrutture critiche e, in alcuni casi, sono state permesse dalle campagne condotte e dall'accesso ottenuto prima dell'invasione.
- L'invasione dell'Ucraina da parte della Russia ha dimostrato la potenziale sovrapposizione delle operazioni informatiche e della guerra cinetica come nuovo standard de facto.

Chiedi al tuo CISO

- Abbiamo adottato misure per rafforzare i nostri sistemi contro attacchi distruttivi e dirompenti?
- Quali sono stati i risultati del test più recente del nostro piano di backup e continuità operativa?
- Dovremmo utilizzare le informazioni sulle minacce per combattere le operazioni informative?

Le operazioni finanziarie della Corea del Nord

Quali sono le informazioni importanti?

- Oltre alle tradizionali missioni di raccolta di informazioni e agli attacchi dirompenti, nel 2022 gli operatori della Repubblica Popolare Democratica di Corea (RDPC) hanno mostrato un maggiore interesse per il furto e l'utilizzo della criptovaluta.
- Queste operazioni sono state altamente redditizie e probabilmente continueranno senza sosta per tutto il 2023.

Chiedi al tuo CISO

- Quanto siamo preparati ad affrontare le minacce finanziarie più rilevanti per la nostra organizzazione?

Spostamento dell'attenzione e tecniche non comuni

Quali sono le informazioni importanti?

- Gli aggressori con minori competenze tecniche stanno esercitando impatti enormi sulle organizzazioni.
- Le loro operazioni hanno provocato furti di dati, furto di proprietà intellettuale e danni significativi alla reputazione.
- Questi aggressori sembrano motivati dalla notorietà più che dal denaro o dallo spionaggio, hanno dimostrato intraprendenza e sono disposti a ricorrere a tangenti e persino al bullismo o alle minacce per raggiungere i loro obiettivi.

Chiedi al tuo CISO

- Come stiamo riducendo il rischio che la tecnica del social engineering e altre minacce simili raggiungano i nostri dipendenti?
- Quali sono i programmi di cui disponiamo per proteggere i nostri dipendenti, soprattutto i dirigenti e i dipendenti altamente visibili, da questi tipi di attacchi?
- Come reagiremmo se le informazioni proprietarie o le informazioni di identificazione personale dei clienti venissero rubate e utilizzate a scopo di estorsione contro di noi?
- Abbiamo una procedura per acquisire rapidamente criptovaluta in risposta a una minaccia di estorsione?

Focus sul cloud: caso di studio del red team

Quali sono le informazioni importanti?

- Le iniziative del red team aiutano le organizzazioni a valutare le capacità del loro programma di sicurezza rispetto a scenari di attacco reali e a migliorare i loro assetti di sicurezza.
- Mandiant ha mostrato a un'azienda di servizi pubblici come gli aggressori potevano accedere a risorse critiche del cloud e dell'ambiente tecnologico operativo.

Chiedi al tuo CISO

- Abbiamo una visibilità completa su come la nostra organizzazione stia utilizzando effettivamente il cloud?
- Stiamo controllando regolarmente le configurazioni errate che gli aggressori possono sfruttare?
- Stiamo testando le nostre implementazioni di architettura nel cloud?

Campagne ed eventi globali

Quali sono le informazioni importanti?

- Per proteggere meglio i clienti per tutto il 2022, il team Campagne ed eventi globali di Mandiant ha indagato sulle attività di spionaggio russo, sul ransomware e su vulnerabilità significative come la Log4Shell.
- Mandiant condivide informazioni e indicatori preziosi per aiutare i nostri clienti e la comunità a proteggersi da queste campagne.

Chiedi al tuo CISO

- Cosa stiamo facendo per monitorare e applicare le patch alle vulnerabilità della nostra rete?
- Come stiamo utilizzando le informazioni sulle minacce attuali per prendere decisioni più consapevoli?

APT42 - Risultati degni di nota

Quali sono le informazioni importanti?

- APT42 è un gruppo di minacce legato all'Iran che conduce attività di spionaggio utilizzando sofisticati attacchi di phishing e l'ingegneria sociale.
- L'attività di APT42 rappresenta una minaccia per i funzionari di politica estera, i commentatori e i giornalisti che lavorano su progetti correlati all'Iran, in particolare quelli di Stati Uniti, Regno Unito e Israele.

Chiedi al tuo CISO

- Cosa possono fare i nostri team di sicurezza, informatica e aziendali per proteggere tutti i dipendenti?
- In quale modo stiamo riducendo il rischio che le minacce di social engineering raggiungano i nostri dipendenti?
- Come possiamo sensibilizzare i nostri dipendenti nei confronti del phishing e di altri tentativi di ingegneria sociale?

Per saperne di più, visita la pagina www.mandiant.com/m-trends

Mandiant

11951 Freedom Dr, 6th Fl, Reston,
VA 20190 Stati Uniti d'America
+1.703.935.1700
+1.833.3MANDIANT (362.6342)
info@mandiant.com

Informazioni su Mandiant

Mandiant è nota per essere leader nel campo della cyber defence. Fornisce informazioni sulle minacce ed eroga servizi di risposta agli incidenti. Forte di decenni di esperienza in prima linea, Mandiant aiuta le aziende a sviluppare maggiore sicurezza nella difesa e nella risposta alle minacce informatiche. Mandiant fa ora parte di Google Cloud.

MANDIANT
ORA PARTE DI Google Cloud