TREND MICRO | research

FUTURE/TENSE

TREND MICRO
SECURITY PREDICTIONS
FOR 2023

IN QUESTO REPORT

04 Ransomware

06 Tecnologia Cloud

08 Perimetro aziendale

10 Social Engineering

12 Blockchain

14 Vulnerabilità

16 Regolamenti industriali

18 Piattaforme di cybersecurity

20 Uno sguardo al 2023

Il 2023 potrebbe essere ricordato come l'anno in cui le linee di attacco cybercriminali sono state tracciate e ritracciate più volte, sullo sfondo di un panorama di minacce informatiche sospeso in una sorta di limbo: le aziende non sono più impegnate a cercare un punto fermo all'indomani dello sconvolgimento provocato dalla pandemia di Covid-19, ma nonostante si continui a parlare di "nuova normalità"[1] il mondo deve ancora arrivare al capolinea della pandemia. In questo contesto, la migrazione di massa degli asset aziendali verso gli ambienti digitali ha condotto a uno scenario sempre più complesso e stratificato, che offre un terreno fertile a cybercriminali capaci di sfruttare qualsiasi assenza di visibilità.

Quando le aziende espandono il loro business, e contestualmente si espongono alla crescente possibilità di essere attaccate, è essenziale che non trascurino l'elemento umano su entrambi i fronti di un cyberattacco. Molte realtà si sono ora riorganizzate intorno al lavoro ibrido, ma l'attenuazione dei confini tra lavoro in ufficio e lavoro da remoto impone ai team responsabili della sicurezza di abbandonare le strategie basate su specifiche soluzioni verticali convenzionali, in modo da poter coprire qualsiasi potenziale punto di ingresso che cybercriminali opportunisti potrebbero sfruttare. È indispensabile che il senior management mantenga una visione del quadro complessivo dell'infrastruttura digitale con un approccio alla sicurezza maggiormente olistico, ma le minacce destinate a emergere nel 2023 interesseranno una varietà di stakeholder, tra i quali team incaricati della sicurezza, legislatori e consumatori finali. Le aziende, o quantomeno i loro CFO, dovranno far fronte alle azioni dei governi decisi a estendere le normative relative alla sicurezza dei dati[2], nonché a una economia globale sull'orlo di una recessione[3], che renderà certamente più complicato finanziare le attività di prevenzione e la risposta alle minacce.

L'anno in corso sarà anche il periodo in cui aziende e utenti finali si prenderanno una pausa per riconsiderare quelle che, non molto tempo fa, sembravano essere innovazioni trasformative. Nel 2023 il fascino di metaverso e NFT (non-fungible tokens) potrebbe esaurirsi, ma la blockchain su cui si basano continuerà a essere un rifugio sicuro per i criminali informatici che, per loro natura, operano nell'ombra. La fiducia dell'opinione pubblica nei software open source resta ancora incerta ed è possibile un aumento degli attacchi volti a capitalizzare la quantità di errori destinati a emergere nel codice open source, mettendo in difficoltà gli sviluppatori. Analogamente, le vulnerabilità che hanno scosso il settore della cybersicurezza, come Log4Shell, possono appartenere ormai a un recente passato, ma continuano a creare preoccupazioni nei legislatori e nelle aziende che si interrogano sulle criticità future che, appunto, possono scaturire dal mondo open source.[4]

I cybercriminali in questo periodo di incertezza assumeranno un atteggiamento prudente e continueranno a sfruttare vecchi ma collaudati punti deboli, anziché correre grandi rischi che pure promettono grandi risultati. Rivolgeranno dunque le proprie attenzioni a protocolli e dispositivi obsoleti che le aziende hanno opportunamente iniziato a dismettere da tempo e li utilizzeranno come vettori di attacco innovativi. Le aziende dovrebbero prestare la massima attenzione alla riproposizione, sotto nuove vesti, di minacce già conosciute, dal momento che i cybercriminali torneranno a sfruttare tattiche consolidate. Le truffe sempre più raffinate basate sul social engineering e la dimostrata capacità dei soggetti dediti a tali reati di approfittarsi delle persone – l'anello debole di qualsiasi perimetro di sicurezza – si ripresenteranno anche nel 2023 per diventare ancora più efficaci con l'introduzione di nuove tecnologie come i deepfake. Sempre più malviventi si adatteranno poi a tecniche del passato per effettuare incursioni dirette nel cloud[5], al fine di assumere il controllo di tool e servizi legittimi da usare nel quadro di strategie di attacco complessive.

Altri cybercriminali, nel corso del 2023, continueranno a ottimizzare metodi già utilizzati, rendendoli sempre più professionali. Nel contempo, team di esperti di sicurezza e legislatori anticrimine riusciranno finalmente a costringere gli autori degli attacchi ransomware a rivedere il loro modo di agire e alcuni di essi potrebbero persino reinventarsi completamente, specializzandosi nell'estorsione di dati.

I criminali informatici potrebbero anche accontentarsi di lasciar trascorrere il 2023 aspettando la prossima ondata di cambiamenti, e nel frattempo le aziende possono considerare l'anno in corso come un'opportunità per gettare le basi di contromisure lungimiranti in grado di ridurre l'impatto dei cyberattacchi.

Questo report fornisce gli insight elaborati dagli esperti di sicurezza Trend Micro con l'obiettivo di supportare i decision makers a intraprendere scelte consapevoli e sviluppare una risposta strategica in grado di proteggere le aziende su più fronti.

/RANSOMWARE

I modelli di business del ransomware continueranno a cambiare e porteranno a sempre più casi di ricatto e furto di dati

Lo scenario del ransomware è destinato a grandi mutamenti nel 2023, dal momento che i responsabili di questi attacchi sembrano essere sotto assedio. Le forze dell'ordine internazionali hanno colpito questo genere di attività con la promessa di sanzioni, come nei casi di Evil Corp[6] e di Lazarus.[7] Incidenti come la neutralizzazione di REvil[8] e le fughe di informazioni attorno alla gang Conti[9] hanno inoltre mostrato al mondo che anche i più importanti provider RaaS (Ransomware-as-a-Service) non sono immuni dall'autodanneggiarsi. Pur prescindendo dall'effetto di questi colpi decisivi alla loro immagine, è probabile che le tattiche di doppia estorsione precedentemente diffuse nei circoli del ransomware non saranno più così devastanti come nel passato, in quanto chi deve difendersi continuerà ad aumentare la propria capacità di resilienza di fronte ad attacchi di questo tipo.

Questi fattori porteranno a cambiamenti notevoli tra gli operatori del ransomware, che dovranno scegliere se continuare a percorrere una strada già nota piuttosto che passare a un nuovo modello di business. Per rendere le proprie attività a prova di futuro dovranno ricercare nuovi sistemi per mettere a frutto le competenze acquisite. Le gang più organizzate, quelle che dispongono facilmente di interi team di hackers e per le quali la cifratura crittografica dei dati è solo una componente degli attacchi, saranno spinte a innovare, a loro volta, di fronte ai nuovi scenari. È probabile che alcune di esse elimineranno del tutto la parte di codifica crittografica, per concentrarsi invece sulla monetizzazione dei dati, sottraendo dai sistemi colpiti preziose informazioni rivendibili, come i numeri delle carte di credito.

Altre organizzazioni criminali seguiranno un percorso diverso passando direttamente alle estorsioni, una mossa strategica che consentirà di riorientare gli attacchi e mantenere la stessa kill chain del passato, facendo però a meno del payload rappresentato dal ransomware. Per quelle che decideranno di dedicarsi totalmente a questo modello di business, non si tratterà di una inversione di rotta, come dimostrato dalla gang Conti che già dispone di unità specializzate nell'estorsione dei dati.[10] Anche se è una deviazione dal normale modello del ransomware, estorcere denaro direttamente alle vittime permetterà ai criminali di raccogliere un discreto bottino senza attirare le attenzioni indesiderate dei media e delle forze dell'ordine.

Un altro modo con il quale gli operatori del ransomware potrebbero adattarsi è quello di rivolgere le loro attenzioni verso il cloud. Sempre più aziende spostano dati e asset critici sul cloud, ad esempio Gartner stima che quest'anno la spesa totale per i servizi offerti su cloud pubblici arriverà a 592 miliardi di dollari.[11] Pertanto, il soggetto criminale che volesse mantenere un'attività ransomware redditizia non avrà altra scelta se non quella di seguire chi passa al cloud. Gli ambienti cloud sono rimasti finora immuni a questi attacchi grazie alle significative differenze esistenti tra le infrastrutture IT in cloud e quelle on-premise, considerando che le varianti del ransomware sono state normalmente create per attaccare queste ultime.[12] Tuttavia, ciò fa anche del cloud un proficuo terreno di caccia per chi sa che le possibili risposte agli attacchi ransomware devono essere ancora ben collaudate, in particolare in merito agli attacchi diretti contro le risorse cloud che contengono dati persistenti come object storage, block storage e database.[13] Gruppi cybercriminali come Alert e Monster,[14] che hanno già iniziato a usare framework cross-platform per il malware allo scopo di colpire sia gli utenti Windows che quelli Linux, potrebbero essere già degli anticipatori dello sviluppo di varianti di ransomware di tipo cloud-aware.

Un altro modo con il quale gli operatori del ransomware potrebbero adattarsi è quello di rivolgere le proprie attenzioni verso il cloud. Poiché sempre più aziende spostano dati e asset critici sul cloud, il soggetto criminale che volesse mantenere un'attività ransomware redditizia non avrà altra scelta se non quella di seguire chi passa al cloud.

L'evoluzione dei gruppi ransomware non sarà limitata solamente alle opzioni sopra considerate. È probabile che col tempo si perfezioni la capacità di tali gruppi di assumere decisioni di business e sviluppare attacchi maggiormente mirati. Attacchi versatili di questo genere si baseranno su ransomware per le vittime che ritengono più importante la continuità operativa, sulla estorsione dei dati se la preoccupazione prioritaria è la reputazione del brand, o su una strategia di uscita trasparente qualora i cybercriminali dovessero decidere che l'attacco non vale l'attenzione indesiderata che può suscitare.

/CLOUD TECHNOLOGY

Un'applicazione disomogenea della tecnologia cloud danneggerà le aziende, in quanto aumenta l'adozione di nuovi strumenti

Negli ultimi tre anni le aziende hanno adottato rapidamente la tecnologia cloud migrando asset e operazioni per agevolare il lavoro da casa così come le soluzioni contactless. Le maggiori sfide per le aziende, in particolare per quelle abituate a usare strumenti più tradizionali, sono state la velocità della migrazione, l'adozione di tecnologie cloud di nuova realizzazione e l'integrazione di questi cambiamenti nell'ambiente di lavoro ibrido. Tutto questo è destinato a proseguire nel 2023, tanto che Forrester prevede che nei settori regolamentati e in quello finanziario l'adozione del cloud continuerà a ritmi senza precedenti.[15] Alla luce di tali cambiamenti, i principali aspetti della sicurezza a cui le aziende dovrebbero prestare attenzione sono quelli che emergono dalla mancanza di uniformità nell'implementazione della tecnologia cloud e dalla sua errata configurazione.

In collaborazione con

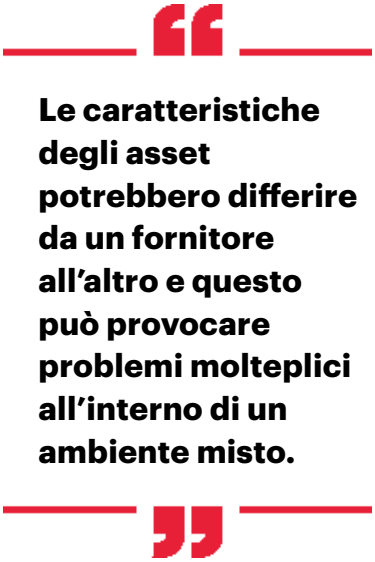
VicOne

I problemi di sicurezza saranno la conseguenza di applicazioni disomogenee, visto che molti CISO (Chief Information Security Officer) non hanno ancora familiarità con le nuove tecnologie o non dispongono della banda necessaria per supervisionare tutti i cloud vendor. Nel backup dei dati, ad esempio, potrebbe esserci un'opzione "ripristino" nel cloud del fornitore A e una soluzione "ripristino" nel cloud del fornitore B, ma le due procedure potrebbero essere molto differenti tra loro. Risultano entrambe collaudate? Il personale è capace di eseguire i due processi di ripristino in parallelo? Sono queste le situazioni che creeranno problemi alle aziende. Anche le caratteristiche degli asset potrebbero differire da un fornitore all'altro, e ciò può provocare molteplici problemi all'interno di un ambiente misto.

Sono prevedibili anche errori di configurazione lato utente, errori che offrono ai criminali informatici una via di accesso ai sistemi enterprise. Gli ambienti cloud aziendali coinvolgono numerosi vendor con differenti policy, asset, servizi interconnessi e risorse. Capire appieno e configurare un ambiente del genere è, quando va bene, difficile. E in questa fase di accelerazione nell'adozione di nuove tecnologie, lo scenario diventa ancora più preoccupante. Gli errori di configurazione rappresentano il rischio più significativo per gli ambienti cloud. Come segnalato lo scorso anno, il 65% - 70% di tutti i problemi di sicurezza relativi al cloud deriva proprio da configurazioni errate.[16]

Potrebbero sorgere problemi anche dal lato degli sviluppatori. Chi sviluppa in cloud lavora sempre più in modo agile, con il rischio quindi di trascurare la sicurezza. È probabile che i cybercriminali sfrutteranno le vulnerabilità di applicazioni e servizi legati a servizi interni ed esterni, dal momento che le aziende potrebbero non essere sempre in pari con le politiche di patching per arginare tempestivamente le vulnerabilità stesse. Osserveremo anche malviventi che sfrutteranno la vecchia tecnica del "living off the land" (letteralmente "vivere delle risorse della terra", ovvero usare le risorse della vittima contro lei stessa) adeguandola al cloud.[17] In un attacco "living off the cloud", il malintenzionato avrebbe già accesso al sistema della vittima usando quindi di nascosto tool legittimi per le attività criminose. Per esempio, potrebbe fare in modo che le soluzioni di backup scarichino informazioni private in una destinazione storage controllata dall'hacker. Questo significa che per gli hacker non è necessario creare propri strumenti software e che è possibile usare questo metodo per restare annidati nei sistemi delle vittime, sfruttando al massimo la propria presenza.

Un nuovo obiettivo di attacco che vale la pena tenere sotto controllo è rappresentato dalle cloud API (Application Programming Interface) per vetture connesse. La maggior parte delle automobili di nuova produzione possiede infatti eSIM (embedded SIM) utilizzate, tra l'altro, per trasmettere dati telematici, comunicare con i cloud server di back-end e creare hotspot Wi-Fi.



Le applicazioni server di back-end basate su cloud comprendono smart app in grado di avviare, fermare e aprire un'autovettura da remoto, così come altre app che monitorano le condizioni del percorso stradale. Le cloud API, perno dell'intera architettura di rete, sono già strettamente integrate con il veicolo stesso, ed è possibile che i criminali informatici cercheranno di sfruttare le falle nella sicurezza presenti poiché queste automobili rappresentano bersagli di alto valore. La API di Tesla ne è un valido esempio: il controllo sull'accesso dipende totalmente da un apposito token e una volta che un criminale ne entra in possesso, si impadronisce dell'auto. Nel 2022 un ragazzino era riuscito ad assumere il controllo di 25 Tesla durante un esperimento di hacking, evidenziando l'importanza dei token delle API per la sicurezza dei veicoli.[18]

Le automobili sono diventate sistemi informatici potenti e complessi che dovrebbero essere protetti con la stessa accortezza adottata per i sistemi enterprise. Le applicazioni per autovetture connesse sono una novità ancora in fase di sviluppo, ma la loro capacità di resistenza alle minacce cyber è ancora poco chiara. Le vetture connesse sono un sistema di sistemi, le cui componenti sono fornite da produttori differenti. Sarà difficile riuscire a garantire la sicurezza da parte di ogni produttore.

il perimetro enterprise si estenderà alle abitazioni degli utenti, abituati ormai a lavorare in un ambiente ibrido

Il lavoro ibrido non era sconosciuto prima della pandemia di Covid-19, ma sono finiti i tempi in cui l'approccio alla sicurezza di un'azienda si limitava alle reti on-premise. Sempre più organizzazioni adottando modelli di lavoro flessibile, destinati a diventare la norma entro il 2024.[19] Uno studio realizzato da Cisco dimostra come questi modelli contribuiscano alla soddisfazione e alla produttività del personale, sebbene solo il 28% del campione intervistato giudichi la propria azienda adeguatamente preparata in relazione al lavoro ibrido.[20]

Tuttavia, con una forza lavoro remota che si sposta continuamente tra reti aziendali e reti domestiche non possono che emergere falle nella sicurezza.[21] Le aziende che si devono difendere hanno poca visibilità sulle reti domestiche dei dipendenti, che potrebbero oltretutto condividere con altri familiari che lavorano per aziende diverse. Nonostante tutti i vantaggi che offre, il lavoro ibrido può innescare effetti collaterali dispendiosi: secondo uno studio effettuato congiuntamente da IBM e Ponemon Institute, le violazioni dei dati possono costare mediamente 5,54 milioni di dollari per le aziende con almeno l'81% di dipendenti remoti, contro un costo di circa 3,15 milioni di dollari per quelle in cui lavora da casa solo la metà del personale.[22]

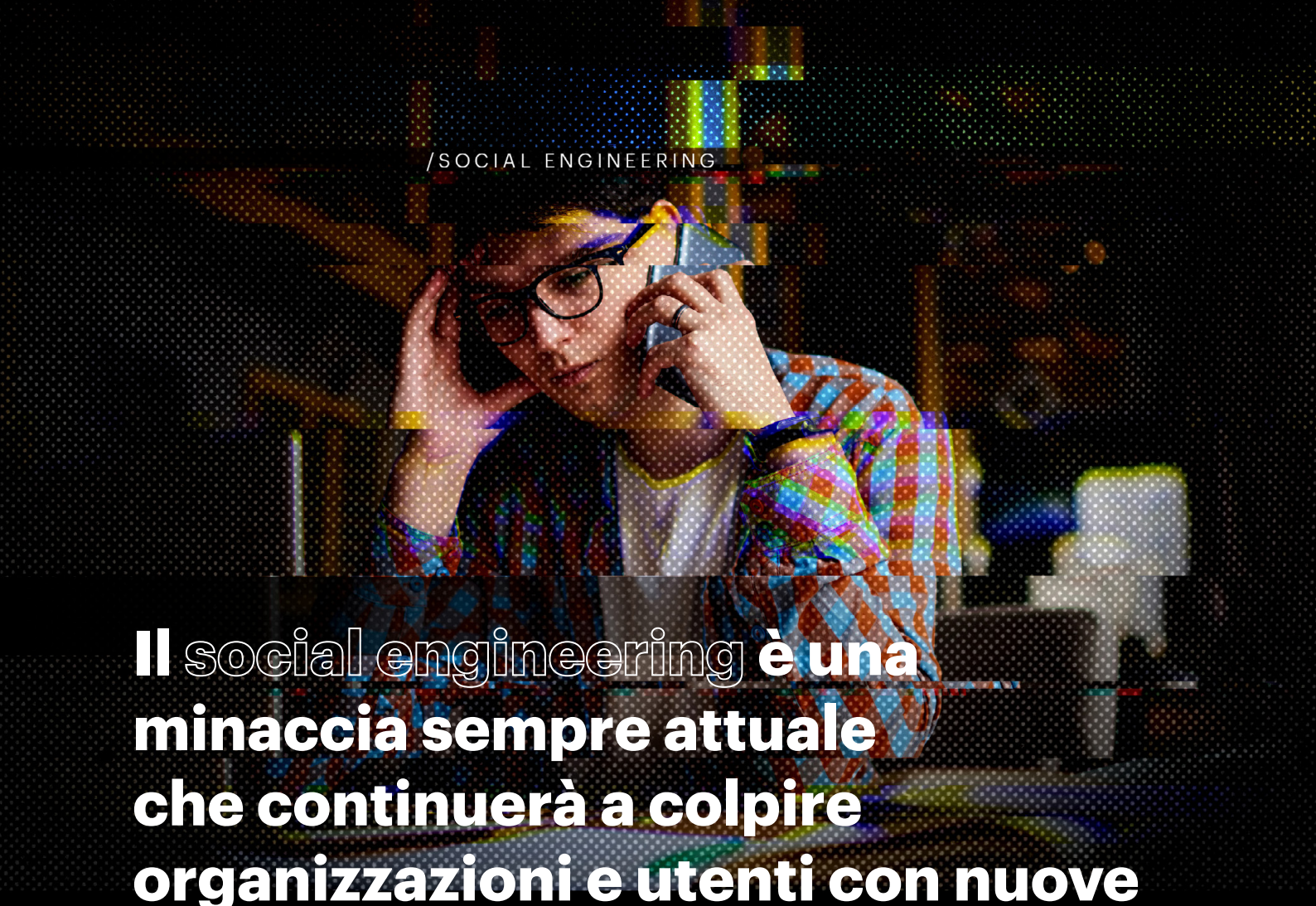
Gli attacchi diretti contro le VPN sono esplosi di quasi il 2000% all'inizio del 2021[23], in un periodo in cui erano ancora in vigore i lockdown e il mondo cercava di adeguarsi ai cambiamenti introdotti dal lavoro remoto. Quest'anno è probabile che cybercriminali creativi sfruttino appieno le postazioni di lavoro ibrido che stanno diventando il nuovo status quo, con un'ondata di attacchi basati su worm di rete, oppure finalizzati a colpire le connessioni domestiche collegate a VPN (Virtual Private Network) per poi eseguire movimenti laterali. In questo modo non solo potranno compromettere le reti delle aziende, ma anche altre reti a cui sono collegati i dispositivi dei vari membri della famiglia.

Le vecchie abitudini sono dure a morire e, nonostante il fatto che il database CVE (Common Vulnerabilities and Exposures) contenga almeno 500 vulnerabilità note riguardanti le VPN, uno studio condotto nel 2022 da Zscaler e Cybersecurity Insiders suggerisce che molte aziende stiano continuando a fare affidamento proprio sulle VPN.[24]

Nonostante le tattiche di mitigazione come l'autenticazione multifattore (MFA) che rafforza le barriere contro gli attacchi, il perimetro enterprise è diventato troppo ampio per poter gestire in sicurezza i vari elementi cloud, le policy BYOD (Bring Your Own Device) e le numerose applicazioni as-a-service che sono oggi diffuse in molte aziende impegnate nella trasformazione digitale.[25] In epoche meno complicate l'approccio del "fossato intorno al castello" poteva essere sufficiente per molte aziende, ma la situazione potrebbe cambiare a breve dal momento che è probabile un aumento nell'adozione dei modelli zero trust nel corso del 2023.

Guardando al futuro, le aziende possono rispondere alle esigenze di tutti i loro dipendenti, sia quelli in ufficio che quelli a casa, con un approccio zero trust. Implementare un ambiente zero trust nel quale l'identità di tutti i dispositivi, di tutti gli utenti e di tutte le app viene considerata vulnerabile e quindi deve essere esplicitamente verificata e associata a una condizione minima di accesso necessario, riduce la possibilità che qualche malintenzionato possa stabilire un accesso all'interno di una rete.[26] Inoltre le soluzioni ZTNA (Zero Trust Network Access) offrono alle aziende un'alternativa alle VPN che rientra in una strategia zero trust più ampia. A differenza delle VPN che forniscono pieno accesso all'intera rete, ZTNA stabilisce solamente una connessione sicura tra gli utenti autorizzati e una specifica applicazione o uno specifico servizio, evitando che un cybercriminale possa muoversi liberamente all'interno di una rete.[27]

Esistono già diversi framework che tracciano varie roadmap a seconda della tipologia di organizzazione interessata a integrare un approccio zero trust nelle proprie operation. Il modello Zero Trust Edge (ZTE) di Forrester, per esempio, delinea il modo in cui i principi zero trust possono essere applicati ai servizi di rete e alla sicurezza del cloud,[28] mentre la Zero Trust Architecture (ZTA) del National Institute of Standards and Technology (NIST) utilizza zero trust per guidare il design di sistemi industriali ed enterprise.[29] Alle aziende sempre più distribuite intenzionate a a intraprendere il percorso verso il cloud può tornare utile il modello Secure Access Service Edge (SASE) di Gartner, un'architettura di rete basata sui principi zero trust che consolida le funzionalità di base delle tecnologie di sicurezza e di rete come ZTNA, Secure Web Gateway (SWG) e Cloud Access Security Broker (CASB).[30] Dal momento che SASE può essere implementata anche in un unico stack software, le aziende possono fornire connessioni sicure ai dipendenti remoti e alle reti delle loro filiali senza l'appesantimento provocato dall'uso di molteplici applicazioni differenziate.



Il social engineering è una minaccia sempre attuale che continuerà a colpire organizzazioni e utenti con nuove tecnologie, come i deepfake

I cybercriminali possono sempre contare sulla fallibilità umana, come punto fermo nel continuo evolvere di economie e tecnologie. Ecco perché gli attacchi basati sul social engineering non passano mai di moda: sono talmente versatili che nel 2023 è probabile l'avvento di nuove versioni potenziate di tattiche ben note e collaudate. Gli attacchi di social engineering più utilizzati fanno leva su temi e notizie di attualità che trovano ampio interesse da parte del pubblico,[31] ma è prevedibile un aumento dei raggiri costruiti sulla ricerca di anime gemelle. I truffatori continueranno infatti a cercare persone sole che più facilmente possono cedere a qualche versione rinnovata della classica trappola romantica, dove profili di utenti fasulli vengono utilizzati per attirare le potenziali vittime in una relazione affettiva con l'obiettivo di estorcere denaro.

Il modello di truffa si è evoluto rispetto a quello in cui il malfattore utilizza un pretesto per ottenere un aiuto finanziario:[32] in certi casi l'obiettivo ultimo è quello di entrare in possesso delle informazioni personali delle vittime adescate su siti fasulli di appuntamenti o, più di recente, come nel caso di "pig butchering" o Sha Zhu Pan, di convincerle a investire su finte piattaforme per il trading di criptovalute.[33]

Truffe di questo tipo rappresentano un vasto business, tanto che nel 2022 la Federal Trade Commission (FTC) statunitense le ha inserite al vertice della classifica delle varie categorie di frodi dell'ultimo quinquennio con 1,3 miliardi di dollari estorti in totale.[34] La situazione è peggiorata nel corso della pandemia,[35] e fino a quando il mondo non si sarà liberato totalmente dal Covid-19 è possibile che i cybercriminali si inventino modi innovativi per approfittare di vittime alla ricerca di una relazione sentimentale durante un lockdown.

Un'altra area nella quale i malviventi daranno nuova vita a tecniche datate combinandole con strumenti moderni è quella delle truffe BEC (Business Email Compromise), dove gli stessi impersonano, attraverso la posta elettronica, alti dirigenti aziendali per sottrarre denaro: un tipo di truffa che continuerà a colpire le organizzazioni anche nel 2023. Il mercato delle truffe BEC è destinato a crescere a un tasso annuale del 19,4%. Anche se il ricorso a software open source per la sicurezza delle email aiuterà a ostacolare questa crescita, le truffe BEC restano decisamente redditizie: entro il 2027 il giro d'affari arriverà a circa 2,8 miliardi di dollari.[36] Si tratta di danni finanziari talmente devastanti per le aziende che, in una recente nota, l'FBI ha sottolineato come le truffe BEC siano una delle principali minacce per l'economia globale.[37]

I tentativi di truffe BEC si sono evoluti fino al punto che oggi i criminali attivi in questo settore hanno messo a catalogo proposte "BEC-as-a-service",[38] chiara indicazione del fatto che stanno diventando sufficientemente esperti e professionali da commercializzare le loro competenze per generare nuovi flussi di ricavi. L'abbondanza e l'accessibilità di informazioni online consentirà di perfezionare ulteriormente le attività BEC rendendole ancora più mirate. Una scarsa attenzione alle password può agevolare il furto di credenziali, mentre sul dark web

> **I truffatori continueranno a cercare persone sole che più facilmente possono cedere a qualche nuova versione della classica trappola romantica.**

è in vendita una vastissima quantità di dati di login[39] ; tuttavia, i criminali informatici hanno dimostrato che non devono nemmeno infrangere la legge per mettere nel mirino i loro prossimi bersagli, in quanto è possibile acquistare lunghi elenchi di indirizzi email da società che si occupano legittimamente di lead generation e che vendono queste liste a scopi di marketing.[40]

I criminali continueranno a sfruttare le potenzialità delle tecnologie di intelligenza artificiale (AI) e machine learning facendo ricorso ai deepfake per potenziare gli aspetti di social engineering dei loro attacchi BEC, strategia che abbiamo già riscontrato "in the wild" nel corso di una nostra ricerca.[41] Nel 2023 i deepfake avranno un'ampia varietà di casistiche di utilizzo cybercriminale, permettendo di impersonare le proprie vittime per trarre in inganno banche e servizi di criptovaluta o persino per creare account utente destinati ai furti di identità. Le truffe basate sull'uso di deepfake sono per ora poco frequenti, ma stanno acquisendo popolarità nelle comunità underground che offrono servizi per la realizzazione di immagini e video fasulli;[42] non passerà quindi molto tempo prima che i tool e le tecniche utili a questi attacchi entrino nella normale disponibilità dei cybercriminali in generale.[43]

/BLOCKCHAIN

L'hype che circonda le novità digitali come NFT e il metaverso è destinato a calare, ma i cybercriminali punteranno alla tecnologia blockchain

L'interesse nei confronti di NFT e metaverso, un tempo i beniamini di Internet, continuerà a scemare[44]. All'inizio del 2022 il mondo era in preda alla NFT-mania e sul mercato degli NFT si scambiavano 17,2 miliardi di dollari, cifra che a settembre era scesa a 466,9 milioni.[45] Anche se le truffe basate sugli NFT potranno proseguire nel 2023, il loro impatto non sarà tuttavia significativo, considerato che i prezzi elevati degli NFT[46] avranno smorzato l'interesse del pubblico nei loro confronti.

Al culmine della loro popolarità, le persone acquistavano NFT di avatar e altri articoli digitali da collezione che si riteneva potessero diventare parte dei mondi del metaverso,[47] spazi virtuali in 3D sui quali Internet aveva riposto le proprie speranze per trovare un nuovo terreno fertile per lo sviluppo di innovazioni nella comunicazione e nella collaborazione.[48] Ma il metaverso ha deluso quelle aspettative e gli esperti del settore non sono concordi sul fatto che si tratti di una tecnologia destinata a durare.[49] Nonostante questo, il lavoro sul metaverso va avanti, quindi è probabile che sacche di attività illegali possano annidarsi in particolare nel cosiddetto Darkverse,[50] l'angolo criminale del Metaverso nel quale si riuniscono piccole comunità underground di malviventi. Ma i cybercriminali vanno dove ci sono le persone, quindi è probabile che nel 2023 questi potranno essere solo incidenti isolati.

> **Le truffe basate sugli NFT potranno andare avanti nel 2023, ma il loro impatto non sarà tuttavia significativo, dal momento che i prezzi elevati degli NFT avranno attenuato l'interesse del pubblico nei loro confronti.**

In netto contrasto con quanto sopra, la blockchain sarà un territorio di frontiera brulicante di attività che potrebbero proseguire ben oltre l'inizio del 2023 e durare anche nei prossimi anni, perché la blockchain è alla base della registrazione sicura e decentralizzata delle transazioni riguardanti le criptovalute. Anche se l'euforia riguardante le valute digitali è scemata a causa dell'abbondanza di truffatori interessati a infiltrarsi nei crypto-wallet degli utenti per sottrarre seed phrase,[51] Internet nel suo complesso non ne farà a meno considerando l'utilità che offrono agli utenti, così come agli autori degli attacchi. Criptovalute come Monero, corredate di funzionalità per la privacy, che consentono maggior libertà di agire in modo anonimo,[52] saranno ancora ampiamente usate dai criminali per i trasferimenti di fondi. Ma considerando la volatilità delle valute digitali,[53] è probabile che le persone le convertano rapidamente in moneta tradizionale anziché conservarle nei wallet, in modo da evitare gli effetti di drastici crolli di mercato. Questo cambiamento nel comportamento degli utenti spingerà i malviventi a progettare ulteriori meccanismi di riciclaggio del denaro.

È possibile anche che gli attacchi collegati alle criptovalute continuino a essere sferrati da Paesi nei quali i cybercriminali hanno sviluppato una specializzazione in relazione agli asset digitali. Solo nel 2022 alcuni specifici gruppi di hacker sono stati identificati e sospettati di rapine di alto profilo, come quella messa a segno contro Horizon Bridge, società statunitense che agevola i trasferimenti di asset attraverso le blockchain,[54] e il gioco online Axie Infinity, i cui utenti guadagnano criptovaluta mentre giocano.[55] Secondo un report bancario, l'interesse verso le criptovalute nasce dall'anonimato che esse consentono e dalla difficoltà nel tracciare le transazioni[56] che possono aiutare a ottenere finanziamenti e risorse.[57]

Più nello specifico, è possibile assistere a un aumento del rischio di violazioni per le piattaforme di exchange di criptovalute. I criminali saranno indubbiamente attirati da siti che agiscono da banche e broker specializzati in moneta digitale senza tuttavia essere vincolati agli stessi obblighi assicurativi e di trasparenza dei tradizionali istituti finanziari.[58] Ma soprattutto potrebbero derubare queste piattaforme per milioni di dollari, come dimostrato dagli attacchi avvenuti contro società come Liquid Global,[59] FTX[60] e Binance.[61]

I criminali sfrutteranno ulteriormente le vulnerabilità e colpiranno superfici di attacco solitamente trascurate, come il software open source

I malviventi sono decisamente creativi, sempre impegnati a esaminare la postura di sicurezza di un'azienda da diversi punti di vista per trovare crepe nei sistemi di difesa. Quest'anno i criminali colpiranno le aziende distratte che avranno tralasciato di controllare e sostituire i protocolli obsoleti presenti nelle proprie reti, una pericolosa dimenticanza che potrebbe aprire le porte a cyberattacchi. In particolare, un sondaggio del 2021 aveva evidenziato che il 92% delle aziende continuava a usare protocolli non sicuri come per esempio Microsoft SMBv1. I produttori hanno smesso da tempo di supportare quei vecchi protocolli[62] che molte varianti di ransomware sfruttano comunemente per infiltrarsi nelle reti. Le aziende che si ostinano a utilizzarli sono a rischio di infezione da parte di ransomware come WannaCry e NotPetya.[63]

Anche elementi della sicurezza dei dispositivi che vengono spesso trascurati, come l'uso dei router, richiameranno le attenzioni indesiderate dei cybercriminali. Coloro che vorranno muoversi sottotraccia approfitteranno facilmente della mancanza di visibilità delle aziende sui dispositivi collegati alle reti corporate, specie nel caso di organizzazioni poco attente ad aggiornare i firmware o a mantenere un log delle attività. Anche quando gli stessi produttori avvertono i propri clienti riguardo ai pericoli rappresentati da router vulnerabili, come nel caso della botnet Cyclops Blink che ha colpito i router Wi-Fi Asus[64], per esempio, da uno studio del 2022 emerge che la maggior parte degli utilizzatori di questi dispositivi non ha mai preso in considerazione l'idea di aggiornarli, offrendo ai malviventi il perfetto vettore di attacco nell'era dell'Internet of Things (IoT).[65]

I dispositivi collegati a Internet e i sistemi maggiormente esotici correranno ulteriori rischi in presenza di un malware scritto con linguaggi di programmazione insoliti come Rust e Golang, che permettono ai cybercriminali di compilare malware per sistemi operativi differenti, rendendo la prossima generazione di varianti malware molto più difficile da rilevare, analizzare e sottoporre a reverse-engineering.[66]

È probabile che nel 2023 anche i criminali approfondiscano il modo in cui il software viene costruito concentrandosi sulle vulnerabilità presenti nelle componenti condivise del software stesso. Opportunità in questo ambito sono già state sfruttate, come ha evidenziato lo studio State of the Software Supply Chain Report di Sonatype, che ha scoperto nel 2022 un incremento del 633% anno su anno degli attacchi diretti contro le repository di software open source, sull'onda dei 3,1 trilioni di richieste di software open source a livello mondiale.[67] È possibile che le vulnerabilità zero-day nel software open source avranno ricadute estese a molti settori, specialmente all'automotive dove viene ampiamente usato per i chip, l'hardware, il firmware, i sistemi operativi e le applicazioni dei veicoli.

Dopo la scoperta di errori critici all'interno di Log4j che hanno costretto Internet a riconsiderare la fiducia implicitamente riposta nel software open source, soggetti pubblici e privati stanno innalzando le difese contro possibili attacchi basati su queste vulnerabilità. Google, per esempio, ha lanciato un programma di bug bounty in ragione della propria dipendenza da software open source di terze parti, nella speranza di intercettare e risolvere gli errori prima che possano finire in mani pericolose.[68] Insieme ad altri colossi tecnologici come Apple, Amazon e IBM, Google ha anche proposto la formazione di un gruppo dedicato alla manutenzione e al supporto dei progetti open source.[69] Dal canto loro, i legislatori statunitensi stanno iniziando a riconoscere l'importanza del ruolo ricoperto dal software open source nel plasmare il mondo digitale, come evidenziato dall'introduzione della proposta di legge Securing Open Source Software Act[70] che, se approvata, imporrebbe alla Cybersecurity and Infrastructure Security Agency (CISA) di lavorare a un framework di rischio e offrire misure di sicurezza che possano guidare il governo federale nell'utilizzo del software open source.

Attualmente la maggior parte dei software comprende un codice di terze parti commissionato appositamente per un certo prodotto o per componenti off-the-shelf preconfezionati progettati per svolgere una specifica funzione.[71] Ciò potrebbe spingere i cybercriminali a infiltrarsi all'interno di risorse ampiamente diffuse come Python Package Index (PyPI) o npm, il package manager di JavaScript, in modo da introdursi con un malware camuffato da codice legittimo. Ora che la maggior parte dei progetti cloud-native si avvale di librerie e dipendenze, inclusi i software open source,[72] un malware camuffato è un punto debole sul quale le aziende possono scivolare. Poiché librerie software vengono spesso incorporate durante il ciclo di sviluppo di un progetto e quindi raramente controllate per la ricerca di vulnerabilità note, qualsiasi loro criticità ricade a tutti gli effetti all'interno delle cloud operation in azienda.

Per consolidare le proprie difese, le aziende dovranno quindi impegnarsi ad analizzare e patchare periodicamente le varie configurazioni software, preferibilmente nell'ambito di un piano di gestione delle vulnerabilità a tenuta stagna. Rispetto alle aziende più piccole, le realtà più strutturate facilmente dispongono già di policy per la sicurezza del software open source, oltre che di team dedicati alla supervisione della sicurezza e di misure di monitoraggio automatizzate in grado di neutralizzare gli attacchi di tipo supply chain, tipiche di chi cerca di sfruttare la capillare diffusione del software open source.[73] Tuttavia sarà necessario creare anche una distinta base del software per ciascuna applicazione impiegata: questo elenco delle varie componenti in uso diventerà essenziale per la sicurezza del software e la gestione del rischio nelle supply chain delle aziende, fornendo una sorta di inventario dei componenti e delle dipendenze software così da poter sapere quali versioni e sistemi possono essere vulnerabili non appena viene scoperta una falla nel software stesso.[74]

Le industrie diventeranno più tecnologiche ma dovranno affrontare carenze di personale e normative verticali

Può sembrare una buona idea restare fermi e tranquilli di fronte a una possibile recessione, ma è proprio nei momenti di crisi che i costi delle opportunità sono inferiori, liberando budget per la trasformazione digitale senza incidere sulla bottom line.[75] In previsione della congiuntura economica che potrebbe verificarsi nel 2023, è probabile che le aziende più strutturate investiranno in tecnologie avanzate come la connettività 5G. Le recenti innovazioni nel campo del 5G, che consentono di supportare eMBB (enhanced Mobile Broadband), URLCC (Ultra-Reliable and Low-Latency Communication) e mMTC (massive Machine Type Communication), promettono di schiudere nuove casistiche d'uso e opportunità di mercato per le aziende lungo il loro percorso verso l'Industrial Internet of Things (IIoT).[76]

In collaborazione con

txOne networks

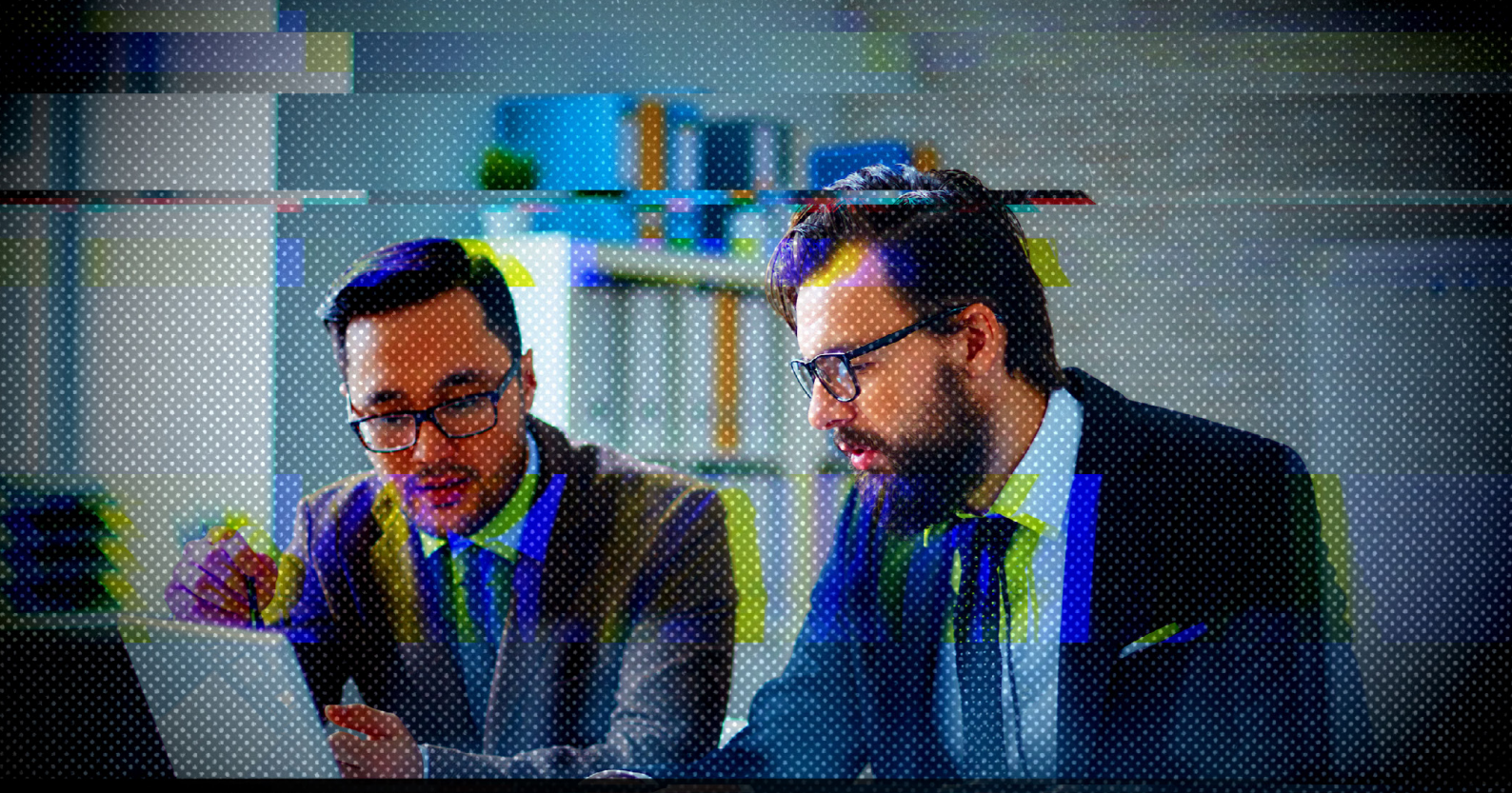
La crescente necessità di reti a elevata affidabilità e bassa latenza da parte delle industrie è sicuramente destinata ad alimentare il mercato IIoT 5G in tutto il mondo, per il quale si stima un valore di 18,9 miliardi di dollari entro il 2030;[77] qualunque pausa nell'attività economica offre un'opportunità ideale per evolvere andando oltre le vecchie reti 4G.

Analogamente è probabile un graduale aumento degli OEM (Original Equipment Manufacturer) dotati di proposte e soluzioni che incorporano la AI. L'adozione della AI su vasta scala all'interno dell'industria non avverrà dalla sera alla mattina, ma sarà accelerata in alcune aree delle operation, in particolare quelle con requisiti di resa molto elevata. Per le aziende impegnate a digitalizzare le proprie fabbriche, i tool basati su AI promettono anche di essere una forza moltiplicatrice di efficienza consentendo di prevedere meglio i comportamenti di acquisto dei clienti[78] e automatizzare attività complesse per gli operatori umani che supervisionano gli asset industriali.[79] Mentre le industrie si rivolgono all'IT per ottenere un vantaggio competitivo, anche i malfattori approfitteranno di questa tecnologia emergente per potenziare gli attacchi in termini di automazione e ricerca,[80] facendo della AI offensiva una minaccia incombente che le realtà industriali dovranno tenere sotto controllo negli anni a venire.

L'accresciuta integrazione tra IT e OT[81] determinata da queste tecnologie trasformative diventerà una lama a doppio taglio per le industrie, specialmente laddove le strategie di sicurezza per le infrastrutture IT sono separate da quelle per le infrastrutture OT: una convergenza che, pur consentendo di monitorare le operazioni da vicino,[82] espone le aziende a minacce impreviste. Nel 2023 è probabile un trend in crescita per quanto concerne i cyberattacchi basati su IT che colpiscono inavvertitamente i sistemi OT collegati alle reti IT, rivelando i sistemi OT quale vettore di attacco sottoutilizzato attraverso cui i criminali informatici possono spostarsi lateralmente tra ambienti OT e IT.[83]

Anche se le aziende si stanno mettendo al riparo su questo fronte, la vera sfida è reperire expertise in grado di tenere la tecnologia perfettamente al sicuro, e nel 2023 gli ambienti OT/ICS (Operational Technology/ Industrial Control Systems) saranno tra quelli maggiormente colpiti dalla carenza di competenze nella sicurezza. Le sfide della cybersecurity in questo ambito sono legate spesso alla mancanza di personale e all'errore umano,[84] per cui è probabile che tali fattori renderanno zoppicanti i sistemi OT e lasceranno gli ambienti industriali in mano a team di sicurezza sguarniti e tuttavia incaricati di proteggere le reti di molteplici fabbriche. È risaputo che i malintenzionati si allenano su sistemi simili a quelli dei loro obiettivi industriali per sviluppare malware customizzati per ambienti OT/ICS,[85] pertanto le aziende che non riescono a trovare personale qualificato per gestire le nuove tecnologie appena adottate potrebbero trovarsi a dover affrontare interruzioni e problemi nell'ambito OT/ICS. Sulla base di una nostra ricerca, abbiamo calcolato che interruzioni del genere possono provocare mediamente perdite finanziarie fino a 2,8 milioni di dollari per incidente.[86]

La necessità di competenze nella sicurezza OT/ ICS è inoltre essenziale per gestire le esigenze di cybersicurezza dei mercati verticali,[87] destinate ad aumentare nel nuovo anno. I sistemi OT sono già severamente regolamentati in taluni settori, come nel caso dei produttori statunitensi di apparecchiature diagnostiche[88] e imbarcazioni marittime,[89] e nel 2023 è probabile un aumento delle aziende che si dirigeranno verso forme di collaborazione e autoregolamentazione. I moderni impianti industriali sono noti per comportarsi proattivamente quando si tratta di proteggersi: le linee guida per la cybersicurezza possono essere definite dalle società capofila piuttosto che dallo stesso senior management, ma molte smart factory adottano misure di sicurezza soprattutto per essere conformi agli standard vigenti nei rispettivi settori.[90] L'industria dovrà anche restare aggiornata a fronte di una crescita delle regolamentazioni, siano esse settoriali piuttosto che governative, destinate a rendere gli ambienti OT/ICS sempre più controllati. Anche se normative del genere possono già esistere a livello nazionale, cyberattacchi contro il settore industriale come quelli che hanno colpito la supply chain di Colonial Pipeline[91] hanno spinto i legislatori a prevenire futuri attacchi introducendo ulteriori direttive ispirate all'Executive Order (EO) 14028 "Improving the Nation's Cybersecurity" promulgato negli Stati Uniti.[92]



/CYBERSECURITY PLATFORMS

Le aziende abbandoneranno l'approccio alla cybersicurezza basato su soluzioni verticali specifiche

Nel 2023 numerose aziende metteranno la parola fine alle strategie di sicurezza circoscritte passando finalmente ad approcci maggiormente olistici. Anche se molte di esse continueranno ad affidarsi a un repertorio di soluzioni verticali eterogenee e spesso frammentate, ovvero progettate per affrontare le varie minacce una per una, tool di questo tipo non riescono più a tenere testa alle sempre più sofisticate minacce cyber dirette contro le aziende, soprattutto in un'epoca cloud-native. Queste soluzioni individuali finiscono con l'accumularsi, inondando i team responsabili della sicurezza di allarmi costanti che rischiano di passare inosservati per la troppa frequenza.[93] Le aziende possiedono in media 46 tool di monitoraggio specifici, il che rende difficile capire a quali alert dare la priorità con l'ulteriore pericolo di sottovalutare i segnali di un attacco effettivo.[94]

In risposta a questo, l'esigenza di una piattaforma di cybersicurezza unificata è destinata a diffondersi nelle aziende che richiedono una visibilità superiore su asset sparsi tra ambienti, reti e sistemi operativi. Per poter neutralizzare attacchi da parte di criminali sempre più metodici e professionali, le aziende dovranno essere nella posizione di poter rilevare attività sospette sui propri sistemi su una scala più vasta: un approccio basato su piattaforma integra i prodotti del fornitore di cybersicurezza con strumenti di terze parti,[95] il che non solo razionalizza la user experience ma fornisce anche a chi si difende visibilità e telemetria enterprise-wide sull'intera infrastruttura IT, che rappresenta la superficie d'attacco da mappare.[96] La sfida per il nuovo anno non è solo quella di consolidare i diversi tool per rilevare eventuali minacce, ma anche di recuperare il ritardo nei confronti di criminali che oggi operano come vere e proprie aziende. La struttura organizzativa della gang Conti, per esempio, comprende un dipartimento delle risorse umane e dipendenti stipendiati.[97]

È inoltre probabile un aumento dell'interesse nei confronti degli MSP (Managed Service Provider), considerati un vettore di attacco alternativo al colpire singole vittime. Compromettere la rete di un MSP, che ha accesso a numerosi clienti, permetterebbe infatti di attaccare le infrastrutture di più aziende in una volta sola massimizzando l'impatto dell'offensiva.[98] È possibile che non vengano colpiti solamente gli MSP ma anche gli MSSP (Managed Security Service Provider) e i tool che essi utilizzano. Ritorcere il toolset di un MSSP contro sé stesso permette di aggirare meglio chi si difende, costringendolo ad analizzare le numerose applicazioni usate sia dall'MSSP che dal proprio team di sicurezza interno per determinare la reale fonte dell'attività sospetta.

Le forze dell'ordine sono già sulle tracce di criminali che intendono colpire gli MSP, tanto che la CISA ha diramato un avviso per sollecitare gli MSP e i loro clienti a rafforzare i rispettivi livelli di sicurezza contro i cybercriminali – in particolare i gruppi APT (Advanced Persistent Threat) sponsorizzati da Stati nazionali – che potrebbero gettare nel panico le supply chain globali colpendo gli MSP per entrare nelle reti dei loro clienti.[99] La CISA e le agenzie con cui essa collabora raccomandano una serie di contromisure come il rilevamento sugli endpoint, il monitoraggio delle difese di rete e il whitelisting delle applicazioni esplicitamente autorizzate. Queste attività di mitigazione possono essere razionalizzate all'interno di una soluzione completa basata su piattaforma in grado di crescere insieme alle organizzazioni.

Anche se è possibile un aumento delle aziende interessate ai vantaggi offerti dalle piattaforme per la sicurezza, la diffusione di queste ultime richiede anche la convinta adesione da parte del senior management. Insieme con i CISO, nel 2023 anche i CFO (Chief Finance Officer) avranno più voce in capitolo nell'orientare le priorità di acquisto nel campo della cybersicurezza. Ciò potrebbe tuttavia lasciare insufficientemente protette le aziende meno accorte che si concentrano più sui costi che sulle funzionalità: un recente sondaggio condotto su CFO di tutto il mondo ha mostrato che l'87% del campione ha fiducia nelle capacità di neutralizzazione dei cyberattacchi da parte delle rispettive aziende,nonostante il 61% abbia subito almeno tre incidenti nell'arco degli ultimi 18 mesi.[100] Una intera distesa di tool non può cancellare il fatto che, secondo uno studio di Accenture, il ruolo di molti CFO è già sovraccarico di responsabilità.[101] L'input e il coinvolgimento dei CFO è fondamentale per un corretto approccio alla sicurezza di un'azienda, dal momento che rientra proprio tra le loro funzioni il doversi occupare anche di premi cyberassicurativi in costante aumento, sotto l'occhio meticoloso degli assicuratori stessi che chiedono di esaminare le misure di sicurezza dei propri assicurati.[102]

In questo contesto, le aziende dovranno risolvere il gap di consapevolezza del senior management circa i pericoli che i cybercriminali rappresentano per le normali attività quotidiane.

UNO/ SGUARDO AL 2023

Le previsioni di Trend Micro per il 2023 delineano le tendenze e i rischi che si verificheranno nello scenario della cybersicurezza sulla base delle osservazioni e delle approfondite ricerche condotte dai propri esperti. Prepararsi alle minacce in evoluzione che emergeranno quest'anno impone alle aziende di disporre di un piano di difesa stratificato e rafforzato da misure di mitigazione come:

- **Proteggere ambienti e sistemi con una strategia zero trust.** Considerati gli attuali ambienti di lavoro misti, sarebbe incosciente per le aziende pensare che l'intero traffico interno sia sicuro. Adottando l'atteggiamento zero trust di "mai fidarsi, sempre verificare" nella propria architettura IT, le aziende possono minimizzare i danni di qualsiasi attacco cyber futuro senza sacrificare la produttività degli utenti che hanno bisogno di accedere alle risorse corporate per il proprio lavoro

- **Investire sulla formazione dei dipendenti.** Il personale è l'ultima e più debole linea di difesa nella cybersecurity, un fattore che i criminali non esitano a sfruttare. Nessuna misura di sicurezza può bloccare un avversario quando sono i dipendenti stessi che inconsapevolmente gli permettono di entrare. Per questo motivo, una formazione che permetta alla forza lavoro di identificare i segnali di pericolo può fare un'enorme differenza nella gestione di minacce potenzialmente devastanti

- **Aumentare la trasparenza attraverso una piattaforma di sicurezza completa.** Le aziende possono trarre vantaggio dal consolidamento di tutte le loro funzionalità di monitoraggio e rilevamento all'interno di un'unica piattaforma olistica. Questo aumenta la capacità di intercettare attività sospette sulle reti aziendali e riduce inoltre il carico di lavoro assegnato ai team responsabili della sicurezza, mantenendoli pronti e reattivi. In alternativa, le aziende possono ridurre il ventaglio dei fornitori di sicurezza conservando quelli che offrono soluzioni versatili e multifunzionali

- **Scoprire i punti deboli delle infrastrutture IT per mezzo di stress test.** Le aziende dovrebbero possedere un piano per garantire la propria capacità di risposta a differenti scenari di attacco, specialmente quelli che comportano l'avvenuta violazione dei gateway perimetrali. Per esempio, le aziende dovrebbero essere in grado di prevedere la propria situazione operativa effettiva nel caso in cui solamente metà del personale IT fosse disponibile per affrontare la violazione del proprio Internet gateway, dei propri record DNS (Domain Name System) o di qualsiasi altro sistema critico. Riservare del tempo per allenarsi su attacchi simulati fornisce ai team di sicurezza un'esperienza sul campo priva di rischi reali

- **Fare un inventario dei servizi cloud per razionalizzare l'uso del cloud stesso.** La visibilità sul cloud è essenziale per poter mettere ordine nel caos della gestione degli innumerevoli servizi cloud usati dalle aziende. Una strategia di monitoraggio del cloud dovrebbe anzitutto mappare tutte le soluzioni collegate all'infrastruttura cloud aziendale, così da mantenere informati i team responsabili della sicurezza sul valore che questi servizi forniscono all'azienda, sui dati a cui questi servizi hanno accesso e sui contatti disponibili per ottenere ulteriore supporto. In questo modo sarà possibile tagliare qualsiasi ridondanza che assorbe risorse preziose e tenere il passo con i crescenti standard di conformità per la sicurezza del cloud.

Nel 2023 la dura realtà della migrazione verso il cloud, del lavoro da remoto e dello sviluppo software metterà senz'altro alla prova la resilienza e la prontezza dei team incaricati della sicurezza. Per affrontare le incertezze che le aspettano nello scenario della sicurezza, le aziende avranno bisogno di una suite di protezione in grado di determinare e minimizzare i rischi di violazioni su molteplici layer. Ma, soprattutto, se si vuole tenere testa alle minacce cyber che arriveranno nel 2023 e oltre, le strategie di difesa devono essere basate su insight affidabili e relativi ai fattori che determinano il ciclo di vita delle minacce.

Bibliografia

1 Janna Anderson, Lee Rainie, and Emily A. Vogels. (Feb. 18, 2021). *Pew Research Center.* "Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges." Consultato il 12 novembre 2022 all'indirizzo https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges.

2 Janna Anderson, Lee Rainie, and Emily A. Vogels. (Feb. 18, 2021). *Pew Research Center.* "Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges." Consultato il 12 novembre 2022 all'indirizzo https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges.

3 Janna Anderson, Lee Rainie, and Emily A. Vogels. (Feb. 18, 2021). *Pew Research Center.* "Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges." Consultato il 12 novembre 2022 all'indirizzo https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges.

4 Janna Anderson, Lee Rainie, and Emily A. Vogels. (Feb. 18, 2021). *Pew Research Center.* "Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges." Consultato il 12 novembre 2022 all'indirizzo https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges.

5 Janna Anderson, Lee Rainie, and Emily A. Vogels. (Feb. 18, 2021). *Pew Research Center.* "Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges." Consultato il 12 novembre 2022 all'indirizzo https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges.

6 Danny Palmer. (Jan. 14, 2022). *ZDNet.* "Russian authorities take down REvil ransomware gang." Consultato il 18 novembre 2022 all'indirizzo https://www.zdnet.com/article/russian-authorities-take-down-revil-ransomware-gang.

7 Danny Palmer. (Jan. 14, 2022). *ZDNet.* "Russian authorities take down REvil ransomware gang." Consultato il 18 novembre 2022 all'indirizzo https://www.zdnet.com/article/russian-authorities-take-down-revil-ransomware-gang.

8 Danny Palmer. (Jan. 14, 2022). *ZDNet.* "Russian authorities take down REvil ransomware gang." Consultato il 18 novembre 2022 all'indirizzo https://www.zdnet.com/article/russian-authorities-take-down-revil-ransomware-gang.

9 Danny Palmer. (Jan. 14, 2022). *ZDNet.* "Russian authorities take down REvil ransomware gang." Consultato il 18 novembre 2022 all'indirizzo https://www.zdnet.com/article/russian-authorities-take-down-revil-ransomware-gang.

10 Josh Stella. (March 18, 2022). *Business Wire.* "Why Ransomware Attacks Steer Clear of the Cloud." Consultato il 18 novembre 2022 all'indirizzo https://www.businesswire.com/news/home/20220318005081/en/Why-Ransomware-Attacks-Steer-Clear-of-the-Cloud.

11 Josh Stella. (March 18, 2022). *Business Wire.* "Why Ransomware Attacks Steer Clear of the Cloud." Consultato il 18 novembre 2022 all'indirizzo https://www.businesswire.com/news/home/20220318005081/en/Why-Ransomware-Attacks-Steer-Clear-of-the-Cloud.

12 Josh Stella. (March 18, 2022). *Business Wire.* "Why Ransomware Attacks Steer Clear of the Cloud." Consultato il 18 novembre 2022 all'indirizzo https://www.businesswire.com/news/home/20220318005081/en/Why-Ransomware-Attacks-Steer-Clear-of-the-Cloud.

13 Josh Stella. (March 18, 2022). *Business Wire.* "Why Ransomware Attacks Steer Clear of the Cloud." Consultato il 18 novembre 2022 all'indirizzo https://www.businesswire.com/news/home/20220318005081/en/Why-Ransomware-Attacks-Steer-Clear-of-the-Cloud.

14 Josh Stella. (March 18, 2022). *Business Wire.* "Why Ransomware Attacks Steer Clear of the Cloud." Consultato il 18 novembre 2022 all'indirizzo https://www.businesswire.com/news/home/20220318005081/en/Why-Ransomware-Attacks-Steer-Clear-of-the-Cloud.

15 Danny Palmer. (Jan. 14, 2022). *ZDNet.* "Russian authorities take down REvil ransomware gang." Consultato il 18 novembre 2022 all'indirizzo https://www.zdnet.com/article/russian-authorities-take-down-revil-ransomware-gang.

16 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives.* "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

17 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives.* "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

18 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives.* "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

19 Danny Palmer. (Jan. 14, 2022). *ZDNet.* "Russian authorities take down REvil ransomware gang." Consultato il 18 novembre 2022 all'indirizzo https://www.zdnet.com/article/russian-authorities-take-down-revil-ransomware-gang.

20 Cisco. (May 24, 2022). *Cisco.* "Cisco Study: Hybrid work is enhancing employee well-being, but needs to be more inclusive." Consultato il 18 novembre 2022 all'indirizzo https://news-blogs.cisco.com/apjc/2022/05/24/cisco-study-hybrid-work-is-enhancing-employee-well-being-and-productivity-in-asean-but-efforts-are-needed-to-make-it-more-inclusive.

21 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives.* "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

22 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives.* "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

23 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives.* "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

24 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives.* "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

25 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives.* "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

26 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives.* "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

27 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

28 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

29 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

30 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

31 Danny Palmer. (Jan. 14, 2022). *ZDNet*. "Russian authorities take down REvil ransomware gang." Consultato il 18 novembre 2022 all'indirizzo https://www.zdnet.com/article/russian-authorities-take-down-revil-ransomware-gang.

32 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

33 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

34 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

35 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

36 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

37 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

38 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

39 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

40 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

41 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

42 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

43 Mark Nunnikhoven. (Jan. 13, 2021). *Trend Micro Research, News, and Perspectives*. "The Top Worry In Cloud Security for 2021." Consultato il 18 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.html.

44 Danny Palmer. (Jan. 14, 2022). *ZDNet*. "Russian authorities take down REvil ransomware gang." Consultato il 18 novembre 2022 all'indirizzo https://www.zdnet.com/article/russian-authorities-take-down-revil-ransomware-gang.

45 Danny Palmer. (Jan. 14, 2022). *ZDNet*. "Russian authorities take down REvil ransomware gang." Consultato il 18 novembre 2022 all'indirizzo https://www.zdnet.com/article/russian-authorities-take-down-revil-ransomware-gang.

46 Danny Palmer. (Jan. 14, 2022). *ZDNet*. "Russian authorities take down REvil ransomware gang." Consultato il 18 novembre 2022 all'indirizzo https://www.zdnet.com/article/russian-authorities-take-down-revil-ransomware-gang.

47 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

48 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

49 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

50 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

51 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

52 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

53 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

54 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

55 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

56 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

57 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

58 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

59 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

60 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

61 CBS News. (Oct. 7, 2022). *CBS News*. "Hackers access $570 million in crypto with attack on Binance." Consultato il 18 novembre 2022 all'indirizzo https://www.cbsnews.com/news/binance-hack-100-million-cryptocurrency-blockchain.

62 Kaspersky. (June 08, 2022). *Kaspersky*. "87 critical vulnerabilities discovered in routers in 2021." Consultato il 19 novembre 2022 all'indirizzo https://www.kaspersky.com/about/press-releases/2022_87-critical-vulnerabilities-discovered-in-routers-in-2021.

63 Kaspersky. (June 08, 2022). *Kaspersky*. "87 critical vulnerabilities discovered in routers in 2021." Consultato il 19 novembre 2022 all'indirizzo https://www.kaspersky.com/about/press-releases/2022_87-critical-vulnerabilities-discovered-in-routers-in-2021.

64 Kaspersky. (June 08, 2022). *Kaspersky*. "87 critical vulnerabilities discovered in routers in 2021." Consultato il 19 novembre 2022 all'indirizzo https://www.kaspersky.com/about/press-releases/2022_87-critical-vulnerabilities-discovered-in-routers-in-2021.

65 Kaspersky. (June 08, 2022). *Kaspersky*. "87 critical vulnerabilities discovered in routers in 2021." Consultato il 19 novembre 2022 all'indirizzo https://www.kaspersky.com/about/press-releases/2022_87-critical-vulnerabilities-discovered-in-routers-in-2021.

66 Lorna Mitchell. (Sept. 23, 2022). *Dark Reading*. "Neglecting Open Source Developers Puts the Internet at Risk." Consultato il 18 novembre 2022 all'indirizzo https://www.darkreading.com/attacks-breaches/neglecting-open-source-developers-puts-the-internet-at-risk.

67 Lorna Mitchell. (Sept. 23, 2022). *Dark Reading*. "Neglecting Open Source Developers Puts the Internet at Risk." Consultato il 18 novembre 2022 all'indirizzo https://www.darkreading.com/attacks-breaches/neglecting-open-source-developers-puts-the-internet-at-risk.

68 Lorna Mitchell. (Sept. 23, 2022). *Dark Reading*. "Neglecting Open Source Developers Puts the Internet at Risk." Consultato il 18 novembre 2022 all'indirizzo https://www.darkreading.com/attacks-breaches/neglecting-open-source-developers-puts-the-internet-at-risk.

69 Lorna Mitchell. (Sept. 23, 2022). *Dark Reading*. "Neglecting Open Source Developers Puts the Internet at Risk." Consultato il 18 novembre 2022 all'indirizzo https://www.darkreading.com/attacks-breaches/neglecting-open-source-developers-puts-the-internet-at-risk.

70 Lorna Mitchell. (Sept. 23, 2022). *Dark Reading*. "Neglecting Open Source Developers Puts the Internet at Risk." Consultato il 18 novembre 2022 all'indirizzo https://www.darkreading.com/attacks-breaches/neglecting-open-source-developers-puts-the-internet-at-risk.

71 Lorna Mitchell. (Sept. 23, 2022). *Dark Reading*. "Neglecting Open Source Developers Puts the Internet at Risk." Consultato il 18 novembre 2022 all'indirizzo https://www.darkreading.com/attacks-breaches/neglecting-open-source-developers-puts-the-internet-at-risk.

72 Lorna Mitchell. (Sept. 23, 2022). *Dark Reading*. "Neglecting Open Source Developers Puts the Internet at Risk." Consultato il 18 novembre 2022 all'indirizzo https://www.darkreading.com/attacks-breaches/neglecting-open-source-developers-puts-the-internet-at-risk.

73 Lorna Mitchell. (Sept. 23, 2022). *Dark Reading*. "Neglecting Open Source Developers Puts the Internet at Risk." Consultato il 18 novembre 2022 all'indirizzo https://www.darkreading.com/attacks-breaches/neglecting-open-source-developers-puts-the-internet-at-risk.

74 Lorna Mitchell. (Sept. 23, 2022). *Dark Reading*. "Neglecting Open Source Developers Puts the Internet at Risk." Consultato il 18 novembre 2022 all'indirizzo https://www.darkreading.com/attacks-breaches/neglecting-open-source-developers-puts-the-internet-at-risk.

75 Jun Morimoto. (July 11, 2022). *Trend Micro Research, News, and Perspectives*. "Private 5G Network Security Expectations Part 3." Consultato il 23 novembre 2022 all'indirizzo https://www.trendmicro.com/en_ph/research/22/g/private-5g-network-security-part-3.html.

76 Jun Morimoto. (July 11, 2022). *Trend Micro Research, News, and Perspectives*. "Private 5G Network Security Expectations Part 3." Consultato il 23 novembre 2022 all'indirizzo https://www.trendmicro.com/en_ph/research/22/g/private-5g-network-security-part-3.html.

77 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

78 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

79 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

80 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

81 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

82 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

83 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

84 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

85 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

86 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

87 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

88 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

89 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

90 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

91 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

92 Trend Micro. (March 30, 2022). *Trend Micro Research, News, and Perspectives*. "An In-Depth Look at ICS Vulnerabilities Part 1." Consultato il 25 novembre 2022 all'indirizzo https://www.trendmicro.com/en_us/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html.

93 Trend Micro. (Oct. 12, 2021). *Trend Micro*. "Cybersecurity Tool Sprawl Drives Plans to Outsource Detection and Response." Consultato il 18 novembre 2022 all'indirizzo https://www.multivu.com/players/English/8967351-trend-micro-cybersecurity-tool-sprawl-drives-plans-outsource-detection-response.

94 Trend Micro. (Oct. 12, 2021). *Trend Micro*. "Cybersecurity Tool Sprawl Drives Plans to Outsource Detection and Response." Consultato il 18 novembre 2022 all'indirizzo https://www.multivu.com/players/English/8967351-trend-micro-cybersecurity-tool-sprawl-drives-plans-outsource-detection-response.

95 Jim DeLoach. (June 21, 2022). *Forbes*. "Cybersecurity And Data Privacy: 7 Challenges For CFOs To Address." Consultato il 23 novembre 2022 all'indirizzo https://www.forbes.com/sites/jimdeloach/2022/06/21/cybersecurity-and-data-privacy-7-challenges-for-cfos-to-address.

96 Jim DeLoach. (June 21, 2022). *Forbes*. "Cybersecurity And Data Privacy: 7 Challenges For CFOs To Address." Consultato il 23 novembre 2022 all'indirizzo https://www.forbes.com/sites/jimdeloach/2022/06/21/cybersecurity-and-data-privacy-7-challenges-for-cfos-to-address.

97 Jim DeLoach. (June 21, 2022). *Forbes*. "Cybersecurity And Data Privacy: 7 Challenges For CFOs To Address." Consultato il 23 novembre 2022 all'indirizzo https://www.forbes.com/sites/jimdeloach/2022/06/21/cybersecurity-and-data-privacy-7-challenges-for-cfos-to-address.

98 Jim DeLoach. (June 21, 2022). *Forbes*. "Cybersecurity And Data Privacy: 7 Challenges For CFOs To Address." Consultato il 23 novembre 2022 all'indirizzo https://www.forbes.com/sites/jimdeloach/2022/06/21/cybersecurity-and-data-privacy-7-challenges-for-cfos-to-address.

99 Jim DeLoach. (June 21, 2022). *Forbes*. "Cybersecurity And Data Privacy: 7 Challenges For CFOs To Address." Consultato il 23 novembre 2022 all'indirizzo https://www.forbes.com/sites/jimdeloach/2022/06/21/cybersecurity-and-data-privacy-7-challenges-for-cfos-to-address.

100 Jim DeLoach. (June 21, 2022). *Forbes*. "Cybersecurity And Data Privacy: 7 Challenges For CFOs To Address." Consultato il 23 novembre 2022 all'indirizzo https://www.forbes.com/sites/jimdeloach/2022/06/21/cybersecurity-and-data-privacy-7-challenges-for-cfos-to-address.

101 Jim DeLoach. (June 21, 2022). *Forbes*. "Cybersecurity And Data Privacy: 7 Challenges For CFOs To Address." Consultato il 23 novembre 2022 all'indirizzo https://www.forbes.com/sites/jimdeloach/2022/06/21/cybersecurity-and-data-privacy-7-challenges-for-cfos-to-address.

102 Jim DeLoach. (June 21, 2022). *Forbes*. "Cybersecurity And Data Privacy: 7 Challenges For CFOs To Address." Consultato il 23 novembre 2022 all'indirizzo https://www.forbes.com/sites/jimdeloach/2022/06/21/cybersecurity-and-data-privacy-7-challenges-for-cfos-to-address.

FUTURE/TENSE

TREND MICRO
SECURITY PREDICTIONS
FOR 2023

TREND MICRO™ | research

TREND MICRO™ RESEARCH

Trend Micro, leader globale di cybersecurity, è impegnata a rendere il mondo un posto più sicuro per lo scambio di informazioni digitali. Con oltre 30 anni di esperienza nella security, nel campo della ricerca sulle minacce e con una propensione all'innovazione continua, Trend Micro protegge oltre 500.000 organizzazioni e milioni di individui che utilizzano il cloud, le reti e i più diversi dispositivi, attraverso la sua piattaforma unificata di cybersecurity. La piattaforma unificata di cybersecurity Trend Micro One abilita tecniche avanzate di difesa dalle minacce, rilevamento e risposta estesi (XDR) e si integra con i diversi ecosistemi IT, inclusi AWS, Microsoft e Google, permettendo alle organizzazioni di comprendere, comunicare e mitigare al meglio i rischi cyber. Con 7.000 dipendenti in 65 Paesi, Trend Micro permette alle organizzazioni di semplificare e mettere al sicuro il loro spazio connesso.

www.trendmicro.com