GUIDA PER PMI · L'EVOLUZIONE DI WAZUH

Dark Web Monitoring per PMI

Scopri se le credenziali della tua azienda sono già in vendita, prima che lo faccia qualcun altro.

> Una guida operativa per chi gestisce una PMI: come funziona il furto silenzioso di identità, dove finiscono le password rubate, e come trasformare un'esposizione scoperta in tempo in un incidente evitato.

IN QUESTA GUIDA

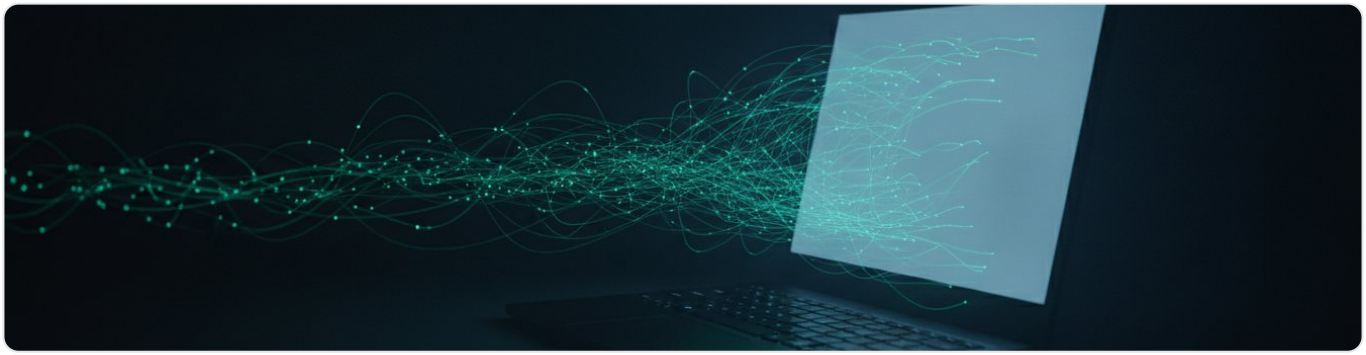
ArcaSafe S.r.l. · Partner Wazuh · Azienda certificata ISO/IEC 27001 e ISO 9001
SOC gestito on-prem con tecnici certificati · Cybersecurity, NIS2 & GDPR

> Le credenziali dei tuoi dipendenti valgono più di quanto pensi, e forse sono già in vendita. Questo ebook spiega, senza allarmismi, come funziona il furto silenzioso di identità, dove finiscono le password rubate e come una PMI può accorgersene prima del danno. Fatti, meccanismi e un playbook operativo: niente fuffa.

CAPITOLO 01

⚠ Infostealer, il furto silenzioso

L'infostealer è la minaccia più sottovalutata del panorama attuale, proprio perché non fa rumore. A differenza del ransomware, che blocca i file e chiede un riscatto in modo plateale, l'infostealer entra, copia e se ne va. Nel giro di pochi secondi svuota tutto ciò che il browser ha memorizzato: password salvate, dati delle carte, cronologia, autofill. Poi passa alla parte più preziosa, i cookie di sessione.



L'infostealer svuota il browser in pochi secondi: password, carte, cronologia e cookie di sessione.

Qui sta il punto che quasi nessuno spiega ai propri utenti. Il cookie di sessione è il "biglietto" che il sito rilascia dopo che ti sei autenticato: finché è valido, il servizio ti riconosce senza richiedere di nuovo la password né il secondo fattore. Chi ruba quel cookie e lo importa nel proprio browser eredita la tua sessione già aperta. Risultato: l'MFA viene semplicemente aggirato, perché l'attaccante non deve autenticarsi, gli basta riutilizzare un accesso già avvenuto.

I vettori di infezione sono banali e quotidiani. Software "craccato" e keygen, falsi installer di programmi noti, estensioni fasulle, allegati e link di phishing, pubblicità malevola sui motori di ricerca. Famiglie come RedLine, Lumma, Vidar o StealC si comprano a poche decine di euro e non richiedono competenze avanzate. Un solo click su un dispositivo, e l'intero "portachiavi" di quell'utente finisce nelle mani sbagliate. Per una PMI il rischio si moltiplica con lo smart working e i dispositivi personali: il portatile di casa del collaboratore non ha l'EDR aziendale né le stesse policy, ma su quel browser c'è la password della VPN, del gestionale, della posta Microsoft 365.

Il tratto più insidioso è il silenzio. L'infezione non genera un incidente evidente: nessun file cifrato, nessun riscatto, nessun alert. Le credenziali vengono impacchettate in un "log" del dispositivo e spedite all'operato-

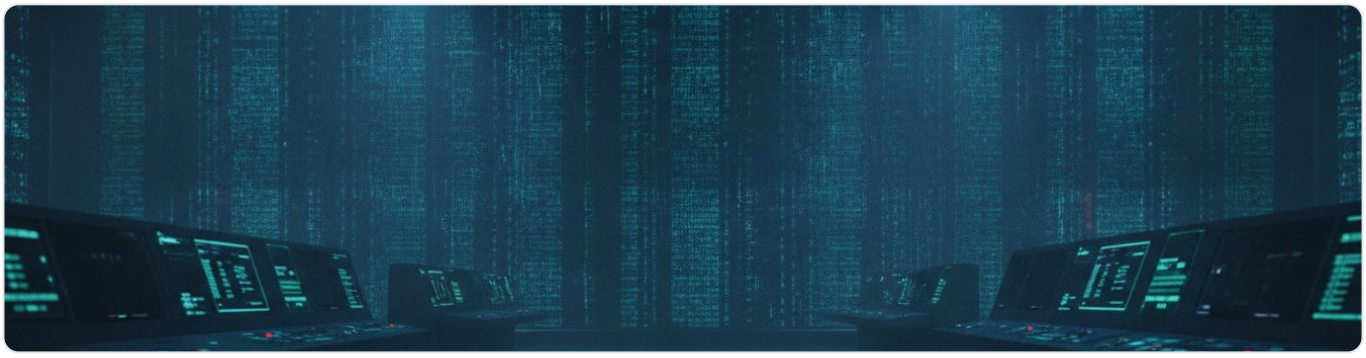
re, che le rivende. Spesso passano mesi prima che qualcuno colleghi un accesso anomalo a quel furto iniziale. In termini NIS2, è esattamente il tipo di evento che dovresti rilevare e notificare — ma che senza monitoraggio dedicato resta invisibile.

> **L'MFA non basta da solo**
>
> Chi ruba un cookie di sessione eredita l'accesso già autenticato: non deve autenticarsi, gli basta riutilizzarlo.

CAPITOLO 02

Dove finiscono le tue password

Una credenziale rubata non resta ferma: entra in una filiera. Capire questa filiera è ciò che distingue chi reagisce in tempo da chi scopre tutto a danno avvenuto. Il primo canale è il breach dump: l'archivio che emerge quando un servizio online viene violato. Milioni di coppie email-password finiscono in file scaricabili, spesso pubblicati per notorietà o per alimentare il mercato. Se un tuo dipendente ha usato la mail aziendale per registrarsi a un forum, un e-commerce o un tool poi violato, quella password è nel dump, insieme al dominio della tua azienda.



Breach dump, log di infostealer e combolist: la filiera commerciale della credenziale rubata.

Il secondo canale, oggi il più pericoloso, è il log dell'infostealer. Qui non c'è un singolo servizio violato: c'è un intero dispositivo svuotato. Un log contiene decine o centinaia di credenziali in chiaro, i cookie di sessione, l'indirizzo IP, il sistema operativo, persino gli screenshot. Questi log si vendono su marketplace e canali Telegram, singolarmente o in abbonamento. Il terzo è la combolist: liste enormi di username e password aggregate da più fonti, ripulite e ordinate per essere date in pasto agli strumenti di credential stuffing. Con una combolist e un po' di automazione, un attaccante prova le stesse coppie su decine di servizi, contando su un fatto statistico: le persone riusano le password.

Il mercato che muove questi dati è maturo e commerciale. Non parliamo di hacker incappucciati, ma di venditori con listini, recensioni e assistenza clienti. Un accesso a un pannello aziendale può costare pochi euro; le credenziali di un amministratore, molto di più. La merce è cercabile: si filtra per dominio, per servizio, per Paese.

Il dettaglio che pesa di più sulla difesa è il tempo. Tra il furto e lo sfruttamento passano frequentemente mesi. In quella finestra la credenziale viene rivenduta più volte, cambia mani, si diffonde. Per te significa due cose. La prima: probabilmente qualcosa di tuo è già lì fuori, adesso. La seconda, più utile: se riesci a intercettare la comparsa di un tuo dominio in un dump o in un log quando appare, hai il tempo di agire prima che qualcuno provi davvero quelle chiavi. È esattamente lo spazio che il monitoraggio dark web va a coprire.

> ✓ **Il tempo è la tua finestra**
>
> Tra il furto e lo sfruttamento passano spesso mesi: se intercetti la comparsa del tuo dominio quando appare, agisci prima che qualcuno provi quelle chiavi.

CAPITOLO 03

Umbra spiegato

Umbra è il modulo di Identity Risk & Dark Web Monitoring di Wazuh. In una frase: sorveglia i tuoi domini contro infostealer, breach dump e combolist, cercandoli live, e ti avvisa quando compare qualcosa che ti riguarda. Non è un report annuale né una scansione una tantum: è vigilanza continua sull'identità digitale della tua azienda.

Vigilanza continua su breach noti, log di infostealer e combolist, con HIBP, CloudSEK e Criminal IP.

Il funzionamento parte dal perimetro che conosci: i tuoi domini di posta e i servizi collegati. Umbra confronta in modo continuativo queste identità con le fonti dove circolano le credenziali rubate, integrando la base "classica" già consolidata di Wazuh: Have I Been Pwned (HIBP) per i breach noti e feed di threat intelligence come CloudSEK e Criminal IP. La ricerca è "live": quando un nuovo log o un nuovo dump emerge, la corrispondenza col tuo dominio viene rilevata a ridosso della comparsa, non con mesi di ritardo.

Ogni risultato è pensato per essere consultabile in sicurezza, e tre garanzie contano più di tutto. Primo: ogni record è datato, così sai a quando risale l'esposizione e puoi valutarne l'attualità. Secondo: ogni record porta la fonte, così distingui un breach di un servizio esterno da un log di infostealer che indica un dispositivo compromesso, che è ben più grave. Terzo, e decisivo: le password restano mascherate. Vedi che una credenziale è trapelata, ne conosci la data e l'origine, ma la console non ti espone il segreto in chiaro. Puoi

indagare senza trasformare lo strumento di difesa in un ulteriore rischio, e senza problemi di conservazione di dati sensibili.

Il tutto vive in una console operativa, non in un PDF statico. Gli avvisi compaiono direttamente in console e, con il piano Pro, vengono instradati dove lavori davvero: email, Slack o webhook verso i tuoi strumenti. Per una PMI il valore è concreto e duplice. Da un lato la conformità: NIS2 chiede di rilevare gli incidenti e gestirli, e una credenziale in vendita è un segnale precoce di incidente. Dall'altro l'operatività: sapere, con data e fonte, che l'account di un collega è esposto ti permette di chiuderlo prima che venga usato. Nel prossimo capitolo vediamo come Umbra trasforma questi record in una mappa d'impatto.

> ✓ **Consultabile in sicurezza**
>
> Ogni record è datato, porta la fonte e le password restano mascherate: indaghi senza trasformare la difesa in un nuovo rischio.

CAPITOLO 04

Il grafo dell'identità e il "blast radius"

Un elenco di credenziali trapelate è utile, ma da solo non racconta il rischio reale. La domanda che conta non è "quante password sono esposte", ma "cosa succede davvero se questa specifica credenziale viene usata". Umbra risponde con un grafo dell'identità (entity graph), che collega i puntini invece di lasciarti una lista da leggere a mano.

Dall'identità all'infezione al dossier del dispositivo: il grafo mostra il raggio d'impatto del riuso password.

Il percorso del grafo segue la catena logica di un compromesso. Si parte dall'identità, l'account o l'utente. Da lì si risale all'infezione, l'evento che ha generato l'esposizione. Quell'evento apre il dossier del dispositivo infetto: quale macchina è stata svuotata, quando, con quali caratteristiche. Dal dossier si dirama ogni credenziale rubata da quel dispositivo, non solo quella che stavi guardando. E qui arriva il concetto chiave: il password-reuse blast radius, il raggio d'impatto del riuso della password.

Il blast radius risponde a una domanda che tiene sveglio chi gestisce l'IT: se questa password è stata riusata, dove altro apre la stessa porta? Il grafo evidenzia i punti in cui la medesima credenziale, o una sua variante ovvia, ricompare su altri servizi e account. Una singola password rubata smette di essere un

problema isolato e mostra la sua vera estensione: la VPN, il gestionale, la posta, il portale del fornitore. Vedi il "raggio" del danno prima che l'attaccante lo percorra.

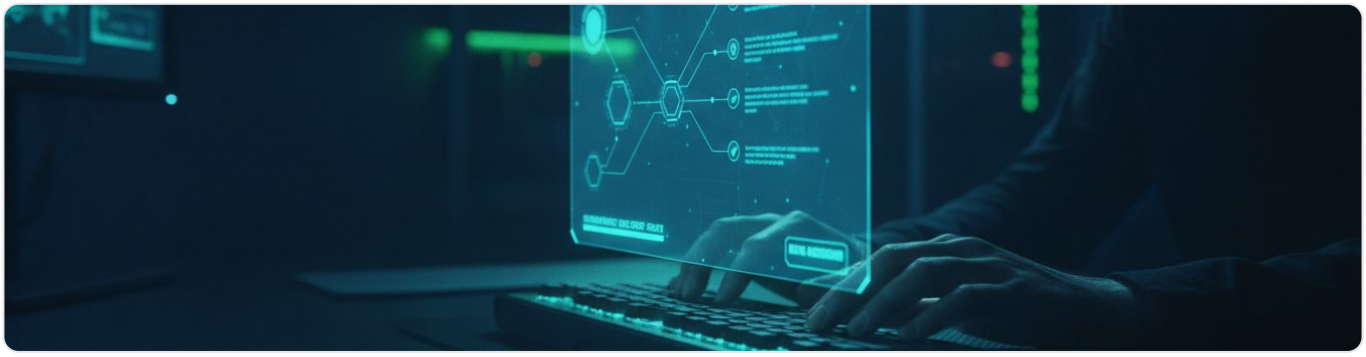
Il vantaggio operativo è enorme rispetto alla lista piatta. Con un elenco, resetti la credenziale segnalata e ti senti a posto, ma hai chiuso una finestra lasciando aperte le altre della stessa stanza. Col grafo capisci che quel dispositivo compromesso ha esposto anche altre chiavi, e che quell'utente riusa la stessa password su tre sistemi critici. La priorità cambia: non stai spegnendo un allarme, stai contenendo un'esposizione. C'è anche un beneficio di comunicazione: il grafo rende visibile, anche a chi non è tecnico, perché un singolo furto su un portatile di casa può mettere a rischio l'intera azienda. È lo strumento con cui giustifichi al management un reset massivo o l'attivazione dell'MFA ovunque: non un'opinione, ma una mappa. E nell'ottica NIS2, questa ricostruzione dell'impatto è esattamente ciò che serve per valutare la gravità di un incidente e documentarlo.

> ✓ **Non un allarme: un'esposizione**
>
> Col grafo non stai spegnendo il singolo alert, stai contenendo tutta l'esposizione che quel furto ha aperto.

CAPITOLO 05

Playbook: cosa fare quando una credenziale trapela

Un alert di esposizione non è un incidente da temere, è un vantaggio di tempo. La differenza la fa avere una sequenza pronta invece di improvvisare. Ecco un playbook essenziale, ordinato per priorità, adattabile a qualsiasi PMI.



Sei mosse ordinate per priorità: dalla qualifica del record alla valutazione della notifica NIS2.

- **1. Qualifica il record.** Prima di muoverti, leggi cosa ti dice Umbra. La data: è un'esposizione recente o vecchia di anni? La fonte: è un breach di un servizio esterno o un log di infostealer? Questa distinzione decide tutto. Un breach esterno riguarda una password; un log di infostealer significa che un dispositivo è stato compromesso, e il problema non è solo la credenziale, ma la macchina.
- **2. Resetta la password, subito e ovunque serva.** Cambia la credenziale esposta sull'account coinvolto. Poi usa il grafo e il blast radius: se quella password era riusata, resettala su ogni servizio in cui compare. Non fermarti al primo account.

- **3. Revoca le sessioni attive.** Il passo che quasi tutti dimenticano, ed è il più importante contro l'infostealer. Cambiare la password non invalida i cookie di sessione già rubati: l'attaccante resta dentro. Forza il logout globale, revoca token e sessioni su posta, VPN, gestionale e SaaS coinvolti. Solo così chiudi davvero la porta.
- **4. Verifica e rafforza l'MFA.** Controlla che il secondo fattore sia attivo sull'account e che nessun metodo sospetto sia stato aggiunto dall'attaccante. Ricorda che l'MFA non ferma il furto di sessione: va accompagnato da rotazione delle credenziali e revoca dei token, non usato come unica difesa.
- **5. Indaga il dispositivo.** Se la fonte è un log di infostealer, quella macchina va considerata compromessa fino a prova contraria. Isolala, esegui una scansione approfondita, valuta la bonifica o la reinstallazione. Non ha senso resettare le password se il malware è ancora lì a rubarle di nuovo.
- **6. Documenta e valuta la notifica.** Registra evento, impatto e azioni. In ottica NIS2, un'esposizione di credenziali può rientrare tra gli incidenti da gestire e, secondo i casi, da notificare: la ricostruzione con data, fonte e blast radius è la base della tua valutazione.

Qui il monitoraggio diventa risposta. Per le PMI che non hanno un SOC interno, ArcaSafe porta questo playbook dal rilevamento alla risposta gestita, integrando Umbra con Exigence per orchestrare i passi sopra in modo tracciato. Il monitoraggio ti dice cosa è successo; la risposta gestita fa in modo che venga chiuso.

> ✓ **Da alert a risposta gestita**
>
> ArcaSafe integra Umbra con Exigence: il monitoraggio dice cosa è successo, la risposta gestita fa in modo che venga chiuso.

Vuoi sapere se la tua azienda è già esposta?

Le credenziali dei tuoi dipendenti circolano in un mercato reale, e il tempo è l'unica risorsa che puoi ancora giocarti a tuo favore. Umbra ti dà visibilità continua, record datati e con fonte, password mascherate e un grafo che misura l'impatto vero del riuso. ArcaSafe ti aiuta a trasformare quella visibilità in azione, dal primo alert alla risposta gestita. Se vuoi sapere se la tua azienda è già esposta, una verifica iniziale della tua superficie di esposizione è il modo più semplice per partire: senza impegno, con dati veri.

Richiedi la verifica di esposizione →

Un click apre un'email già compilata: aggiungi i tuoi dati e invia. Oppure scrivici a commerciale@arcasafe.eu.

ArcaSafe S.r.l. · Via G. Segantini 5, 20825 Barlassina (MB) · CF e P.IVA 09546870966 · info@arcasafe.eu · PEC arcasafe@pec.it · arcasafe.eu · Partner Wazuh · ISO/IEC 27001 e ISO 9001