TREND MICRO | research

TURNING THE TIDE

La marea è salita, è ora di invertire la tendenza

Le previsioni sulla sicurezza di Trend Micro per il 2021

TURNING THE TIDE

Le previsioni sulla sicurezza di Trend Micro per il 2021

La pandemia di coronavirus (Covid-19) ha cambiato il modo in cui molte aziende operano trasformando in normalità il lavoro da remoto. Passare da un ufficio tradizionale a una workstation domestica — situazione potenzialmente destinata a durare a lungo — presenta tuttavia nuovi rischi per la sicurezza delle aziende dal momento che sempre più malintenzionati cercano di sfruttare la spiacevole situazione provocata dal Covid-19.

Nelle nostre previsioni per il 2020 avevamo affermato che il vecchio paradigma, quello nel quale le reti restano tradizionalmente isolate dietro un firewall aziendale, sarebbe venuto meno. Protezioni e configurazioni tradizionali non sono più adeguate in un ecosistema che impone il ricorso a una vasta varietà di servizi e piattaforme.

Quando la pandemia di Covid-19 ha colpito, le aziende hanno dovuto fare rapidamente i conti con una nuova realtà che ha fatto emergere i problemi presenti e mai risolti ed evidenziato tutte le segnalazioni di criticità ignorate per anni dalla cybersecurity. La situazione ha anche evidenziato come le aziende di tutto il mondo corrano il forte rischio di interrompere improvvisamente le attività a causa di cyberattacchi, crisi globali e altri possibili eventi estremi. Anche se il rischio c'è sempre stato, la pandemia ha solo sottolineato la gravità del problema: come si è equipaggiati o preparati in vista di scenari del genere?

Nel 2021 le aziende dovranno darsi da fare per restare al sicuro, a fronte di una crescita della dipendenza dall'online. Affrontiamo qui gli sviluppi che non sono solamente plausibili ma anche prevedibili. Esamineremo i fattori trainanti della cybersecurity per il prossimo futuro e il modo in cui le aziende dovranno adattarsi di fronte all'influenza esercitata dalle minacce e dalle tecnologie. Il nostro studio intende offrire ad aziende e decision maker la possibilità di definire una risposta appropriata e strategica, in grado di reggere di fronte a cambiamenti e imprevisti.

I cybercriminali utilizzeranno le postazioni di home office come nuovi hub criminali

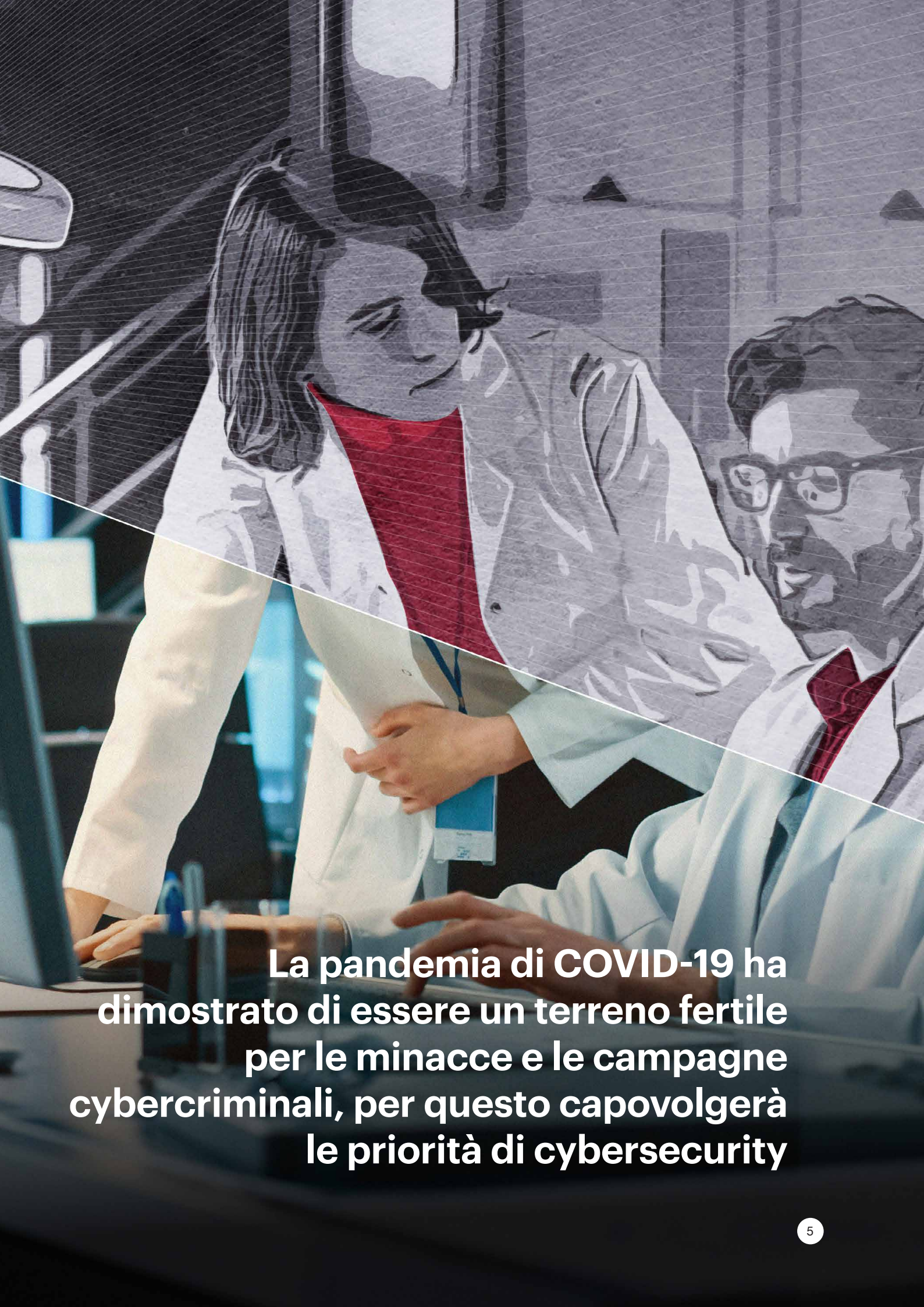
L'attuale pandemia e i conseguenti lockdown imposti in molti angoli del pianeta hanno costretto una grande quantità di dipendenti a entrare in un territorio sconosciuto, quello del telelavoro, molto spesso facendoli lavorare da casa a tempo pieno. Di conseguenza molti dipendenti e molte aziende stanno iniziando a valutare la fattibilità di proseguire con il modello dello smart working anche in prospettiva futura. In circostanze del genere utenti e organizzazioni dovranno proteggere le postazioni di lavoro domestiche dalle minacce, e questo vale non soltanto per i team IT chiamati a mettere improvvisamente in sicurezza intere forze lavoro remote, ma anche per i singoli utenti che saranno chiamati a prendere le loro precauzioni.

I confini tra vita lavorativa e vita privata sono venuti meno, e il lavoro viene svolto attraverso ISP (Internet Service Provider) domestici solitamente attraverso router e macchine senza patch, con altri dispositivi connessi in parallelo o membri della stessa famiglia che condividono i medesimi computer pur lavorando per aziende differenti. Per quanto le reti VPN (Virtual Private Network) possano proteggere le connessioni con l'azienda, gli utenti che lavorano da casa dovranno essere attenti alle vulnerabilità delle VPN che potrebbero favorire attacchi da remoto.[1, 2]

Le reti domestiche diventeranno inoltre il punto di partenza dal quale muoveranno i cybercriminali interessati ad assumere il controllo delle macchine e passare ad altri dispositivi collegati alla stessa rete, con l'obiettivo di mettere un piede all'interno di qualche azienda. Questi personaggi cercheranno di sfruttare il software installato o vulnerabilità lasciate prive di patch per saltare da una macchina all'altra fino a quando non troveranno un bersaglio adatto. Questi cosiddetti "attacchi supply chain" si diffonderanno quindi ad altri utenti. I dipendenti che accedono a informazioni riservate e sensibili (per esempio chi lavora nelle risorse umane, nelle vendite o nel supporto tecnico) saranno inoltre oggetto di attacchi mirati per la sottrazione di dati e la mancanza di un sistema IDS (Intrusion Detection System) o di un firewall abbinata alla disponibilità di una connessione Internet ad alta velocità, semplifica parecchio lo spostamento di un malintenzionato da una rete aziendale all'altra.

I router sono considerati da tempo bersagli privilegiati per attacchi remoti contro dispositivi connessi. I cybercriminali offriranno accesso a router compromessi come un nuovo servizio, per vendere la possibilità di entrare all'interno di reti domestiche. Queste proposte access-as-a-service diventeranno un lucroso modello di business per i malintenzionati che potranno stabilire una presenza persistente e offrire ai loro colleghi l'accesso a reti domestiche di alto valore, come quelle delle abitazioni di dirigenti o amministratori IT. Le aziende dotate di reti convergenti saranno i principali obiettivi e si troveranno nel mirino di chi intende guadagnare vendendo accesso a reti OT (Operational Technology). Nel 2021, saper sfruttare un punto debole nello spazio IT (Information Technology) potrà risultare redditizio per chi vuole far cassa con gli accessi alle reti OT.

Disporre di policy aziendali dettagliate per la sicurezza aiuterà a fare in modo che lo scambio di dati tra uffici e dipendenti che lavorano da remoto sia protetto adeguatamente e che gli ambienti home office non diventino un gateway per varie forme di cybercrimine. Un piano di risposta agli incidenti dovrà definire l'approccio alla sicurezza di un'azienda con una rete nella quale siano presenti macchine discrete. Le aziende dovranno istruire i dipendenti in smart working affinché mettano al sicuro router domestici e IoT (Internet of Things), oltre che l'utilizzo di reti VPN (Virtual Private Network). Ciò dovrebbe comprendere un briefing sui rischi del riutilizzare le stesse password e mantenere le password di default di router e dispositivi IoT. Raccomandiamo inoltre di segmentare le reti residenziali in modo da isolare i computer aziendali (per esempio ricorrendo a una VLAN, Virtual Local Area Network, dedicandola esclusivamente all'attività lavorativa).



La pandemia di COVID-19 ha dimostrato di essere un terreno fertile per le minacce e le campagne cybercriminali, per questo capovolgerà le priorità di cybersecurity

I cybercriminali approfittano di qualsiasi evento di rilievo per manipolare e sabotare e la pandemia di coronavirus non fa eccezione: semplicemente cambiano le tattiche per sfruttare le paure collettive collegate al Covid-19. Nel nostro report di metà 2020[3] avevamo notato un netto incremento nel numero di email fraudolente, spam e tentativi di phishing inerenti al Covid-19 da quando era iniziata la crisi. I cybercriminali continueranno a cogliere le opportunità di social engineering e manterranno attive campagne contenenti esche ispirate al coronavirus..

Il Covid-19 continuerà a porre sfide di cybersecurity alle aziende globali. L'e-commerce, per esempio, ha registrato in questi anni una crescita sostenuta e la pandemia non ha fatto altro che rafforzarla. Il crimine organizzato cercherà di penetrare nel settore logistico man mano che l'online shopping aumenta e, con esso, la quantità di pacchi e colli che devono essere consegnati. Reati come sabotaggio della produzione, contrabbando e trasporto di merci contraffatte emergeranno come modalità operativa dei cybercriminali nel corso della pandemia.

Il settore della sanità, in particolare, finirà sotto i riflettori. Molti medici sono passati alla telemedicina e l'erogazione di servizi sanitari è divenuta ancora più critica, quindi la sicurezza IT dei sistemi nella sanità sarà messa alla prova. I team responsabili della sicurezza non dovranno solamente affrontare i rischi associati ai dati dei pazienti e agli attacchi di malware,[4] ma anche la possibilità di subire spionaggio.

Gruppi di malintenzionati effettueranno ricognizioni nei laboratori dove si sviluppano i vaccini per il coronavirus colpendo in particolare gli istituti che hanno pubblicamente comunicato di lavorare alla ricerca contro il Covid-19. I criminali tenteranno di acquisire intelligence sui risultati ottenuti e sottrarre i dati di ricerca sui vaccini e su altri medicinali. Questi potenziali furti di informazioni medicali rallenteranno la ricerca stessa mettendo a rischio il rilascio e la produzione di cure adatte.

Anche le campagne di disinformazione renderanno difficile per gli utenti riuscire a far chiarezza tra le mille incertezze della pandemia. I malintenzionati sfrutteranno la disinformazione per attirare gli utenti affinché facciano click su allegati e link pericolosi. Questi tentativi di truffa saranno veicolati tramite email, app fasulle, domini civetta e social media, pretendendo di offrire informazioni utili alla salute o su presunti vaccini e relative liste d'attesa.[5] I vaccini saranno quindi utilizzati come argomento esca per il phishing non appena diventeranno disponibili.

Il lavoro da remoto costringerà le organizzazioni a ripensare le infrastrutture di security non più sostenibili e a considerare gli ambienti ibridi

Nel 2021 il lavoro da remoto si consoliderà e gli ambienti ibridi, quelli nei quali attività personali e lavorative si mischiano in una stessa macchina, lanceranno una sfida significativa alle aziende che potranno esercitare un controllo inferiore su quel che i loro dipendenti utilizzano. Mescolare attività personali e lavorative (ad esempio adoperare la stessa macchina per svolgere attività online differenti) attenua il confine tra gli ambienti in cui i dati vengono conservati ed elaborati. Se un dispositivo di lavoro viene infettato, i dati personali saranno presi in considerazione in fase di pulizia e ripristino della macchina? Esiste un modo per tenere traccia dei dati che vengono stampati o esportati? Questa minore visibilità da parte delle aziende circa quel che accade sui dispositivi è ulteriormente aggravata quando i dipendenti accedono ad applicazioni personali da quegli stessi dispositivi.

Dopo che varie tecnologie impiegate per il telelavoro hanno fatto notizia per le loro carenze di sicurezza, i modelli zero trust sono destinati ad acquistare importanza nel 2021 come approccio efficace alla forza lavoro distribuita. Eliminando la fiducia implicita su qualsiasi cosa sia collegata internamente o esternamente alla rete, tutto viene di conseguenza verificato.[6] Attraverso la micro-segmentazione, un'architettura zero trust permette agli utenti di accedere solamente alle specifiche risorse necessarie all'interno di determinati perimetri. Un ambiente del genere assicura una robusta postura di sicurezza rendendo molto più difficile la compromissione delle reti da parte dei malintenzionati. L'approccio zero trust si integra facilmente con la tecnologia basata su cloud SASE (Secure Access Service Edge) fornendo ai team di sicurezza la visibilità necessaria su tutto il traffico in ingresso e in uscita.

Sulla scia della pandemia, le aziende hanno modificato le loro infrastrutture IT e velocizzato il passaggio verso il cloud. Infrastrutture che normalmente faticherebbero sugli aggiornamenti tecnologici stanno invece accelerando i programmi di trasformazione. Coloro che si affidano alle tradizionali soluzioni on-premise non potranno tenere il ritmo delle necessità che la sicurezza di applicazioni e software in cloud possono richiedere. Sarà quindi un obiettivo delle aziende, indipendentemente dal settore o comparto economico, quello di assicurarsi di essere sufficientemente versatili e agili da riuscire a vincere le sfide che le attendono.

Dai viaggi virtuali all'entertainment remoto, continueranno a sorgere nuovi modelli di business man mano che vari operatori porteranno ulteriori innovazioni sulle piattaforme digitali. Le soluzioni tecnologiche emergenti aiuteranno nel lavoro quotidiano degli utenti home office per mezzo di app basate su IA. Prima di dover affrontare inevitabilmente nuove forme di crimine digitale, queste app faranno comunque fatica a farsi conoscere e prendere piede sul mercato.

In risposta alla pandemia, le aziende hanno capito la necessità di riorientare la propria sicurezza e proteggere i dipendenti remoti per assicurare la continuità business. I team IT dovranno ribaltare gli approcci alla sicurezza per includere il telelavoro a lungo termine. Le aziende farebbero inoltre bene a definire policy per lo smart working (compreso il coordinamento con Managed Service Provider) e la gestione dei dati facendo rispettare il più possibile la linea di separazione tra utilizzo personale e utilizzo business dei dispositivi.

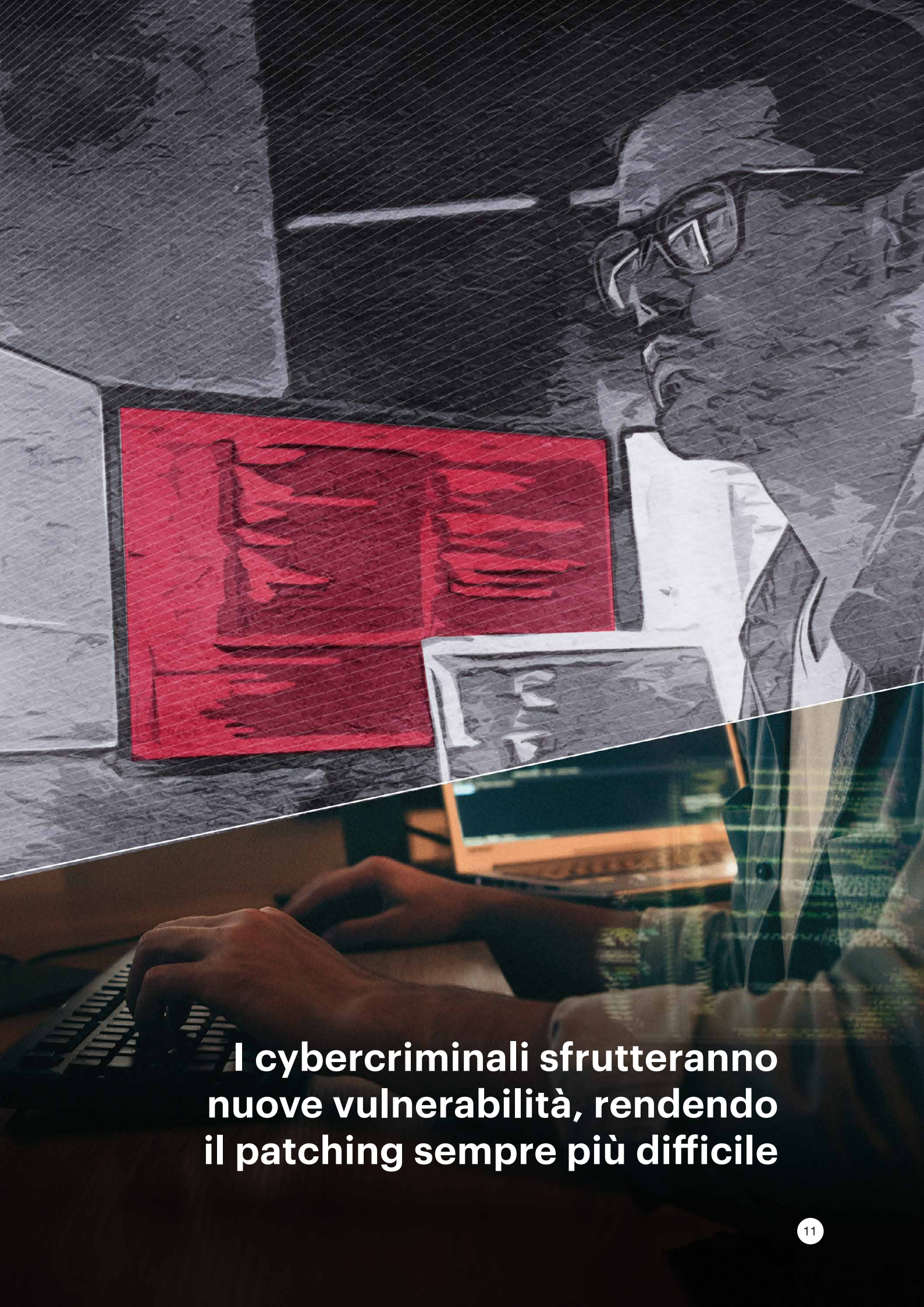
L’utilizzo di tecnologie di contact tracing aumenterà l’attenzione dei cybercriminali nei confronti dei dati degli utenti

Livelli inediti di raccolta di dati[7] stabiliti nel tentativo di monitorare lo stato di salute delle persone attireranno criminali e attivisti politici interessati a ottenere tali informazioni. La fretta con cui si implementano queste misure non farà altro che aumentare il rischio di lasciare i dati esposti o di farseli possibilmente sottrarre.

Un accesso rapido ai dati potrebbe essere cruciale nella lotta alla pandemia, ma l'attenuazione delle misure di tutela della privacy provoca un insieme di altri problemi. Database di grandi dimensioni unitamente a implementazioni affrettate sono obiettivi succulenti per i malintenzionati che intendono compromettere i dati così raccolti e conservati. I gruppi cybercriminali possono abusare di questi dati in vari modi, per esempio estraendo le informazioni sulle identità per rivenderle tramite i loro canali underground.

L'assenza di protezioni e rigidi protocolli lascia i server o i database vulnerabili. Le pubbliche amministrazioni dovranno preparare e implementare i passi necessari per tenere i dati al riparo dagli hacker.

Le iniziative tese a rallentare la diffusione del virus comprendono anche i lockdown, che hanno implicazioni economiche su diverse supply chain. L'impatto economico e operativo genera nelle aziende limitazioni di budget per le attività rivolte alla sicurezza rendendo difficile il lavoro dei team chiamati a mantenere, se non addirittura incrementare, la copertura protettiva a fronte di disponibilità finanziarie ridotte.



I cybercriminali sfrutteranno nuove vulnerabilità, rendendo il patching sempre più difficile

Anche se le vulnerabilità zero-day tendono a conquistare le luci della ribalta quando si parla di attacchi, le vulnerabilità già note (o n-day) provocheranno significative preoccupazioni nel 2021. Se il termine zero-day si riferisce a bug o errori che sono appena stati identificati ma per i quali manca ancora una patch, le vulnerabilità n-day sono quelle che sono state rese pubblicamente note e per le quali possono essere già disponibili patch. Esistono infinite vulnerabilità note, e molte aziende scopriranno di avere il fianco notevolmente esposto nei rispettivi footprint digitali.

Nel 2021 si verificherà una rapida diffusione delle vulnerabilità n-day annunciate dalla comunità dei ricercatori insieme con le tecniche necessarie per metterle a frutto. Gli attaccanti trasformeranno le vulnerabilità appena annunciate in armi utilizzabili nei loro framework di attacco. Nel corso di Operation Poisoned News, i malintenzionati hanno sfruttato il codice presentato nella prova concettuale (POC) di una vulnerabilità n-day approfittando di diversi bug per l'escalation dei privilegi resi noti da Google Project Zero.[8] I responsabili di Earth Kitsune hanno agito in modo simile modificando gli exploit pubblicati da Project Zero e dalla Zero Day Initiative (ZDI) di Trend Micro.[9]

Le vulnerabilità n-day rappresenteranno una miniera d'oro per i cybercriminali che sono alla ricerca di punti deboli pronti da usare immediatamente. Gli exploit riportati negli attacchi possono essere anche accompagnati da documenti consultabili pubblicamente, a differenza delle vulnerabilità zero-day che richiedono un lungo e difficile lavoro prima di essere identificate e messe a frutto.

Prevediamo l'apertura di marketplace specializzati nelle vulnerabilità n-day o nella vendita di bug noti e sfruttabili, laddove i dati inerenti alla vulnerabilità vengono modificati secondo le esigenze del malintenzionato di turno. Non è fantasioso ipotizzare l'offerta di un servizio di personalizzazione degli exploit a seconda dell'attacco desiderato. Se questo permettesse anche a operatori relativamente inesperti di sferrare i loro attacchi, una proposta del genere risulterebbe comunque particolarmente interessante per quei gruppi criminali che sono conosciuti per sfruttare vulnerabilità zero-day e n-day contro bersagli di alto valore. I gruppi più sofisticati, inoltre, potenzieranno l'impiego di tool per il penetration testing come il diffusissimo Cobalt Strike, il cui codice sorgente è stato apparentemente divulgato nel novembre 2020.[10]

Le API’s saranno il nuovo vettore di attacco preferito dai cybercriminali per le violazioni aziendali

Una Application Programming Interface (API) non è altro che un software intermediario che permette la comunicazione tra più applicazioni – dalla condivisione di dati e dalla messa a disposizione di funzionalità fino alla razionalizzazione delle operazioni e della connettività di sistema – fornendo protocolli, routine e tool per poter implementare servizi e software all'interno di dispositivi compresi quelli IoT. Molte aziende si affidano alle API per fornire l'accesso ai loro sistemi interni e interagire con i clienti attraverso app.

L'avvertenza è che le API rappresentano anche un frutto maturo per i malintenzionati che vanno alla ricerca di un punto di ingresso alle reti aziendali. Con l'aumentare della presenza delle API nello spazio enterprise, la loro superficie di attacco diventerà più visibile. Le API sono destinate a essere un bersaglio privilegiato dal momento che servono anche per l'integrazione di terze parti, e prevediamo che la sicurezza delle API sarà una nuova area di interesse per i cybercriminali nel 2021.

Per quanto già universalmente diffuse, le API sono ancora molto indietro per quanto riguarda la sicurezza e introducono diversi punti deboli che possono essere sfruttati come vettori per violare le applicazioni enterprise. Alcuni casi avvenuti di recente hanno provocato l'accesso a informazioni personali di utenti[11, 12] e la scoperta di codice sorgente e accessi vulnerabili a servizi di backend.[13]

Le API sono anche relativamente semplici da scoprire, hanno molti parametri che si prestano a comprometterle, e sono insicure. I tradizionali meccanismi di difesa come Captcha, JavaScript o tool SDK per ambienti mobili non possono essere usati efficacemente per prevenire un attacco automatizzato,[14] il che significa che le API sono protette solo parzialmente se non per nulla. Consigliamo quindi di configurare meccanismi di autenticazione e controllo degli accessi con un approccio difensivo approfondito unito al monitoraggio regolare dei log di accesso.

I software enterprise e le applicazioni cloud utilizzati per il lavoro da remoto saranno bersagliati da bug critici

Come conseguenza di un aumento delle attività di ricerca, ci aspettiamo che i software e i servizi utilizzati nel lavoro distribuito incappino in un maggior numero di vulnerabilità che saranno rese pubblicamente note. Consultando i dettagli delle vulnerabilità che vengono rilasciati apertamente, gli utenti possono verificare i problemi di sicurezza dei loro sistemi, ma ciò permette anche a ricercatori e malintenzionati di cercare vulnerabilità simili all'interno dei sistemi, specialmente se i difetti scoperti sono relativamente nuovi. I ricercatori si concentreranno soprattutto sui bug di natura critica e sulle relative varianti presenti nel software enterprise e in altre tecnologie usate per il telelavoro. Cybercriminali e gruppi di malintenzionati sfrutteranno per le loro campagne i punti deboli dei pacchetti software più diffusi.

Nel 2021 saranno particolarmente ricercate le vulnerabilità legate a Microsoft Teams, SharePoint, Office 365 ed Exchange. Trattare informazioni potenzialmente sensibili all'interno di queste piattaforme software di collaborazione rappresenterà un'importante preoccupazione per le aziende che hanno crescenti quantità di dipendenti in remoto, specialmente nei settori regolamentati come i servizi finanziari e la sanità.

Con una rinnovata spinta per passare agli ambienti cloud e all'uso di strumenti di collaborazione, la sicurezza del cloud sarà un argomento più attuale che mai. Per ottenere visibilità sui sistemi e rispondere alle esigenze di scalabilità, le aziende raccolgono e conservano enormi quantità di dati attraverso molteplici fonti e ambienti. Questi cloud di log, tuttavia, saranno l'obiettivo centrale di moderni cybercrimini di alto profilo. Negli ambienti cloud si conservano spesso interi patrimoni di preziosi dati sensibili che i criminali possono usare per scoprire punti di accesso alle reti.

L'adozione delle tecnologie cloud avvenuta nel 2020 proseguirà nel 2021 per reagire agli effetti della pandemia sulle operazioni aziendali. Ci aspettiamo che questa tendenza continui a crescere anche quando la pandemia verrà meno. Verso la fine del 2021 la maggior parte dei workload si troverà nel cloud. Le aziende che si sono mosse in modo frettoloso e disordinato dovranno fare i conti con le implicazioni relative alla sicurezza. Prevediamo che le violazioni dei dati e delle infrastrutture cloud non saranno causate solamente dai cloud provider, ma anche dagli errori di configurazione e dai passi falsi compiuti da utenti inconsapevoli.

Altri elementi di preoccupazione per chi adotta il cloud riguardano i tentativi degli hacker di assumere il controllo dei relativi server per installare immagini di container modificate in modo tale da essere dannose. Ci aspettiamo un boom di immagini vulnerabili all'interno di varie architetture in concomitanza con la fiducia illimitata che gli utenti metteranno nei depositi di container e nei relativi servizi. Queste immagini dannose cercheranno di prendere il controllo delle repository e modificare le risorse a fini malevoli.[15] I dati vulnerabili saranno un problema comune che porterà a violazioni e attacchi basati su cloud.

Andiamo avanti: attenzione alla cybersecurity

Le previsioni sulla sicurezza di Trend Micro per il 2021 riflettono il lavoro di ricerca e gli approfondimenti dei nostri esperti sulle tematiche emergenti nei campi della tecnologia e della sicurezza. Ecco ora alcune raccomandazioni per contrastare le minacce che abbiamo elencato con attività di intelligence e risposta globale:

Promuovete la consapevolezza e la formazione degli utenti. I malintenzionati continueranno a far leva sulle paure che circondano il Covid-19 e gli utenti devono essere quindi informati sulle tattiche e sui possibili vettori di attacco. Le aziende dovrebbero rafforzare le conoscenze delle minacce ed estendere le loro best practice interne anche alle abitazioni dei loro dipendenti. Condividete ciò che è bene fare e non fare nel telelavoro e consigliate di non usare dispositivi personali.

Mantenete un rigido controllo sugli accessi a reti aziendali e home office. Le aziende dovrebbero impegnarsi per creare policy basate sulla sicurezza e un piano di risposta che copra l'intero perimetro delle loro operazioni in caso di incidente. In questo modo si rafforzeranno servizi, workstation e dati corporate mentre le aziende potranno lavorare in remoto. Evitate di fidarvi implicitamente di asset o account utente indipendentemente da dove si trovino.

Reiterate le misure di sicurezza basilari e i programmi per la gestione delle patch. Nei prossimi mesi di telelavoro continueranno a spuntare nuovi punti deboli, ed è quindi essenziale implementare regolarmente aggiornamenti e patch di applicazioni e sistemi che sono oggi più vulnerabili che mai.

Potenziate il rilevamento delle minacce con le competenze di esperti. Dovete assicurarvi una gestione avanzata H24 di minacce e incidenti nei workload cloud, nella posta elettronica, negli endpoint, nelle reti e nei server con l'assistenza di analisti specializzati nella sicurezza. Potete ottenere insight più approfonditi sugli attacchi e mettere in ordine di priorità gli allarmi attraverso una intelligence completa su quanto accade nel settore della sicurezza e soluzioni specifiche all'avanguardia.

Fonti

1 Cybersecurity and Infrastructure Security Agency. (January 10, 2020). *US-CERT.* “Continued Exploitation of Pulse Secure VPN Vulnerability.” Accessed on Nov. 10, 2020, at https://us-cert.cisa.gov/ncas/alerts/aa20-010a.

2 Charlie Osborne. (July 17, 2020). *ZDNet.* “Cisco releases security fixes for critical VPN, router vulnerabilities.” Accessed on Nov. 10, 2020, at https://www.zdnet.com/article/cisco-releases-fixes-for-critical-vpn-router-vulnerabilities/.

3 Cybersecurity and Infrastructure Security Agency. (October 28, 2020). *US-CERT.* “Ransomware Activity Targeting the Healthcare and Public Health Sector.” Accessed on Nov. 10, 2020, at https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

4 Cybersecurity and Infrastructure Security Agency. (October 28, 2020). *US-CERT.* “Ransomware Activity Targeting the Healthcare and Public Health Sector.” Accessed on Nov. 10, 2020, at https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

5 Trend Micro. (April 24, 2020). *Trend Micro.* “Developing Story: COVID-19 Used in Malicious Campaigns.” Accessed on Nov. 10, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

6 Mary K. Pratt. (January 16, 2020). *CSO Online.* “What is Zero Trust? A model for more effective security.” Accessed on Nov. 12, 2020, at https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html.

7 Elizabeth Beattie. (April 3, 2020). *Al Jazeera Media Network.* “We’re watching you: COVID-19 surveillance raises privacy fears.” Accessed on Nov. 11, 2020, at https://www.aljazeera.com/news/2020/4/3/were-watching-you-covid-19-surveillance-raisesprivacy-fears.

8 Elliot Cao et al. (March 24, 2020). *Trend Micro.* “Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links.” Accessed on Nov. 12, 2020, at https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/.

9 Nelson William Gamazo Sanchez et al. (October 19, 2020). *Trend Micro.* “Operation Earth Kitsune: Tracking SLUB’s Current Operations.” Accessed on Nov. 12, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-earth-kitsune-tracking-slub-s-current-operations.

10 Lawrence Abrams. (November 11, 2020). *BleepingComputer.* “Alleged source code of Cobalt Strike toolkit shared online.” Accessed on Nov. 17, 2020, at https://www.bleepingcomputer.com/news/security/alleged-source-code-of-cobalt-strike-toolkit-shared-online/.

11 Zack Whittaker. (August 20, 2020). *TechCrunch.* “Fearing coronavirus, a Michigan college is tracking its students with a flawed app.” Accessed on Nov. 11, 2020, at https://techcrunch.com/2020/08/19/coronavirus-albion-security-flaws-app/.

12 Guy Rosen. (September 28, 2018). *Facebook.* “Security Update.” Accessed on Nov. 11, 2020, at https://about.fb.com/news/2018/09/security-update/.

13 Danny Palmer. (April 2, 2019). *ZDNet.* “Security flaws in banking apps expose data and source code.” Accessed on Nov. 11, 2020, at https://www.zdnet.com/article/security-flaws-in-banking-apps-expose-data-and-source-code/.

14 Edward Amoroso. (June 5, 2020). *Help Net Security.* “Understanding cyber threats to APIs.” Accessed on Nov. 11, 2020, at https://www.helpnetsecurity.com/2020/06/05/api-security-threats/.

15 Trend Micro. (May 14, 2019). *Trend Micro.* “Container Security: Examining Potential Threats to the Container Environment.” Accessed on Nov. 12, 2020, at https://www.trendmicro.com/vinfo/us/security/news/security-technology/container-security-examining-potential-threats-to-the-container-environment.

TURNING THE TIDE

La marea è salita, è ora di invertire la tendenza

Le previsioni sulla sicurezza di Trend Micro per il 2021

TREND MICRO | research

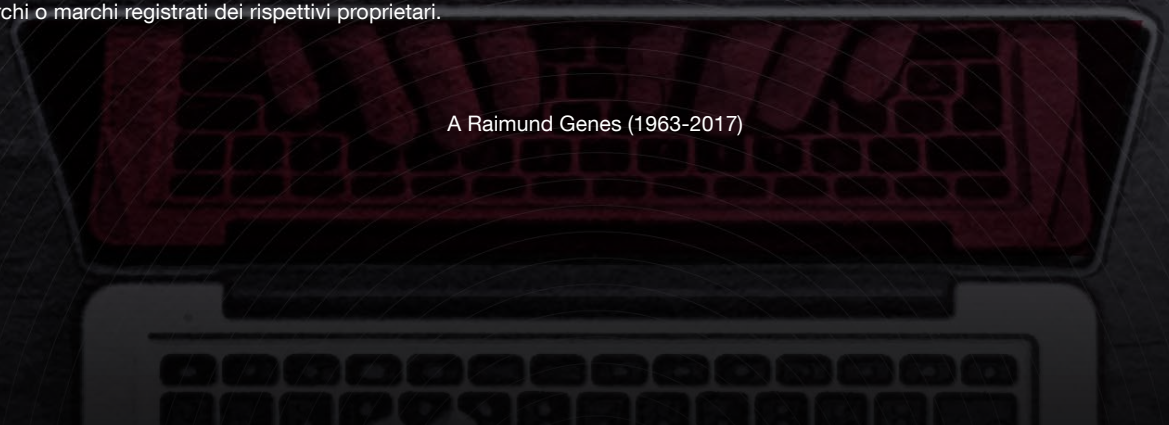
TREND MICRO™ RESEARCH

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 e nel campo della ricerca sulle minacce, con una propensione all'innovazione continua, Trend Micro permette a Istituzioni, aziende e persone di essere resilienti grazie a soluzioni connesse che proteggono i workload cloud, gli endpoint, le email, i dispositivi IIoT (Industrial Internet of Things) e le reti. In particolare, la strategia di security XGen™ di Trend Micro alimenta tutte le soluzioni attraverso un insieme di tecniche intergenerazionali di difesa dalle minacce, ottimizzate per i principali ambienti. Queste utilizzano un'intelligence condivisa per una protezione migliore e più veloce.

Con più di 6.800 dipendenti in oltre 65 Paesi e detenendo le informazioni sulle minacce più avanzate al mondo, Trend Micro consente alle im-prese di mettere al sicuro il loro spazio connesso

www.trendmicro.com



A Raimund Genes (1963-2017)